LONDON METROPOLITAN UNIVERSITY

DOCTORAL THESIS

Digital Forensic Readiness in IoT-Enabled Organisations and Forensic Investigation Analysis in Real-Time

---

By:

Oyeyemi Kuku

First Supervisor:

Dr. Alexandros Chrysikos

Second Supervisor

Dr. Shahram Salekzamankhani

A thesis submitted in fulfilment of the requirements

for the degree of Doctor of Philosophy

in the

London Metropolitan University

Cyber Security Research Centre

School of Computing and Digital Media

Date: February 2026

Declaration of Authorship

I, Oyeyemi Kuku, declare that my work is titled "Digital Forensic Readiness in IoT-Enabled Organisations and Forensic Investigation Analysis in Real-Time." I am writing this thesis on my own. I confirm that:

- This work was done wholly or mainly during my candidature for a research degree at this university.
- It has been clearly stated that any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. However, except for such quotations, this thesis is entirely my work.
- I have acknowledged all primary sources of help.
- Where the thesis is based on work I did jointly with others, I have clarified exactly what others did and what I contributed myself.

Signed: Oyeyemi Kuku

_____

Date:

_____

Abstract

The rapid growth of the Internet of Things (IoT) has transformed organisational digital environments into highly distributed, data-driven ecosystems. While many organisations invest heavily in cybersecurity tools to detect and respond to threats, far fewer are equipped to systematically identify, collect, preserve, and analyse digital evidence in a timely, cost-effective, and legally compliant manner. This gap in Digital Forensic Readiness (DFR) is particularly critical in IoT-enabled organisations, where potential evidence is distributed across diverse, often volatile devices, networks, and platforms. This research presents a Digital Forensic Readiness Model aligned with ISO/IEC 27043, specifically tailored for organisational IoT environments. The model combines governance, technical infrastructure, and security preparedness into a unified framework, emphasising forensic readiness as an ongoing organisational capability rather than a reactive, post-incident measure. It supports proactive evidence identification, real-time collection, secure preservation, and reliable chain-of-custody management, thereby protecting the integrity of forensic processes within complex IoT ecosystems.

The model was tested through practical deployment within a controlled organisational setting using real-world security monitoring and forensic tools. Several simulated cyberattack scenarios were conducted to evaluate their effectiveness in realistic operational environments. Machine learning-based analysis was also used to prioritise forensic artefacts and identify key evidential features, enhancing investigative efficiency while adhering to legal and evidential standards. The results demonstrate that the proposed model significantly improves organisational forensic readiness by reducing investigation time, maintaining evidence integrity and traceability, and enabling automated, standards-compliant forensic procedures. This study offers a practical, implementable DFR model that links international forensic standards to real-world IoT deployments, strengthening organisational cyber resilience and digital investigative capabilities.

Acknowledgements

I want to express my sincere gratitude to my first supervisor, Dr Alexandros Chrysikos, for his guidance, support, and invaluable insights throughout this PhD journey. I am equally grateful to my second supervisor, Dr Shahram Salekzamankhani, for his constructive feedback, encouragement, and academic support. Their expertise, mentorship, and commitment were instrumental in the successful completion of this research. I truly thank both supervisors for their motivation, mentorship, and collaborative approach, which were crucial to the successful completion of this PhD.

I would also like to thank Dr Dapo Odunsin for facilitating access to the laboratory and supporting aspects of this research. My sincere appreciation goes to Boštjan Hamler, Chief Technology Officer at Volant Media Limited, and Dimiter Simidchiev, former Head of IT, for their support, technical collaboration, and for providing the resources and environment necessary to conduct this study. I am sincerely grateful to my colleagues at Volant Media for their support, encouragement, and cooperation throughout this research journey. Their assistance and the opportunities provided were invaluable to the successful completion of this study.

I would also like to thank my mother, Deaconess Olufunmilayo Kuku, my sisters, Dr Olubukunola Banjoko and Mrs Yetunde Ogun, for their unwavering support, prayers, and encouragement. My heartfelt appreciation goes to my father in the Lord, Pastor Joseph Obayemi, and to my dear friends, Deacon and Deaconess Niyi Olubodun, and Mr and Mrs Kehinde Ekundayo, for their continual prayers and support.

Finally, my deepest gratitude goes to my beloved wife, Pastor (Mrs) Mutiat Kuku, and my wonderful children, Elijah, Elisha, Elizabeth, and Ezekiel Kuku, for their love, patience, understanding, and unwavering support throughout this journey. Thank you for standing by me every step of the way.

This achievement is as much yours as it is mine, and I will always be grateful for the love and support you have shown me. Thank you all for being part of this remarkable journey.

Table of Contents

List Of Figures

List Of Tables

List Of Abbreviations

ADS	Attack Detection System
AES	Advanced Encryption Standard
APRM	Automated Proactive Readiness Model
APT	Advanced Persistent Threats
BSN	Body Sensor Networks
CATRAM	Cybersecurity Awareness Training Model 34
CFRaaS	Cloud Forensic Readiness as a Service
CoC	Chain of Custody
CPS	Cyber-Physical Systems
CSAM	Cybersecurity Audit Model
DAS	Data Acquiring Systems
DDoS	Distributed Denial of Service
DEO	Digital Evidence Object
DF	Digital Forensic
DFI	Digital Forensic Investigator
DFIF-IoT	Digital Forensic Investigation Framework for IoT
DFR	Digital Forensic Readiness
DFRF	Digital Forensic Readiness Framework
DFRM	Digital Forensic Readiness Model
DLP	Data Loss Prevention
DNN	Deep Neural Networks
DoD	Department of Defence
ETSecIoT	Emerging Technologies for Security in IoT
EU	European Union
FAIoT	Forensic Awareness Internet of Things
FEMS	Forensic Edge Management System
FIF	Forensic Investigation Framework
FIM	File Integrity Monitoring
FN	False Negative
FP	False Positive
FSAIoT	Forensic State Acquisition from IoT
HCO	Human-Centred Organisations
HDFS	Hadoop Distributed File System
HIDS	Host-Based Intrusion Detection System
I.S	Information Systems
I.T.	Information Technology
IEC	International Electrotechnical Commission
IDS	Intrusion Detection System
IOC	Indicators of Compromise
ISO	International Organisation for Standardisation
ISMS	Information Security Management System
IoT	Internet of Things
IoT-FR	Internet of Things Forensic Readiness
IPS	Intrusion Prevention System

ITR	Insider Threat
LEA	Law Enforcement Agencies
LSTM	Long Short-Term Memory
MD5	Message-Digest Algorithm 5
MoD	Ministry of Defence
M-TISM	Modified Total Interpretive Structural Model
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology
OSSEC	Open-Source Security
PCI DSS	Payment Card Industry Data Security Standard
PDE	Potential Digital Evidence
PIMS	Privacy Information Management System
PUF	Physical Unclonable Functions
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFID	Radio Frequency Identification
RSA	Rivest–Shamir–Adleman
SbD	Security by Design
SDN	Software-Defined Networking
SETA	Security Education Training and Awareness
SIEM	Security Information and Event Management
SIFT	SANS Investigative Forensic Toolkit
SOC	Security Operation Centres
SOF-ELK	Security Operations and Forensics Elasticsearch, Logstash, Kibana
TCL	Tool Command Language
TN	True Negative
TP	True Positive
UI	User Interface
XDR	Extended Detection and Response
WSN	Wireless Sensor Networks

1.0 Introduction

The term "Internet of Things" (IoT) was originally coined by Kevin Ashton in a 1999 presentation at Procter & Gamble to promote new Radio Frequency Identification (RFID) technology. A "thing" in the IoT refers to any device that contains a sensor capable of collecting data and transmitting it over a network without human intervention. The technology embedded within the device enables communication with both internal conditions and the external environment, thereby aiding decision-making. The Internet of Things (IoT) can connect to the internet to exchange users' personal information, making IoT devices susceptible to cyberattacks. More research is necessary to protect IoT devices from these threats and attacks. Consequently, there is a risk that personal devices such as laptops, cameras, refrigerators, TVs, and other gadgets could be exploited by cybercriminals for malicious purposes(Al-Masri et al., 2018).

The Internet of Things (IoT) is a rapidly evolving technology that enables interconnected devices and sensors to communicate over the Internet, offering significant benefits in efficiency, automation, and decision-making across sectors such as healthcare, manufacturing, and retail. However, the widespread adoption of IoT also introduces substantial challenges related to security, confidentiality, and interoperability, as heterogeneous devices employ diverse protocols and generate large volumes of sensitive data. As the number of connected IoT devices continues to increase, projected to grow from 9.7 billion in 2020 to over 30.9 billion by 2025, the attack surface available to cybercriminals expands correspondingly(Vailshery Lionel Sujay, 2022). The emergence of IoT botnets has transformed IoT ecosystems from systems designed to enhance safety into what has been described as an “Internet of Vulnerabilities” (Angrishi, 2017).

The Mirai malware attack exemplified this shift in 2016, when thousands of compromised IoT devices were used to launch large-scale distributed denial-of-service (DDoS) attacks against major online services, including Twitter, PayPal, and Netflix (Kebande et al., 2020). Consequently, organisations face persistent cyber threats despite the widespread adoption of security controls such as firewalls,

antivirus software, intrusion detection systems, encryption, and vulnerability management. Studies indicate that more than 60% of organisations continue to experience frequent attacks and escalating security risks from both internal and external sources (Ghelani, 2022). The distributed and data-intensive nature of IoT environments further complicates digital forensic investigations, as IoT forensics involves handling large volumes of heterogeneous digital evidence and addressing complex security and investigative challenges (Sgurev et al., 2020). These factors highlight the growing need for enhanced forensic investigation capabilities and proactive security management in IoT-enabled organisational environments.

According to various studies, UK companies lose around £27 billion annually, equivalent to the European Commission's entire three-year Horizon 2020 innovation, research, and development budget. The average cost of cybercrime across the European Union has risen to €50,000 per incident. The latest data also shows that companies affected by cyber issues and crimes in the past incurred an average cost of €50,000 per year over the 12 months between 2019 and 2020, representing an almost sixfold increase compared to previous years. Most organisations' approach to cyber incidents currently focuses on business continuity and disaster recovery. However, this approach often involves actions that are contrary to the principles of judicial investigation. Organisations can respond to cyber incidents; this means that when there is a security incident or data breach, they first try to resolve the problem, conduct a forensic investigation, and then collect the actual evidence (SPEAR Project, 2021).

The growing threat of online fraud and security breaches poses significant challenges for law enforcement and digital forensics professionals worldwide. Digital Forensics Readiness (DFR) enables organisations to better prepare for investigations. However, the recurring problem is that organisations need a DFR plan to handle forensic incidents. The DFR program will provide proactive capabilities to prepare for digital forensics (Zainudin et al., 2022).

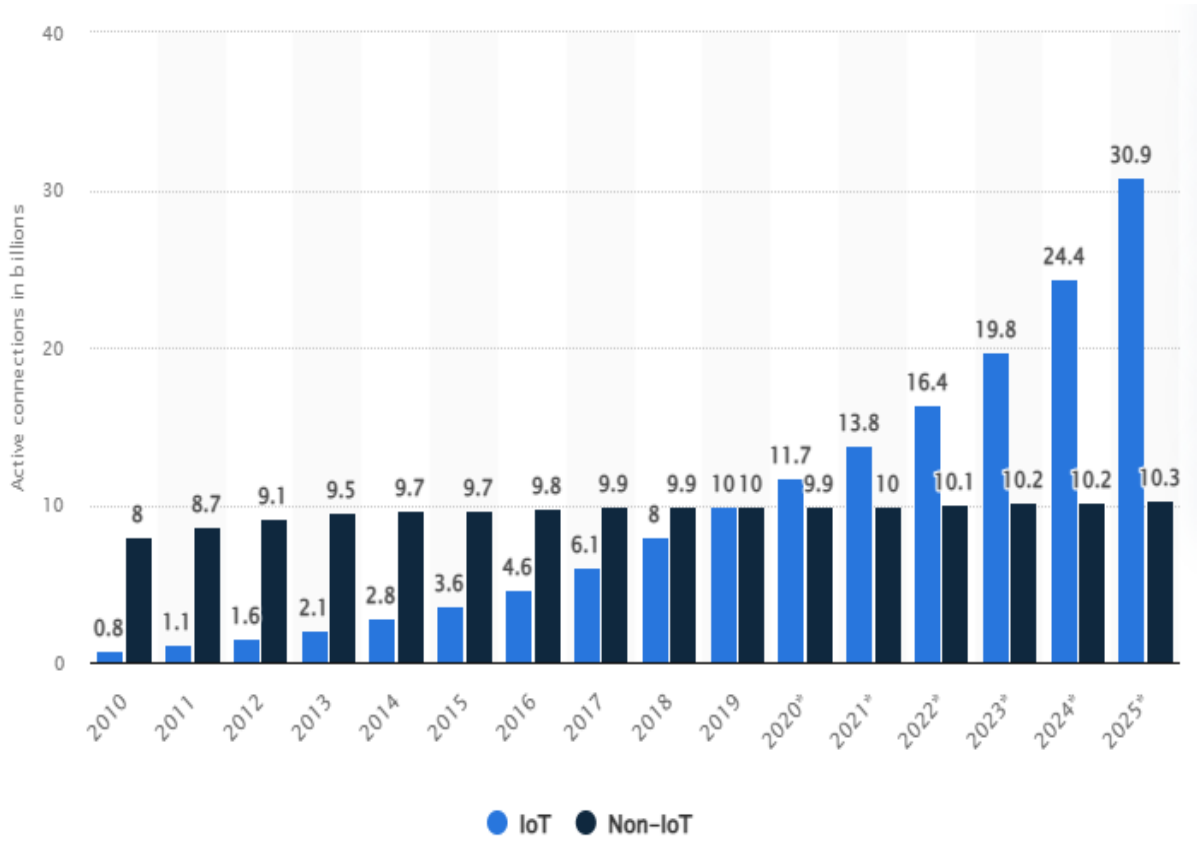

Figure 1: Internet of Things (IoT) and Non-IoT active device connections worldwide from 2010 to 2025 (Vailshery Lionel Sujay, 2022)

Digital forensic investigation involves presenting, documenting, analysing, preserving, and identifying data for use as evidence. In general, digital forensics comprises four steps: identifying the digital assets involved in the digital crime, acquiring digital devices and related assets, analysing data from digital systems related to the crime, and storing information and reporting. Forensic tools are crucial in helping security professionals identify and extract digital traces, ensure the safety of extracted data, and, most importantly, identify cybercriminals. Digital forensics is a powerful tool that conducts post-mortem analysis, collects evidence from various digital media, uses this data to reconstruct potential events, and prepares court-accepted reports (Soltani et al., 2019).

Recent digital forensics trends focus on technologies such as cloud, IoT, and social media forensics, as well as other digital assets (Rondeau et al., 2019). However, IoT forensics stands out as the most challenging area due to the proliferation of IoT devices from multiple manufacturers used in a wide range of applications across most

industries. The complexity and evolving nature of IoT forensics present unique challenges, making it a crucial area of focus for digital forensics professionals (Islam et al., 2019).

IoT devices are widely used and are expanding across a variety of organisations. IoT devices are a target for malicious users due to their vulnerability to cyber-attacks; there has yet to be a widely accepted protocol or standard for IoT (Makura et al., 2021). Vendors are using their proprietary protocols for things-to-things communication. The wide variety of data structures generated by IoT devices makes the examination and analysis phase challenging (Zawoad et al., 2015). The security mechanisms for IoT are evolving; however, devices often do not adhere to best cybersecurity practices and remain vulnerable to attacks and data compromise. Various manufacturers produce IoT devices for specific applications; consequently, standardisation in IoT architectures and data protection is often neglected. As attackers seek vulnerabilities to carry out malicious activities, IoT devices are easy targets for gaining access to IT infrastructure and launching further attacks.

Due to these challenges, organisations using IoT devices for their processes are vulnerable to cyber-attacks (Lezzi et al., 2018). The forensic investigation of these devices for extracting digital evidence has sparked interest in IoT forensics. The IoT devices provide complex and unique challenges for digital forensic analysis (Stoyanova et al., 2020). The challenges in IoT forensics have increased, as forensic investigations must address significant analytical, security, and capacity demands stemming from the volume of data generated by these devices. Data extraction from these devices is problematic because they use different protocols, data formats, and physical interfaces, complicating evidence extraction.

IoT vulnerabilities primarily stem from insecure protocols, misuse of default credentials provided by device manufacturers, and other attack vectors. For example, attackers create and deploy malware that can infect IoT devices, disrupting their operation or rendering them unavailable to authorised users. Furthermore, existing digital forensic tools and methods are ineffective for evaluating IoT devices because extracting data from them is complex (Conti et al., 2018). Therefore, threats such as

malware and other cyberattacks are significant, and the urgency of developing effective IoT forensic methods is essential to overcome the challenges posed by IoT for evidence collection in forensic investigations.

The National Institute of Standards and Technology (NIST) defines digital forensics as "the science of identifying, collecting, analysing and examining digital data evidence". Maintaining the integrity of the information and a strict chain of custody for the data is mandatory (Zawoad et al., 2015). DF is the study of extracting potential digital evidence (PDE) from IoT devices for use in litigation, system hardening, system analysis, and problem-solving. Various types of evidence can be extracted from different IoT devices, making the automatic reconstruction of events very challenging. For example, physical memory images, captured network traffic, log files, the registry, file system metadata, and other system components have different formats. Integrating these large-volume, multi-format data and extracting meaningful information requires considerable effort (Soltani et al., 2019).

Figure 2: The Digital Forensic Flow Process (Zawoad et al., 2015)

Digital Forensic Readiness is the pre-incident plan within the Digital Forensics Investigation lifecycle that addresses the identification, preservation, storage, analysis, and use of digital evidence while minimising forensic investigation costs. In other words, digital forensic readiness aims to manage digital evidence to enable a timely, cost-effective forensic investigation (Mouhtaropoulos et al., 2014).

DFR additionally includes the procedures for identification, reliability, and storage, as well as the systematic, repeatable, and predictable documentation of events, whether ongoing or sporadic, that need investigation. (Ikuesan et al., 2017). However, the complexity of IoT systems and the lack of unified standards impede the digital investigation process and, at times, prevent security agencies and Law Enforcement Agencies (LEAs) from acquiring digital forensic evidence (Kebande et al., 2016).

Digital Forensic Readiness (DFR) in IoT-enabled organisations continues to evolve, and DFR processes are addressed in the ISO/IEC 27043 international standard. This standard emphasises the importance of using standardised processes in readiness activities (ISO, 2015). IoT challenges reinforce the need for organisations to become digital-forensics-ready, particularly when IoT devices are involved in IT operations. There is a need for an effective solution for digital forensics investigations, particularly in IoT environments, to address multiple challenges in a changing threat landscape (Karie et al., 2017).

Given that cyber-attacks cannot be prevented altogether, adequate planning for forensic analysis can strengthen the organisation's digital forensic readiness and reduce the cost of conducting forensic investigations. Further, the organisation can also reduce the impact of cyber-attacks.

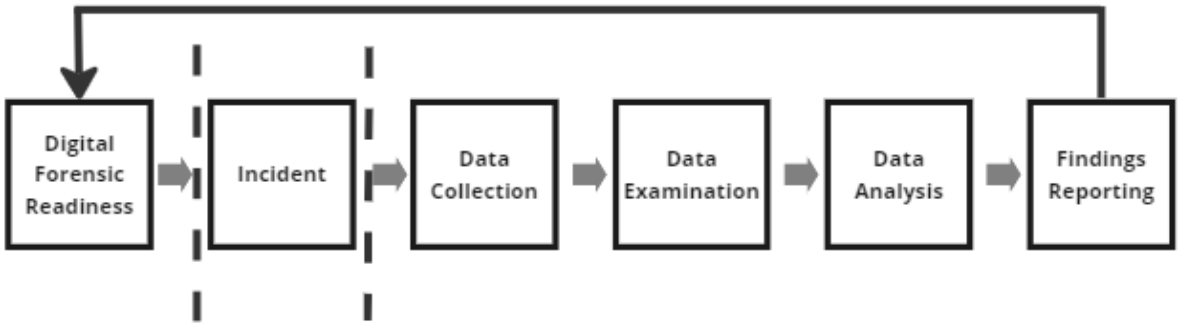

Figure 3: The Digital Forensic Investigation Lifecycle (Mouhtaropoulos, Li and Grobler, 2014)

Despite extensive research on IoT security and digital forensics, a clear gap remains in organisational-level Digital Forensic Readiness for IoT-enabled environments. Existing approaches either focus on post-incident forensics or propose conceptual readiness models that lack standard alignment or practical validation. In particular, limited work integrates ISO/IEC 27043 readiness processes with real-time IoT security monitoring and evidence management. This research addresses this gap by developing and validating a standards-aligned, implementable Digital Forensic Readiness Model designed explicitly for IoT-enabled organisations.

Although Digital Forensic Readiness (DFR), Incident Response (IR), Intrusion Detection (ID), and Security by Design (SbD) are closely related disciplines within

cybersecurity, they serve distinct purposes and operate at different stages of the security lifecycle. A clear distinction between these concepts is important for understanding the contribution of the proposed Digital Forensic Readiness Model. Digital Forensic Readiness focuses on preparing an organisation to efficiently collect, preserve, manage, and utilise digital evidence before a security incident occurs. The primary objective is to maximise the availability and integrity of potential digital evidence while minimising the time, cost, and disruption associated with future investigations. DFR is therefore proactive and evidence-focused.

Incident Response, by contrast, focuses on detecting, containing, eradicating, and recovering from security incidents after they occur. While incident response aims to restore normal business operations and minimise operational impact, Digital Forensic Readiness aims to ensure that relevant evidence is available and preserved in advance to support subsequent investigations.

Intrusion detection focuses on identifying suspicious or malicious activity within a network, system, or device. Intrusion detection systems generate alerts when predefined signatures or anomalous behaviour are detected. However, detection alone does not guarantee that sufficient evidence has been preserved for forensic analysis. DFR goes beyond detection by ensuring that evidential data is collected, stored, and maintained in a legally defensible manner.

Security by Design represents a preventive approach in which security controls are incorporated into systems and applications during their design and development phases. The objective is to reduce vulnerabilities and prevent attacks. While Security by Design aims to minimise security incidents, Digital Forensic Readiness assumes incidents may still occur and focuses on ensuring adequate evidence is available when investigations are necessary.

Therefore, the proposed model does not replace incident response, intrusion detection, or security-by-design practices. Instead, it complements these functions by providing an organisational capability that ensures the continuous generation, preservation, and management of digital evidence to support effective forensic investigation in IoT-enabled environments.

Table 1: Comparison of Digital Forensic Readiness and Related Cybersecurity Functions

Concept	Primary Objective	When Applied	Main Focus	Output
Digital Forensic Readiness	Prepare for future investigations and preserve evidence	Before and during incidents	Evidence collection, preservation, integrity, and traceability	Forensically sound evidence
Incident Response	Contain and recover from security incidents	During and after incidents	Response, containment, eradication, and recovery	Restored business operations
Intrusion Detection	Detect suspicious activities and attacks	During system operation	Monitoring and attack identification	Security alerts and notifications
Security by Design	Prevent vulnerabilities during development	Before system deployment	Secure architecture and secure development practices	Reduced attack surface and stronger security posture

1.1 Study Rationale

The rapid growth of the Internet of Things (IoT) has transformed modern organisations by enabling greater connectivity, automation, and data-driven decision-making across sectors such as healthcare, manufacturing, transportation, and finance. However, this increased connectivity has also expanded the cyber threat landscape, exposing organisations to a growing range of security risks, including malware infections, unauthorised access, data breaches, and distributed denial-of-service attacks. As organisations become increasingly dependent on interconnected digital systems, the need for effective cybersecurity strategies that support both prevention and investigation has become more critical than ever (Rondeau et al., 2019).

Traditional cybersecurity approaches primarily focus on preventing attacks and restoring services after security incidents. While these measures remain essential, they often offer limited support for the systematic collection, preservation, and analysis of digital evidence required for forensic investigations. Consequently, organisations may struggle to identify the root causes of incidents, reconstruct attack timelines, or provide reliable evidence for legal, regulatory, or disciplinary purposes. This

challenge is particularly evident in IoT environments, where evidence may be distributed across numerous heterogeneous devices, platforms, and communication networks.

Digital Forensic Readiness (DFR) offers a proactive approach to addressing these challenges by enabling organisations to prepare for future investigations before incidents occur. Rather than treating digital forensics as a reactive activity performed after a security breach, DFR focuses on establishing policies, processes, technologies, and governance structures that support the continuous generation, preservation, and management of potential digital evidence (Singh Kumar Shanu et al., 2019). Effective forensic readiness can reduce investigation costs, improve response efficiency, strengthen evidential integrity, and enhance organisational resilience against cyber threats.

Despite growing interest in IoT security and digital forensics, research on the effective implementation of forensic readiness in IoT-enabled organisational environments remains limited. Existing studies often focus on technical security controls, post-incident investigations, or conceptual readiness models, with comparatively little attention to practical organisational deployment and validation. Furthermore, many proposed approaches are not aligned with internationally recognised standards such as ISO/IEC 27043, limiting their applicability in real-world forensic investigations.
This research addresses these limitations by developing and evaluating a Digital Forensic Readiness Model tailored to IoT-enabled organisations and aligned with ISO/IEC 27043. The study aims to provide organisations with a structured, practical approach to integrating forensic readiness into their operational environments, thereby improving their ability to identify, collect, preserve, and analyse digital evidence while maintaining readiness for future cyber investigations.

The Internet of Things (IoT) has revolutionised how we live, work, and interact with the world around us. However, this shift increases the risk to critical business infrastructure, such as banks, healthcare, power grids, transportation, multimedia, and telecommunications networks, which have been significant targets of cybercriminals. As a result, cybersecurity is a growing concern for individuals,

organisations, and governments worldwide. The increasing reliance on digital technology and the Internet increases the risk of cyberattacks and data breaches (Radouan et al., 2021). Cybersecurity incidents can lead to a range of consequences, including financial loss, reputational damage, legal and regulatory repercussions, and, in some cases, personal injury. Given the scale of cybersecurity challenges, research is needed to better understand their nature and extent. Cybersecurity research can help identify the types of threats organisations face, the vulnerabilities cybercriminals exploit, and the strategies organisations can use to mitigate those threats. Additionally, it can help organisations better understand the importance of cybersecurity and the need to prioritise cybersecurity measures.

Research findings on cybersecurity inform policy development and decision-making at organisational and governmental levels. The research will provide evidence-based recommendations for developing effective cybersecurity strategies, policies, and practices, thereby improving the overall security and resilience of the digital environment. Additionally, it will help create safer, more resilient digital infrastructures, ultimately protecting individuals, organisations, and governments from the potentially harmful effects of cybercriminals. The study is needed to enable organisations and policymakers to better understand the nature and extent of security threats and to provide evidence-based recommendations for developing effective cybersecurity strategies and policies.

DFR is a proactive approach that organisations can take to ensure they are prepared to respond effectively to potential cyber incidents. In today's digital world, organisations increasingly rely on electronic data to conduct their business and store sensitive information, leaving them vulnerable to cyber threats such as hacking, data breaches, and insider threats. Inadequate preparation for digital forensics can lead to increased downtime, financial losses, reputational damage, and legal and regulatory consequences (Al-Mahrouqi et al., 2015). Organisations can proactively identify potential cyber threats and develop effective mitigation strategies by implementing a readiness model. This includes establishing policies and procedures for collecting and preserving digital evidence, creating an incident response plan, training staff in digital

forensic techniques, and regularly testing and updating the model to ensure its effectiveness. Organisations must increasingly prioritise DFR to reduce the impact of cyber incidents and protect their assets. However, developing and implementing a DFRM can be complex and resource-intensive. Research is needed to provide guidance on best practices for developing and implementing digital forensics readiness across different settings and to evaluate the effectiveness of DFRM.

As DF technology trends evolve, new challenges and IoT-related crimes emerge within organisations. However, little attention has been paid to improving investigation procedures for collecting and analysing evidence from connected devices. To support forensic investigations in such scenarios, a systematic method needs to be implemented from the early stages of inquiries (Salama et al., 2022). This scenario, therefore, calls for the development of new approaches in digital forensics that can effectively support organisations and investigators in addressing the challenges posed by cybercriminals. Many organisations still need to be ready for digital forensics, but the business world's dependence on IT has created a need to build DFR capabilities. Research shows that a carefully considered, planned, and legally contextualised digital forensic readiness strategy can help organisations better manage security incidents while preserving the integrity of evidence collected and keeping investigation costs low (Nik Zulkipli and Wills, 2021).

Before an organisation can successfully deploy digital forensics readiness, several processes must be undertaken, including identifying data sources, defining the digital infrastructure architecture, and identifying hypothetical attack scenarios. Additionally, challenges related to the integrity of digital evidence generation, collection, management, and sharing within an organisation must be addressed. For example, the integrity of the chain of custody (CoC) is critical to the overall success of future digital forensic investigations and the underlying Digital Forensic Readiness Model. Therefore, it is imperative to implement techniques and methods that ensure the integrity of the CoC (Kebande and Ray, 2016). Additionally, all the existing DFR frameworks and models must be standardised to facilitate the adoption of digital forensics readiness processes within organisations.

Cybersecurity challenges in IoT systems are significant and complex, and researchers are continually developing innovative approaches to address them (Al-Masri et al., 2018). As the number of IoT devices grows, maintaining security, privacy, and trust in these systems is critical to ensuring their safe and effective use. Therefore, a study on building digital forensic readiness, grounded in ISO/IEC 27043, must provide organisations with evidence-based guidelines and tools for implementing effective Digital Forensic Readiness Models (ISO, 2015). This study would help organisations better understand the benefits and challenges of digital forensic readiness and provide practical steps to develop and implement such models. Ultimately, this study on digital forensic readiness will help create more resilient and secure digital environments and protect organisations from the potentially devastating consequences of cyber incidents.

The proposed Digital Forensic Readiness Model meets the needs of IoT-enabled organisations, enabling them to identify and collect digital evidence more frequently and to remain ready for investigation when needed. The primary objectives of this study are to optimise vulnerability-based incident response processes and to deploy a Digital Forensic Readiness Model within organisations. The Digital Forensic Readiness Model, and consequently the incident response plan, depend on the organisation's size and must be agreed upon by the stakeholders involved in implementing the plan.

ISO/IEC 27043 is selected as the foundational standard for this study because it provides a comprehensive, structured, and internationally recognised framework for digital forensic investigation and forensic readiness across organisational environments. Unlike other cybersecurity guidelines and incident response frameworks that primarily focus on threat detection, mitigation, or recovery, ISO/IEC 27043 explicitly addresses pre-incident readiness, systematic identification and preservation of evidence, chain of custody, and process integrity, all of which are critical to ensuring that digital evidence remains reliable and legally admissible.

The relevance of ISO/IEC 27043 is particularly significant for IoT-enabled organisations, where evidence sources are highly distributed, heterogeneous, and

dynamically generated across devices, networks, and platforms. Existing IoT security approaches rarely account for these forensic complexities at the organisational level, often treating forensic investigation as a post-incident activity rather than an embedded capability. By grounding this research in ISO/IEC 27043, the study ensures that forensic readiness is treated as a continuous organisational process rather than a reactive technical function.

The increasing complexity of cyber threats within IoT-enabled organisational environments has created a strong operational relationship between Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) platforms, incident response mechanisms, and Digital Forensic Readiness (DFR). Traditionally, intrusion detection and digital forensic investigation have been treated as separate cybersecurity domains. Intrusion detection primarily focuses on identifying malicious activities, generating alerts, and supporting immediate operational response. In contrast, digital forensics focuses on the identification, preservation, analysis, and presentation of digital evidence following a security incident. However, the rapid growth of distributed IoT infrastructures has significantly increased the need to integrate these domains into a unified organisational security strategy.

Modern organisations generate vast volumes of security events, logs, and network traces from interconnected IoT devices, cloud services, endpoints, and communication platforms. Intrusion Detection Systems and SIEM technologies provide real-time monitoring that identifies suspicious behaviour, anomalous network activity, malware execution, unauthorised access attempts, and other Indicators of Compromise (IoCs). Nevertheless, while IDS and SIEM systems are effective for operational threat detection, they are not inherently designed to ensure evidential integrity, forensic preservation, or the management of legally admissible evidence. Consequently, organisations increasingly require Digital Forensic Readiness capabilities to transform operational security data into forensic-ready evidence that supports formal investigations and legal proceedings.

Digital Forensic Readiness extends beyond conventional intrusion detection by

proactively preparing organisations to identify, preserve, collect, and analyse digital evidence before security incidents occur. Unlike traditional reactive forensic investigations that begin after an incident is identified, DFR establishes systematic readiness processes to ensure that forensic evidence is continuously generated, securely preserved, and made available for future investigations. This proactive approach is particularly important in IoT-enabled environments, where evidence sources are highly distributed, heterogeneous, volatile, and continuously generated across multiple devices and network layers.

The relationship between intrusion detection and digital forensic investigation is therefore increasingly interdependent. IDS and SIEM platforms generate operational security intelligence to identify suspicious events. At the same time, Digital Forensic Readiness Models ensure that relevant logs, metadata, network traces, and system artefacts are preserved in ways that support forensic investigation, evidential integrity, and chain-of-custody requirements. In this context, intrusion detection serves as the initial monitoring and alerting mechanism, whereas forensic readiness provides the structured processes required for evidence acquisition, preservation, examination, and investigation.

This integration is particularly significant for IoT-enabled organisations due to the dynamic and decentralised nature of IoT infrastructure. IoT devices continuously generate large volumes of heterogeneous data from sensors, gateways, cloud services, and edge platforms. Security incidents involving IoT systems may therefore produce fragmented evidence spread across multiple locations and formats. Without proactive forensic readiness mechanisms, organisations risk losing critical evidence due to data volatility, storage limitations, inconsistent logging, or inadequate evidence-preservation procedures.

To address these challenges, this research positions Digital Forensic Readiness as a bridging framework linking cybersecurity monitoring and digital forensic investigation. The proposed model integrates Intrusion Detection Systems, SIEM monitoring platforms, incident response processes, and forensic evidence management into a unified operational architecture aligned with ISO/IEC 27043. This

approach enables organisations to move from reactive post-incident investigations to continuous forensic preparedness, supporting real-time evidence generation, automated evidence preservation, and legally defensible investigations. The conceptual relationship underpinning this research is illustrated through the integration of four interrelated organisational functions:

1. Intrusion Detection and Threat Monitoring
2. Security Event Collection and Correlation
3. Digital Evidence Preservation and Chain of Custody
4. Digital Forensic Investigation and Readiness Management

Within the proposed model, IDS and SIEM platforms such as Wazuh serve as the primary monitoring infrastructure, detecting malicious activity and collecting security telemetry. Digital Forensic Readiness processes then operationalise forensic evidence handling through secure logging, metadata preservation, integrity validation, evidence correlation, and support for incident investigation. This integration establishes a continuous forensic workflow that strengthens organisational cyber resilience, reduces investigation costs, and improves forensic efficiency within complex IoT ecosystems.

1.2 Importance of the Study and Originality

In today's digital world, studying cybersecurity is essential to protect individuals, organisations, and governments from the potentially devastating consequences of cyber incidents. This research will help identify threats, vulnerabilities, and risks, and develop effective mitigation strategies. In addition, the study will contribute to the development of a safer, more resilient global cybersecurity model for the benefit of all. Digital forensics readiness is essential for organisations to prepare for and proactively respond to cybersecurity incidents (Karie & Valli, 2021). It improves incident response capabilities, ensures legal and regulatory compliance, protects organisational assets, and builds stakeholder confidence. Implementing a DFRM can help organisations reduce the impact of a cybersecurity incident on their operations and reputation, and protect themselves and their stakeholders from potentially damaging consequences (Karie & Karume, 2017).

One of the main benefits of DFR is that it reduces the cost of digital investigation. For example, imagine an organisation with around 100 clouds running OpenStack without deploying DFR. In the event of a cyberattack, the digital forensic investigator must examine each of the 100 clouds and their images individually. This will increase the cost and time of the forensic investigation. However, once an organisation deploys DFR, the implementation becomes seamless. The DFI can isolate the specific cloud instance where the security breach occurred and focus on that instance alone (Makura et al., 2021).

Security issues in IoT devices are significant, given the enormous amount of data they generate. Hence, the challenges associated with IoT devices must be addressed by improving network and forensic capabilities in a state of readiness to keep pace with IoT device usage in organisations (Radouan Ait Mouha, 2021). For instance, network security must be strengthened, and forensic artefact acquisition processes must be established in organisations. Therefore, organisations need digital forensic readiness capabilities to ensure data security and support forensic investigations during data breaches. Although research on IoT is on the rise, further work is needed on architectures that incorporate DFR in IoT-enabled organisations. Some existing literature explicitly mentions the DFR process, while others treat it implicitly. However, most have shown the necessity of a DFR process in emerging IoT environments (Kebande, Karie and Venter, 2018). The literature review identified vulnerabilities and security challenges in IoT and the need to address them.

Zawoad and Hasan, (2015) proposed a forensic-aware IoT (FAIoT) to support forensic investigations in IoT environments. This model is developed to secure evidence, provenance, and preservation. In addition, it uses a read-only API to access evidence. However, this is a technological solution and does not provide sufficient input for digital forensic readiness in IoT. The framework does not support the ISO/IEC 27043 standard or address the organisational view of DFR.

Hossain et al., (2018) present a forensic investigation framework (FIF) for IoT that uses a public digital ledger. The framework collects data from IoT, cloud, and user devices and securely stores it on a blockchain network for public access. By storing data on a

public digital ledger, the framework ensures integrity, confidentiality, anonymity, and non-repudiation. A case study demonstrates effectiveness, and a prototype demonstrates performance. Although the framework addresses organisational readiness and security processes, it is not based on an international standard or any other approved framework.

Makura et al., (2021) proposed a DFR framework based on the ISO/IEC27043 standard. This framework was presented in a cloud environment for security monitoring. However, the need for digital readiness in IoT requires more thorough attention. These include the pre-incident planning analysis of data representing the PDE process, the planning of the incident detection process, and the definition of the system architecture process, which were not considered in the Study.

Sadineni et al., (2021) propose the Ready-IoT readiness model for monitoring and logging network traffic. The model collects provenance from network traffic, which comprises network parameters and traffic. The model provides provenance graphs; however, there is no evidence that it can detect network attacks. Additionally, digital forensic readiness using standard approaches, which is essential in organisations, needs to be addressed.

Since the IoT-FR is in its conceptual phase, research has focused on conceptual frameworks and theoretical solutions for forensic IoT, with little emphasis on practical Digital Forensic Readiness (DFR) scenarios in organisations. Although the highlighted research indicated that it contributed significantly to DFR in IoT, only some studies have considered it from an organisational-level perspective. Also, most of the research presented is not based on an approved standard, such as the ISO/IEC 27043. The proposed model is designed to be compatible with ISO/IEC 27043.

It was noted that there is a need for readiness processes in IoT frameworks and IoT security mechanisms to support forensic processes in organisations. Unlike existing DFRFs, such as those focused on smart homes, the proposed model accounts for organisational complexities and policy developments. Also, none of the proposed DFR frameworks/models has been verified in real-world organisations (Kebande et al.,

2020). However, the proposed model would be implemented in a real-world organisation environment to evaluate its real-world effectiveness.

Table 2: Digital Forensic Readiness frameworks/models comparisons

Reference	Research Area	Readiness Processes	ISO Standardised	Forensic Processes Targeting Organisations
Ngobeni et al., (2010)	A Forensic Readiness Model for Wireless Networks	✓	×	×
Zawoad et al., (2015)	FIF-IoT: A forensic investigation framework for IoT using a public digital ledger	✓	×	×
Kebande et al., (2016)	A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)	✓	✓	×
Meffert et al., (2017)	Forensic state acquisition from internet of things (FSAIoT):	✓	×	×
Hossain et al., (2018)	FAIoT: Towards Building a Forensic Aware Ecosystem for IoT	✓	×	✓
Hossain et al., (2018)	Probe-IoT: A public digital ledger based forensic investigation framework for IoT	✓	×	×
Chi et al., (2019)	A Framework for IoT Data Acquisition and Forensics Analysis	✓	×	×
Makura et al., (2021)	Digital forensic readiness in operational cloud leveraging ISO / IEC 27043 guidelines on security monitoring	✓	✓	×
Sadineni et al., (2021)	Ready-IoT: A Novel Forensic Readiness Model for Internet of Things	✓	×	×

To meet this research's IoT forensic readiness model objectives and overcome the gaps whereby none of the frameworks/models fully support the three elements highlighted in Table 2;

a) Readiness Process.
b) ISO Standardised - ISO/IEC27043 standard.
c) Forensic Processes Targeting Organisations.

The originality of this research lies in the development and practical validation of an ISO/IEC 27043–aligned Digital Forensic Readiness Model specifically designed for

IoT-enabled organisations. While prior studies have addressed the IoT forensics conceptually or proposed readiness frameworks without standard alignment, this work makes the following original contributions:

1. The integration of organisational, technical, and security readiness processes into a unified, standard-compliant DFR model for IoT environments.

2. The practical implementation and validation of the model using real-world security monitoring tools and controlled attack scenarios.

3. The incorporation of machine learning-based data analysis to support forensic evidence prioritisation and readiness evaluation.

The research proposes a model for Digital Forensic Readiness (DFR) in IoT-enabled organisations, targeting the three elements and critical components of the IoT-FR framework (Organisational Readiness, IoT Security Layer Processes, and IoT Security Layer Processes) shown in Figure 16, and demonstrates its effectiveness in a real-time scenario. The research methodology and design section outlines how this model will be implemented. The study will establish an effective DFR investigation technique to address cybersecurity challenges in IoT-enabled organisations and strengthen this area of forensic investigation and knowledge sharing. These contributions collectively advance both the theoretical understanding and practical implementation of digital forensic readiness in IoT-enabled organisational contexts.

1.3 Research Aim and Objectives

This research aims to design, implement, and evaluate a Digital Forensic Readiness (DFR) model for IoT-enabled organisations, aligned with ISO/IEC 27043, to enable proactive, real-time collection, preservation, and analysis of digital evidence. The study seeks to strengthen organisational preparedness for cyber incidents by integrating forensic readiness processes with IoT security monitoring and validation through practical experimentation, thereby improving evidence integrity, investigative efficiency, and organisational cyber resilience.

1.3.1 Aims of the Study

1) To critically analyse existing digital forensic readiness frameworks and identify limitations in supporting IoT-enabled organisations.

2) To design an ISO/IEC 27043–aligned Digital Forensic Readiness Model addressing organisational, technical, and security requirements in IoT environments.

3) To implement the proposed model within a controlled organisational testbed using real-world security monitoring tools.

4) To evaluate the effectiveness of the proposed model using experimental attack scenarios and forensic performance metrics.

5) To assess the practical challenges, scalability, and limitations of deploying the model in real-world organisational settings.

1.3.2 Expected Outcomes

This study aims to demonstrate that a Digital Forensic Readiness Model aligned with ISO/IEC 27043 can be effectively designed, implemented, and evaluated within IoT-enabled organisational environments. Through practical deployment and experimental validation, the research is expected to show improved organisational preparedness for cyber incidents by enabling proactive evidence identification, real-time evidence generation, secure preservation, and robust chain-of-custody management. The outcomes also include a quantitative assessment of forensic readiness performance, including investigation efficiency, evidence integrity, and response effectiveness, under controlled attack scenarios.

Additionally, the study aims to demonstrate how machine learning–based data analysis can support forensic evidence prioritisation and readiness assessment within IoT contexts, while recognising operational and legal constraints. Collectively, these results are intended to provide empirical evidence of the feasibility, effectiveness, and practical applicability of digital forensic readiness in IoT-enabled organisations, while highlighting key implementation challenges and scalability considerations for real-world adoption.

1.4 Identifying the Research Gap

Despite extensive research on cybersecurity mechanisms, IoT security architectures, and digital forensic investigation techniques, existing studies largely address these areas in isolation. The literature provides strong coverage of post-incident forensic

analysis and attack detection mechanisms; however, comparatively little attention has been given to proactive Digital Forensic Readiness (DFR) in IoT-enabled organisational environments.

In particular, current research lacks an integrated approach that aligns organisational governance, technical evidence generation, and security monitoring within a standard-compliant forensic readiness framework. Although several conceptual IoT forensic models and readiness frameworks have been proposed, many remain theoretical, lack practical validation, or do not fully align with internationally recognised standards such as ISO/IEC 27043. Furthermore, organisational dimensions—including governance structures, policy integration, defined roles, and chain-of-custody management—are often underrepresented, despite their critical importance to legally defensible investigations. Additionally, limited work has examined real-time forensic readiness in IoT environments, where evidence is distributed, dynamic, and potentially volatile. The absence of empirically validated models to support proactive evidence generation and preservation represents a significant gap in both academic research and organisational practice.

These limitations are examined in detail in Section 2.5 (The Gap in the Literature). Addressing this gap, the present research develops and validates an ISO/IEC 27043–aligned Digital Forensic Readiness Model tailored for IoT-enabled organisations, integrating organisational, technical, and security processes to support real-time, standard-compliant forensic readiness.

To address the identified research gap systematically and with methodological rigour, this study progresses from conceptual analysis to empirical validation across successive chapters. Chapter 3 sets out the methodological framework underpinning the research by defining the research paradigm, adopting a quantitative approach, and justifying the choice of research instruments. This ensures analytical consistency and provides a solid foundation for evaluating digital forensic readiness in IoT-enabled organisational contexts.

Chapter 4 operationalises the research objectives by presenting the proposed Digital Forensic Readiness (DFR) Model for IoT environments. It outlines the research design, experimental system configuration, and the practical implementation of security monitoring platforms, including Wazuh and Splunk. By translating theoretical concepts into a deployable architecture, this chapter directly addresses the lack of practically validated, standards-aligned forensic readiness frameworks identified in the literature.

Chapter 5 extends this work through carefully controlled experiments, focusing on detecting brute-force attacks and conducting forensic investigations. The chapter presents a method for proactively generating, collecting, and preserving evidence from real-world log data, thereby addressing the limited empirical research on real-time forensic readiness in distributed and dynamic IoT environments.

Building on the experimental results, Chapter 6 presents a detailed data analysis using machine learning models for cyber-attack detection. This chapter evaluates various models and their performance, addresses the underexplored integration of intelligent analytics into digital forensic readiness frameworks, and enhances the evidential value of the proposed approach.

Chapter 7 critically discusses the findings and introduces the Adaptive Proactive Readiness Model (APRM). It assesses the results, evaluates performance and readiness, and compares APRM with existing Digital Forensic Readiness Models. The chapter also examines data flow and security architecture, highlighting the lack of comparative, evaluation-driven studies that integrate organisational readiness, technical performance, and forensic capability within a unified framework.

Finally, Chapter 8 summarises the research findings and explains the study's contribution to knowledge. Sections 8.3 and 8.4 discuss the research's implications and limitations, while Section 8.5 offers recommendations for future work. Collectively, these chapters demonstrate how the study addresses the identified gap by providing an empirically validated, ISO/IEC 27043–aligned Digital Forensic Readiness Model designed for IoT-enabled organisational environments.

1.5 Related Publications

This section presents material in Chapters 3 to 7 that has been published in peer-reviewed conference proceedings and Journals.

- O Kuku, A Chrysikos, S Salekzamankhani, "Digital Forensic Readiness in IoT-Enabled Organisations and Forensic Investigation Analysis in Real-Time" London Met Student and Staff Research Conference, 'Past-Present-Future: Research at London Met' 3rd July 2024.

- O Kuku, A Chrysikos, S Salekzamankhani, "Digital Forensic Readiness in IoT-Enabled Organisations: Forensic Investigation Analysis in Real-Time" 5th International Conference on Data Analytics & Management (ICDAM-2024)14th & 15th June 2024. https://doi.org/10.1007/978-981-96-3355-5_41

- Kuku, O., Chrysikos, A., Salekzamankhani, S. (2025). Enhancing Forensic Readiness in IoT-Enabled Organisations: A Real-Time Model. In: Swaroop, A., Virdee, B., Correia, S.D., Valicek, J. (eds) Data Processing and Networking. ICDPN 2024. Lecture Notes in Networks and Systems, vol 1288. Springer, Singapore. https://doi.org/10.1007/978-981-96-3102-5_16

- Oyeyemi Kuku, Alexandros Chrysikos, Shahram Salekzamankhani (2024) "Digital Forensic Readiness in IoT-Enabled Organisations and Forensic Investigation Analysis in Real-Time", International Journal of Electrical, Electronics and Data Communication (IJEEDC), pp. 21-28, Volume-12, Issue-9. https://iraj.in/journal/IJEEDC//paper_detail.php?paper_id=21277&nameDigital_Forensic_Readiness_in_Iot-Enabled_Organisations_and_Forensic_Investigation_Analysis_in_Real-Time;

- Kuku, O., Chrysikos, A. & Salekzamankhani, S., "Preparing IoT-enabled organisations for digital forensics: model for readiness and resilience." Int. J. Inf. Secur. 24, 170 (2025). https://doi.org/10.1007/s10207-025-01079-z

- Kuku, O., Chrysikos, A. & Salekzamankhani, S., "Real-Time Forensic Analysis in Internet of Things Environments: Bridging Readiness and Investigation for

Cyber Resilience" The BOHR International Journal of Internet of Things, Artificial Intelligence and Machine Learning (BIJIAM, 2025). https://doi.org/10.54646/bijiam.2025.30

- Kuku, O., Chrysikos, A. & Salekzamankhani, S., "Proactive Forensics: Building Digital Forensic Readiness in IoT-Enabled Organisations for Real-Time Incident Response." International Journal of Information Security. Preprint - https://doi.org/10.21203/rs.3.rs-7959169/v1

1.6 Chapter Summary

IoT has become part of organisational infrastructure, changing various fields, including medicine, production, and municipal services, through increased connectivity. Nonetheless, it is accompanied by new threats, such as unauthorised access, data breaches, and compromised devices, which can compromise entire data centre networks. As a result of these emerging risks, Digital Forensic Readiness (DFR) is mandatory for organisations to identify, preserve, and examine evidence at computer crime scenes before, during, and after cyber threats, facilitating rapid responses while protecting sensitive information.

The diverse and heterogeneous nature of IoT networks and the devices they comprise, along with the varying protocols they employ, which differ in their security levels, makes forensic readiness all the more critical. This chapter raises concerns about DFR in IoT environments. It makes clear that organisations today need a practical, concerted DFR approach aligned with the best practices outlined in ISO/IEC 27043. First, it highlights the lack of IoT forensic preparedness within current frameworks and theories, laying the foundation for a model to address these issues and strengthen organisational IT security and compliance through forensic-based approaches to threat management.

2.0 Literature Review

2.1 Introduction

In today's world, personal computers are widespread and essential across commercial and domestic settings. The digital age is expanding rapidly, as an ever-increasing number of individuals enter the digital world and reap its benefits. Nonetheless, not every internet user adheres to legal and standard practices when using a computer. Negative computing, or the use of computers and the internet for illegal or prohibited purposes, has become increasingly common, and inappropriate computer use encompasses many subdomains to avoid. The field of digital forensics plays a significant role in locating and investigating these subdomains, thereby deterring cyberattacks.

In today's digital age, cybersecurity is a significant concern for individuals, businesses, and governments. The number of threats is rising daily, and attacks are increasing in both frequency and complexity. Not only is the number of potential attackers, along with the size of networks, growing, but the tools available to potential attackers are also becoming more sophisticated, efficient, and practical (Abomhara and Køien, 2015). As technology advances and becomes more sophisticated, the threat posed by cybercriminals also increases. Cybersecurity threats include viruses, malware, phishing, and ransomware (Singh, Ikuesan and Venter, 2019). Viruses are malicious software designed to infect a computer and damage files and the system. Malware is a broader term that includes viruses and other types of malicious software, such as Trojans and spyware (Jang-Jaccard and Nepal, 2014). Phishing is a form of social engineering in which cybercriminals deceive individuals into disclosing sensitive information, such as passwords or credit card numbers. Finally, ransomware is malicious software that encrypts files on your computer and demands payment in exchange for a decryption key (Imperva, 2022).

The potential impact of cybersecurity threats can be significant, including financial losses and reputational damage. Businesses that experience a cyber-attack may lose valuable data and face costly downtime as they work to restore their systems (Ghelani, 2022). They may also face legal liability if they fail to protect customer data adequately. Governments may face similar challenges, as cyber-attacks can disrupt critical

infrastructure and compromise national security. Cyber threats are a significant concern in today's digital age. However, organisations can take specific steps to protect themselves, such as implementing robust security protocols, regularly training employees, and backing up data. Furthermore, as technology advances, staying alert and adapting to emerging threats is essential (Al-Mahrouqi, Abdalla and Kechadi, 2015).

Existing literature highlights the availability of digital traces in IoT devices, thus enabling the possibility of clues to investigate the type of offence (Servida et al., 2019). IoT security considerations enable trace extraction; however, attackers can still compromise a device. Technology developments have fostered the shift to the digital domain. Due to this shift, there is an increase in cybercrimes, threats, and attacks, leading to the loss of sensitive data and compromise (Alghamdi, 2020). Digital forensic investigations help trace the source of an attack using digital methods, and the resulting digital traces are used to identify cybercriminals, supporting further investigations. The threats to digital forensics are specific, as the challenges typically arise from operational, technical, or personnel-related compromises. In this situation, IoT applications in homes and businesses create additional challenges for tracing digital evidence from IoT devices and networks. However, challenges in IoT forensics are compounded by the use of diverse mechanisms, insecure protocols, and data formats. These must be addressed through the standardisation of IoT device manufacturers.

Digital Forensics Readiness (DFR) refers to preparing a digital forensics strategy (i.e., the evidence required) prior to an incident to facilitate efficient and effective investigation. The purpose of DFR is to reduce the effort needed to investigate while maintaining the integrity of the collected digital evidence. The decrease in effort includes reductions in incident response time and cost. This is because a “forensically ready” organisation can respond to an attack rapidly and efficiently. In general, reducing the time involved in incident response minimises the cost of the investigation (Ngobeni et al., 2010).

2.2 Cyber Security Processes

Cybersecurity monitoring technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM) platforms play a significant role in modern organisational security operations. These technologies support real-time monitoring, attack detection, event correlation, and incident response. However, while such systems are highly effective for operational security monitoring, they are not inherently designed to meet digital forensic requirements such as evidential integrity, forensic preservation, metadata reliability, and chain-of-custody management. As a result, Digital Forensic Readiness has emerged as an important complementary discipline that bridges operational cybersecurity monitoring and formal forensic investigation processes. In organisational IoT environments, this integration is increasingly important because distributed IoT infrastructures generate substantial volumes of dynamic and heterogeneous evidence that require continuous monitoring and preservation.

According to Alghamdi (2021) cybersecurity professionals are increasingly turning to digital forensics methodologies and tools to gather and analyse digital evidence and investigate incidents. A survey by India Times in early 2019 stated that "*58% of data breach victims are the persons or organisations who have a small type of business at very low or medium level*". In addition, with the use of mobile devices, tablets, laptops, and other electronic devices continuing to rise, it has become easier for cybercriminals to carry out malicious attacks.

Sharma et al., (2019) said that there's no denying the power of social networks in today's society, but as these networks have grown, so too have cybercrimes, which in turn have fuelled the development of novel forms of attack that could compromise even the most well-protected infrastructures. Cybersecurity experts, academic institutions, and law enforcement agencies use digital forensics to investigate cybercrime. To collect digital evidence, specialists in this field use a scientific approach to digital devices such as flash drives, floppy discs, memory cards, phones, and RAM. Methods such as locating, verifying, analysing, and documenting evidence fall under this category. But as digital forensics technologies advance, so do anti-forensics programs, which hackers use to either delay the detection of digital evidence or wipe

it outright. Even though digital forensics is meant to protect user privacy, new waves of crime have arisen with the introduction of ubiquitous internet access, the Internet of Things, and cloud computing; it is predicted that digital forensics will confront unprecedented hurdles as cyber threats and malware grow more advanced and armed with highly sophisticated and effective anti-forensics tactics. Therefore, it is crucial to study such challenges while also investigating the latest trends in digital forensics.

2.2.1 IT Security Risk Assessments

Assessing the risks to an organisation's information systems is essential in today's interconnected digital ecosystem, as it enables the identification, evaluation, and implementation of solutions. IT security risk assessments play a vital role in understanding a company's vulnerabilities and the potential consequences of a security breach. Systematic risk assessment enables businesses to allocate resources more effectively, develop more precise security measures, and prepare for and respond to incidents. Risk assessments are proactive; thus, they help prevent costly security incidents and maintain stakeholder confidence.

The study by Nurse et al., (2017) examines the growing security threats to IoT devices and recommends using risk assessment tools to enhance the safety of these networked systems. The authors stress the critical need to assess the security threats posed by the exponential growth of IoT devices and the potential consequences of security breaches in these complex IoT ecosystems. They highlight potential risks associated with cloud services, mobile applications, operating systems, and other components of the device ecosystem. The study emphasises the importance of risk assessment as an essential step for identifying and addressing security flaws in IoT systems.

The authors stress that the dynamic and diverse nature of IoT environments may not align immediately with standard security procedures. Consequently, they advocate risk assessment techniques as a systematic approach to ranking potential risks. The authors propose a unique risk assessment approach tailored to the needs of IoT systems. Within this framework, assets, threats, vulnerabilities, and the possible repercussions of security breaches are systematically catalogued. Unauthorised access, data manipulation, and denial-of-service attacks are among the vulnerabilities

the authors further explore as attack vectors within IoT systems. They then outline potential countermeasures, such as promoting intrusion detection systems, authentication procedures, and encryption in IoT infrastructure development. By emphasising the importance of risk assessment in addressing the complex security challenges inherent to IoT systems, Nurse, Creese, and De Roure make a significant contribution to the field of IoT security. Experts, academics, and cybersecurity practitioners concerned with protecting IoT ecosystems may find this paper essential.

Munodawafa and Awad (2018) highlight the significance of assessing security risks in hybrid data centres. This research focuses on the unique challenges and delays in modern data centres for delay-sensitive applications. Hybrid data centres have become an essential part of modern IT infrastructure due to rapid technological changes. The authors acknowledge the importance of these hybrid environments in supporting applications, particularly those that cannot tolerate even short delays. This paper examines the security risk assessment approaches required to ensure the safe and continuous operation of time-sensitive applications in such a setting. Case studies are used to ground the authors' findings in real-world contexts. To better understand how hybrid data centres might affect the performance and security of delay-sensitive applications, they analyse the security risk assessment process in this context. The case study details the difficulties encountered, the evaluation criteria, and the methods used to balance security and application performance. The work of Munodawafa and Awad has significant ramifications for the study and practice of cybersecurity. It highlights the need for a holistic security risk assessment approach, particularly in hybrid data centre settings, including for delay-sensitive applications. This article provides insights into the complexities of safeguarding hybrid data centre infrastructures, making it a valuable resource for experts, researchers, and practitioners in information security.

Zio's (2018) article focuses on the history and future of risk assessment, particularly in the context of reliability engineering and system safety. Future risk assessment procedures will likely be shaped by the author's examination of revolutionary trends, approaches, and problems. As technology evolves and current systems become more

sophisticated, the limits of previous risk assessment methods have become apparent. Zio responds to this changing landscape by emphasising the need to adopt risk assessment methods that are flexible, all-encompassing, and open to considering a wide range of variables. The research concludes that the future of risk assessment will depend heavily on integrating diverse fields of study and datasets. Zio argues that better risk forecasts may be made using data analytics, machine learning, and information fusion. The author contends that risk assessments may be more comprehensive and nuanced by incorporating ideas from many disciplines. Zio also explores the concept of dynamic risk assessment, which recognises that hazards may change over time due to various factors. This calls for the continuous integration of real-time data and systems to monitor risk assessment procedures. This study investigates how sophisticated monitoring tools, sensors, and predictive analytics might provide continuous risk assessment and flexible decision-making. The author also discusses risk assessment based on a focus on resilience. Zio suggests that, in the future, risk assessments should prioritise making systems more resilient to withstand interruptions, in addition to detecting vulnerabilities and threats. This new emphasis on resilience is consistent with the principles of proactive risk management and the prevention of domino effects.

The paper by Lyu et al., (2019) explores the complex relationship between safety and security in the context of cyber-physical systems (CPS). The authors investigate the challenges and approaches to risk assessment that arise from integrating digital and physical elements in such systems. The study begins by recognising the historical development of technology and its integration with physical systems, which led to the birth of CPS. While CPS have many advantages, as Lyu, Ding, and Yang pointed out, merging the digital and physical worlds also raises complex safety and security issues that must be managed. The writers emphasise the need for safety and security when working together. The authors emphasise the need for a holistic risk assessment method that accounts for potential hazards to personnel and property. In addition, the research outlines a systematic risk assessment approach tailored to CPS settings. This paradigm covers the phases of threat, vulnerability, consequence, and risk assessment. The authors explain in detail how each step helps to provide a fuller picture of CPS

risk. Lyu, Ding, and Yang also discuss modelling and simulation, as they are relevant to CPS risk assessment. They argue that the reliability of risk assessments can be improved through scenario modelling. Practitioners may examine the ripple effects of various hazards and develop appropriate countermeasures by conducting simulations.

Ganin et al., (2020) provide a multicriteria decision-making framework for the holistic analysis and management of cybersecurity risks. The authors propose a methodical and organised approach to address the complex nature of cybersecurity concerns. They highlight the need for a thorough method for assessing cybersecurity risks that accounts for the wide range of factors that contribute to a given risk. To evaluate and rank cybersecurity threats, this study presents a unique multicriteria decision framework that uses quantitative and qualitative data. The authors underline the need to assess risks across several dimensions, including technological, financial, operational, and reputational factors. This method is consistent with the broader aims of efficient risk management and recognises the complexity of cybersecurity threats. Identifying, evaluating, and controlling risks are components of the framework. Ganin et al. discuss in detail the methods and instruments used to aid decision-making. They emphasise the need for professional judgement and the combination of different data sources to build a complete picture of threats. Finally, the work by Ganin et al. represents a significant step forward in managing cybersecurity risks. The authors provide a helpful resource for practitioners, academics, and policymakers interested in cybersecurity risk reduction, establishing a thorough multicriteria decision-making framework and offering practical insights through a case study.

2.2.2 Cybersecurity Policies

Cybersecurity policies play a critical role in establishing a framework to protect digital assets, sensitive information, and critical infrastructure against the growing threat of cyberattacks. Cybersecurity policies are essential for organisations to develop a structured approach to safeguarding their digital assets and maintaining stakeholder trust. These policies define guidelines, procedures, and best practices for preventing, detecting, and responding to cyber threats. Well-designed cybersecurity policies can

help organisations mitigate risks, comply with regulations, and establish a culture of security awareness.

Štitilis et al., (2017) compare the European Union (EU) and NATO's cybersecurity policies with those of their member states. This article examines how these multinational organisations and their member nations differ in their approaches to cybersecurity threats. They examine the underlying motivations, concepts, and building blocks of these plans, emphasising their shared aims of strengthening cyber resilience, enhancing international collaboration, and ensuring a safe and accessible online environment. The report also discusses the unique cybersecurity challenges the EU and NATO face, including the ongoing evolution of threats and the need for closer cooperation among member nations. The writers also highlight how countries have addressed national cybersecurity challenges. They investigate discrepancies between national plans and international frameworks in terms of emphasis, priorities, and degree of integration. Finally, the study thoroughly compares the cybersecurity approaches used by the European Union, NATO, and their respective member states. The authors highlight worldwide and regional initiatives to improve cybersecurity coordination by discussing alignment, differences, challenges, and opportunities for cooperation.

Lilli, (2020) explores the cybersecurity policy measures and methods implemented under Obama's presidency in the United States. This paper examines the Obama administration's strategy for addressing the complex, ever-changing cyber threats and challenges confronting the United States today. Lilli emphasises the need for a unified, comprehensive approach to cybersecurity by highlighting how digital technologies disrupt traditionally stable industries. Lilli analyses the steps taken by the Obama administration in cybersecurity policy. The author outlines the Obama administration's cybersecurity strategy, including its central goals, guiding principles, and critical components. The paper's study of the Obama administration's executive actions, policies, and plans to bolster cybersecurity is crucial. The "Cybersecurity National Action Plan" and the "Framework for Improving Critical Infrastructure Cybersecurity" are two programs that Lilli examines in detail to determine their

relevance. These initiatives are intended to strengthen the nation's cyber resilience by increasing public-private sector collaboration, enhancing incident response capabilities, and protecting against cyberattacks. The report also explores the ramifications of President Obama's cybersecurity policy for future administrations and the ever-changing nature of cyber threats. Lilli stresses the need for consistency, flexibility, and a preventive cybersecurity approach in today's interconnected digital environment. Ultimately, Lilli's article comprehensively summarises President Obama's cybersecurity policy aims and tactics. The author sheds light on how the United States responded to the evolving cyber landscape under President Obama by analysing the administration's key goals, initiatives, and obstacles.

Dunn Cavelty and Egloff, (2019) examine the many facets of the state's involvement in cybersecurity against the backdrop of ever-evolving digital threats and difficulties. The authors aim to clarify the state's role in maintaining cybersecurity and to address related concerns about surveillance, privacy, and international collaboration. Cybersecurity receives priority in this study, with the authors noting the increasing urgency of the topic and highlighting the severe consequences that cyber threats pose to national security, economic stability, and personal privacy. The writers explore the many facets of governmental involvement in cybersecurity. The roles of the state as a guardian of national interests, a producer of public goods, and a facilitator of new ideas are all critically examined. The study emphasises the need for the state to strike a balance between these tasks, particularly in cybersecurity. The paper's survey of the conflicts and challenges stemming from the state's cybersecurity activities is essential. The authors discuss the difficulties nations face in safeguarding vital infrastructure and personal data while upholding individual privacy and democratic norms. The writers stress the need to balance the state's involvement in cybersecurity with the rights and liberties of its inhabitants. The study also discusses the worldwide politics of cybersecurity. Finally, the research examines the complex politics of cybersecurity and the evolving role of the state in combating cyber threats. The authors provide helpful insights into the complexity of designing effective cybersecurity laws that align with democratic principles and the ever-changing nature of cyberspace, while balancing security, privacy, innovation, and international collaboration.

Sabillon et al., (2017) provide an approach for conducting cybersecurity audits that they hope will lead to greater organisational confidence in this area. To assess and improve the efficacy of cybersecurity policies and procedures, the authors suggest the Cybersecurity Audit Model (CSAM). The article begins by acknowledging the growing importance of cybersecurity in the digital age, noting the prevalence and complexity of cyberattacks that can compromise sensitive information, disrupt business operations, and tarnish an organisation's reputation. The article introduces the Cybersecurity Audit Model (CSAM), a comprehensive framework for evaluating an organisation's security activities. Organisations may use this methodology to assess their cybersecurity preparedness, identify weaknesses, and set priorities for improvement. The Cybersecurity Audit Model is a significant contribution to cybersecurity assurance made by Sabillon, Serra-Ruiz, Cavaller, and Cano (CSAM). Organisations looking to strengthen their cybersecurity posture amid a growing number of threats will find the authors' systematic approach to measuring cybersecurity maturity and advocating change invaluable.

Mishra et al., (2022) conducted an in-depth analysis and discussion of existing customer service policies to manage customer data better and fulfil consumer needs. Businesses of all stripes, as well as governments, must make cybersecurity a top priority. Many companies invest heavily in cybersecurity to protect their digital assets, data, and communications infrastructure. Establishing a library of security rules for a business enables the uniform application of security controls, a key component of cyber defence. This research compares and examines the most essential and widely utilised cybersecurity policies across businesses to provide comprehensive, actionable guidance for other companies. In this extensive analysis, researchers identified and examined numerous noteworthy, prevalent security policies.

Research across five industries—healthcare, banking, education, aviation, and e-commerce—identified 10 commonalities in their cybersecurity policies. They wanted to establish reliable systems across all sectors and investigate the sector-wide security rules and regulations. Additionally, the study's results show that the significance of cybersecurity needs varies across different businesses. Information under control and

an organisation's security needs guide the selection and application of cybersecurity policies.

Teixeira and Tavares-Lehmann (2022) Lehmann's essay examines the EU's policies and national objectives, considering the opportunities and threats posed by Industry 4.0. The authors analyse the European Union (EU) and its member states' current standing in the context of Industry 4.0, a paradigm shift characterised by the widespread adoption of cutting-edge technology and the overall digitisation of manufacturing and other economic spheres. In this article, the writers explore the fundamental policies and methods implemented by the European Union to leverage the opportunities presented by Industry 4.0.

They examine the European Union's strategy for fostering technical innovation, competitiveness, and long-term economic development. This article explains how the European Union (EU) approaches issues such as research funding, regulatory frameworks, and collaborative efforts. In conclusion, the study by Teixeira and Tavares-Lehmann offers a comprehensive survey of the responses of the European Union and its member states to the Industry 4.0 transformation. Addressing the alignment, obstacles, and opportunities amid this paradigm shift, the authors shed light on Europe's preparedness to reap the benefits of digitisation and cutting-edge technology in the manufacturing sector.

2.2.3 Defining Roles and Responsibilities

Defining roles and responsibilities is fundamental to effective organisation and management. It ensures that individuals and teams understand their tasks, duties, and contributions within a larger context. Delineating roles and responsibilities in professional, personal, or societal contexts promotes accountability, collaboration, and efficient workflows.

Dunn Cavelty and Wenger, (2020) emphasise the complexity posed by rapidly expanding digital technology in international security by exploring the delicate convergence of cybersecurity and security politics. Cybersecurity and security politics are discussed in depth, emphasising how the intricacies of cyber threats challenge conventional security thinking and call for novel solutions. They investigate how

cybersecurity muddies the roles of states, non-state actors, and transnational groups, thereby creating competing political goals. Networked science, defined by the authors as the combined efforts of academics, industry professionals, and government officials to understand and manage cybersecurity issues, is introduced. They highlight the significance of information exchange, specialised knowledge, and teamwork in developing efficient responses to ever-evolving cyber threats. In addition, the study analyses the impact of various stakeholders, such as governments, non-governmental organisations, businesses, and nonprofits, on the development of cybersecurity policy.

The authors investigate how different stakeholders may have competing interests and how they can work together to shape policy outcomes. The authors stress the need for multidisciplinary teamwork, flexible policy approaches, and international cooperation to effectively manage the myriad cyber threats. At the end of their study, they thoroughly examine the interplay between cybersecurity and security politics. The authors shed light on the changing nature of international security in the digital era and the novel approaches needed to navigate this complex terrain by examining the profound interplay among technology, politics, and science.

Luo and Choi, (2022) analyse the role of governments in e-commerce supply chains, with particular attention to cybersecurity issues. Given the constantly shifting nature of cyber risks, the authors investigate whether governments should play a role in regulating and ensuring cybersecurity within e-commerce supply chains. The fast expansion of online commerce and its consequential effect on supply chain operations are acknowledged early in the paper. It highlights the risks resulting from the linked and digital nature of e-commerce supply chains, emphasising the need for cybersecurity within these networks.

The authors investigate the government's potential role in resolving cybersecurity issues in online retail supply chains. The intricacy of cyber risks, the possible economic consequences of breaches, and the roles of numerous stakeholders are all considered as they examine the reasons for and against government action. The writers think of standards, information sharing, investment, and enforcement as possible outcomes of government engagement. Concerns about over-regulation, the pace at which

regulations may be updated to address new dangers, and the potential for innovation to be stifled are among the potential downsides of government interference discussed in this study. The authors simulate and analyse scenarios of government involvement in e-commerce supply chains to assess their effects. Cybersecurity investment choices, data exchange, and supply chain efficiency are among the factors graded. In conclusion, the study offers a deep dive into the role of government agencies in cybersecurity within online retail supply chains. The authors add to the existing discussion about cybersecurity in the digital economy by weighing the pros and cons of government action.

2.2.4 Cyber Threat Detection and Monitoring

Razib et al., (2022) conduct a comprehensive study using a hybrid framework that includes Software-Defined Networking (SDN), Deep Neural Networks (DNN), and Long Short-Term Memory (LSTM) methods to identify cyber risks in smart settings. The authors are concerned with improving the safety of smart environments by using cutting-edge tools and techniques. The authors stress the need for proactive cyber threat identification to protect these intelligent settings. They highlight the sophistication and variability required in detection techniques to stave off current cyber threats.

The authors present a hybrid system that combines SDN, DNN, and LSTM to improve the ability to identify cyber threats in smart settings. The authors explain Software-Defined Networking (SDN), Deep Neural Networks (DNN), and Long Short-Term Memory (LSTM), and how they contribute to the hybrid architecture. This article details how the authors implemented and tested the hybrid architecture using real-world datasets. The authors focus on the framework's capability to efficiently identify a wide range of cyber threats in smart settings, from Distributed Denial of Service (DDoS) attacks to malware infections.

Finally, using a sophisticated hybrid architecture, the study provides valuable information for identifying cyber risks in smart settings. The authors contribute to ongoing efforts to secure the digital landscape and protect smart environments against emerging cyber threats by leveraging SDN, DNN, and LSTM features.

Dionísio et al., (2019) presented an investigation into the use of deep neural networks to identify cyber threats in Twitter data. The authors were interested in identifying potential cyber risks and attacks mentioned on social media platforms using sophisticated machine learning algorithms. The authors advocate using deep neural networks to analyse Twitter data to identify cyber dangers. They emphasise that deep learning approaches have shown promise across many areas due to their ability to capture intricate patterns and interconnections in massive datasets. These authors mine Twitter to compile an enormous dataset of cybercrime- and cyberthreat-related messages. The tweets are used to train and test the deep learning network model. Preprocessing is performed on the gathered tweets to remove noise and prepare the data for feeding into the deep neural network.

In this study, the authors present a deep neural network architecture for automatically detecting and categorising cyber threats, such as malware, phishing, and hacking attempts, from tweets. Using the acquired and cleaned data, the authors train a deep neural network to accurately categorise tweets by topic. They use a wide range of measures to assess the model's effectiveness. Their studies, discussed in the article, show that the suggested deep neural network technique successfully identifies cyber risks using Twitter data. The authors emphasise this method's ability to provide real-time insights into emerging cyber threats and incidents highlighted in the media. Finally, the research offers a valuable examination of how deep neural networks can be used to detect cyber threats using Twitter data. The authors contribute significantly to cybersecurity by presenting a novel method for identifying potential risks and attacks in the online environment using sophisticated machine learning algorithms.

Hossain, Karim, et al. (2018) developed FIF-IoT, a forensic investigation framework for Internet of Things-based systems that leverages a public digital ledger to uncover evidence in criminal investigations. As more devices join the IoT, they become increasingly vulnerable to cyber threats. In addition to their legitimate uses, IoT devices may be used for criminal purposes. Using a public, distributed, and decentralised blockchain network like Bitcoin's, FIF-IoT gathers evidence of interactions among IoT entities (clouds, users, and IoT devices) and stores it securely

as transactions. Therefore, FIF-IoT guarantees strong evidence availability by eliminating a single point of failure in the storage medium and eliminating the need for any entity to control evidence storage. Evidence recorded in the publicly distributed ledger must be trustworthy. Hence, FIF-IoT provides a framework to guarantee these properties. FIF-IoT also provides a mechanism to acquire evidence from the ledger and verify its validity. The authors also claim that FIF-IoT can facilitate the collection of evidence and the validation of its authenticity during a criminal inquiry.

In their research, Razaque et al., (2021) propose an innovative strategy to address cybersecurity threats: a web-based, blockchain-enabled cybersecurity awareness system. This study is critical today, as digital systems are increasingly intertwined and cyber threats have never been more significant. The authors highlight the lack of an effective, transparent method for increasing cybersecurity awareness among individuals and businesses as a critical flaw in current cybersecurity strategies. This research aims to bridge this knowledge gap by advocating for the implementation of a blockchain-enabled system to promote the widespread distribution of cybersecurity awareness materials. Immutability, transparency, and decentralisation are just a few of the features of blockchain technology that make its use in the proposed system remarkable.

The authors stress that consumers can stay up to date on the latest cybersecurity threats and preventive measures through a web-based platform. The authors of this research stress the value of preventive cybersecurity education and training in reducing vulnerability to cyberattacks. The proposed system utilises blockchain technology to provide timely, accurate, and verifiable data on cybersecurity risks, mitigation recommendations, and incident-handling plans as they occur. Given the growing sophistication and specificity of cyber-attacks, this strategy is more critical than ever.

The study also demonstrates the value of multidisciplinary teams in addressing cybersecurity issues. Reflecting the complexity of the cybersecurity environment, the research draws on expertise from professionals across disciplines, including computer

science, data analytics, information systems, and education. This group effort guarantees a comprehensive understanding of the issues and potential solutions. In conclusion, the research presents a novel approach to combating cybersecurity risks using a blockchain-enabled cybersecurity awareness system.

This study highlights the significance of timely, trustworthy information transmission to address the ever-evolving nature of cyber threats, leveraging the transparency and security of blockchain technology. With its focus on awareness and education, the proposed web-based platform makes a critical contribution to cybersecurity. This cross-disciplinary study is essential to preventing cyber threats and ensuring a secure digital future as technology rapidly advances.

According to Grigaliunas et al., (2021) a forensic investigation's goal is to "offer situation awareness in terms of identifying and preserving digital evidence, extracting information, and analysing collected information to assist time-critical decision making". Collecting, inspecting, and analysing digital data from multiple sources, including digital devices, networks, and cloud-based big data, is the process known as digital forensic investigation. In this work, the authors propose and detail a unique digital evidence object (DEO) paradigm for compressing forensic data in digital forensic research.

The proposed DEO model combines category theory with the 5Ws (Who, What, When, Where, and Why) of digital investigative analysis to acquire digital evidence. They provide a real-world example to show how it may aid forensic investigators working with digital evidence. Their findings show that a forensic expert's workload is reduced and decision-making performance is enhanced in a time-sensitive environment when the DEO model reduces the number of false-positive evidence objects provided to the expert.

The study by Maria Jones et al. (2019) explores cybersecurity in the context of Internet of Things (IoT)-based digital forensics, with a specific focus on mobile environments. The authors delve into the intricate dynamics of IoT systems and their potential vulnerabilities, particularly in mobile devices, and propose an analytical approach to

strengthen cybersecurity measures for practical digital forensics in IoT scenarios. The paper sets the stage by acknowledging the rapid proliferation of IoT devices and the growing importance of digital forensics in investigating cyber incidents. In this context, the authors highlight the significance of mobile devices as conduits for IoT interactions and underscore the need for an in-depth analysis of mobile device cybersecurity.

In this paper, the authors propose a strengthened security system that leverages cutting-edge digital forensics technologies to detect potential threats and demonstrate how these technologies can reconstruct past events and provide digital evidence in judicial proceedings. The authors delve into the vulnerabilities introduced by mobile devices into IoT ecosystems, including potential attack vectors, data leakage risks, and the intricate interplay between mobile applications and IoT interactions.

Furthermore, the authors propose an analytical framework to assess and enhance cybersecurity measures in mobile environments. They outline this framework's various dimensions, including evaluating the effectiveness of mobile security protocols, analysing mobile app permissions, scrutinising communication patterns between mobile devices and IoT nodes, and exploring potential security breaches in the mobile environment.

The research paper by Lazzez and Slimani, (2015) delves into the critical domain of web application security attacks and the corresponding forensic investigation techniques. The authors extensively examine the landscape of web application security breaches and highlight the importance of robust digital forensics practices for identifying perpetrators and understanding attack vectors.

The paper begins with an acknowledgement of the prevalent challenges posed by security attacks on web applications. In a rapidly evolving digital landscape, web applications serve as key platforms for a range of services, making them enticing targets for malicious activity. Lazzez and Slimani emphasise the critical need to safeguard web applications against cyber threats, underscoring the need for effective investigative processes to analyse and mitigate security breaches.

The central contribution of the study lies in its thorough exploration of the forensic investigation techniques employed in the aftermath of web application security attacks. The study reinforces its findings by presenting case studies that illustrate the application of forensic investigation techniques in real-world scenarios. These case studies provide practical insights into how various web application attacks can be traced, analysed, and attributed using forensic methodologies.

In their work, Yang et al., (2020) examine the state of security and forensics in the Internet of Things (IoT), including the opportunities and threats it faces. The authors delve into the dynamic nature of IoT technologies, analysing the growing need for robust security measures and efficient forensic approaches to address the inherent dangers and vulnerabilities of networked devices. However, the authors highlight security issues arising from the large number of devices in the network, the variety of communication protocols, and the typically limited processing capacity of IoT devices.

The authors explore the complex interaction between security and forensics, highlighting their mutual benefits in solving IoT-related problems. Prevention of security breaches and assaults is emphasised, as is post-incident forensic investigation to understand the full extent and effect of security incidents. The authors emphasise the need for interdisciplinary research and the sharing of findings throughout the publication to advance IoT forensics and security. They underscore the importance of workshops and conferences like ETSecIoT in fostering creativity, facilitating the exchange of ideas, and accelerating the development of reliable security and forensic solutions for the Internet of Things (IoT).

Zia et *al*., (2017) study discusses the difficulties and complications of digital forensics in the IoT setting (IoT). The Internet of Things (IoT) is revolutionising many fields, but its unique characteristics make it difficult to use standard digital forensics methods. The authors advocate an application-specific digital forensics paradigm to enhance the precision and effectiveness of evidence collection and processing in IoT environments. The authors highlight challenges, such as the wide variety of devices, communication protocols, and data formats, to illustrate how the Internet of Things differs from conventional computing environments. Novel approaches are required

to overcome these obstacles, given the complexities inherent in conducting successful digital forensics investigations within IoT networks.

Many IoT applications, such as smart homes, industrial automation, and healthcare systems, have unique features that traditional digital forensics techniques may not fully account for. The authors' methodology aims to close this gap by tailoring forensic processes to each application's needs. This method accounts for the heterogeneity of IoT installations across data sources, communication methods, and data types. Last but not least, the study by Zia, Liu, and Han provides a relevant and context-aware answer to the new digital forensics problems in IoT settings.

The authors contribute to the development of efficient tactics for evidence gathering and analysis in the evolving IoT environment by acknowledging the complexities of IoT applications and offering an application-specific investigative model. The results of this report have important implications for anyone working in digital forensics, IoT development, and cybersecurity and forensics research.

2.2.5 Training and Awareness

Cybersecurity training and awareness are essential components of any comprehensive cybersecurity strategy. They involve educating individuals within organisations and the public about cyber threats, best practices, and effective measures to prevent and respond to cyber attacks. Cybersecurity training and awareness initiatives are critical for enhancing the overall security posture, reducing vulnerabilities, and fostering a culture of cybersecurity awareness.

Alruwaili's, (2019) research delves further into the role of education in raising people's cybersecurity awareness. The author's primary interest is learning how different training programs have helped people's cybersecurity expertise, habits, and outlooks. The report starts by recognising the significance of human factors in cybersecurity weaknesses. Alruwaili stresses that, even with cutting-edge technology solutions, an organisation's security posture may be severely compromised by the actions and choices of individuals within the organisation. Therefore, people must learn about cybersecurity risks, best practices, and ways to mitigate them.

The author comprehensively reviews the current literature to assess the effectiveness of various cybersecurity awareness training programs. Training formats (such as workshops, online modules, and simulations), training audiences (such as workers, students, and the public), and training outcomes (such as enhanced awareness, improved behaviours, and reduced vulnerabilities) are all discussed in depth. The paper's main contribution is a compilation of previous studies examining the effect of training on cyber-awareness. The author offers helpful insights for enterprises and governments seeking to establish successful cybersecurity training programs by assessing the strengths, limitations, and outcomes of different training methodologies.

In conclusion, the research provides an in-depth analysis of the role of education in raising cybersecurity awareness. The author significantly contributes to our understanding of education's role in reducing cyber risks and promoting a culture of cybersecurity awareness by analysing various training methods, audiences, and outcomes.

He and Zhang, (2019) the paper provides helpful advice for firms looking to develop cybersecurity training and awareness initiatives. The authors offer actionable advice to guarantee the effectiveness of such initiatives in raising cybersecurity awareness and decreasing exposure. The article states that companies must prioritise cybersecurity education and training.

Maintaining a strong security posture requires educating personnel about cybersecurity risks and best practices, given the ever-evolving, increasingly complex nature of cyberattacks. Executive support, customisation, consistent training, interactive learning, practical relevance, measurement and evaluation, a multi-channel approach, continuous learning, role-based training, incorporating social engineering, and feedback mechanisms are just some of the suggestions He and Zhang make for creating practical enterprise cybersecurity training and awareness programs.

Its most significant contribution is the paper's real-world suggestions for making practical cybersecurity training and awareness programs that connect with workers and foster a security culture. He and Zhang offer helpful tips for businesses looking

to improve their cybersecurity by educating employees about the threats they face. Finally, He and Zhang's study concludes with valuable suggestions for developing efficient corporate cybersecurity training and awareness initiatives. The authors make a significant contribution to ongoing efforts to reduce cyber risks and educate and train the workforce to address cybersecurity challenges by emphasising the need for personalisation, engagement, measurement, and continual learning.

The study by Aldawood and Skinner, (2019) presents an in-depth analysis of cybersecurity, social engineering, education, and awareness initiatives. These programs aim to educate people about the dangers of social engineering attacks and improve their ability to recognise and respond to them. The writers focus on identifying the problems, pitfalls, and ongoing concerns related to them. The paper begins by recognising human error as a significant cause of cybersecurity flaws, especially in the context of social engineering attacks. Social engineers coerce victims into disclosing confidential information using psychological and deceptive techniques. Aldawood and Skinner stress the need to inform people of these dangers to lessen their impact.

The authors investigate how well education and training programs protect against social engineering scams. They stress that these initiatives are necessary but not without difficulties. Human psychology, sustainability, adaptability, engagement, and evaluation are some of the primary themes explored in this article. The authors thoroughly evaluate several methods for educating people about social engineering, such as simulations, seminars, e-learning modules, and awareness campaigns. The authors assess the merits and drawbacks of various methods and provide suggestions for improving programme design.

The study concludes with helpful insights into the difficulty of creating training and awareness programs to counter social engineering attempts. The authors contribute to strengthening cybersecurity education and awareness by addressing inherent problems and offering improvement options.

Abu-Amara et al. (2021) propose a SETA-based gamification framework to disseminate cybersecurity information. The authors offer a novel approach to raising awareness of cybersecurity risks and effective practices by combining gamification concepts with the Security Education, Training, and Awareness (SETA) paradigm. The rising prevalence of cyber threats and attacks is recognised as the paper's starting point.

The authors stress that conventional cybersecurity teaching methods may not always keep students engaged or ensure they retain the information they learn. The authors provide the SETA paradigm, a holistic strategy for teaching cybersecurity. Providing personnel with the necessary background information, hands-on training, and ongoing awareness is required to ensure a comprehensive understanding of cybersecurity threats. The study explains how the SETA-based gamification framework can enhance engagement, knowledge retention, and the creation of a security-aware culture in cybersecurity.

The paper's original approach of fusing the SETA model with gamification concepts is a significant contribution. An innovative approach to improving cybersecurity education and awareness is presented through a comprehensive framework that integrates structured instruction with interactive, engaging elements. The paper concludes by presenting a SETA-based gamification framework as an innovative method of enhancing cybersecurity education. The authors add to ongoing efforts to develop more effective and engaging cybersecurity education programs by integrating teaching components with dynamic gaming.

Sabillon et al., (2021) research thoroughly examines a cybersecurity training model that may be used to bolster businesses' efforts to improve employees' understanding of cybersecurity threats. The Cybersecurity Awareness Training Model (CATRAM) is introduced, and a Canadian case study is presented to demonstrate its effective use. The CATRAM model highlights several factors: when developing a custom training programme, it is essential first to identify the organisation's unique requirements and challenges. The authors emphasise the importance of evaluating a company's cybersecurity posture and identifying potential weaknesses. The chapter's main

contribution is the in-depth analysis of the CATRAM model and its practical implementation in the case study. The authors provide businesses with a valuable resource to bolster cybersecurity awareness by offering an organised strategy for planning, executing, and evaluating cybersecurity training programs. Sabillon, Serra-Ruiz, and Cavaller's chapter conclude by presenting the Cybersecurity Awareness Training Model (CATRAM) as a holistic strategy for bolstering cybersecurity awareness initiatives inside organisations. The authors' efforts to increase cybersecurity education and awareness within businesses are strengthened by the case study's evidence of the model's applicability and effectiveness.

Rajan et al., (2021) introduce a modified total interpretive structural model (M-TISM) that gives insights into the complex linkages and interdependencies within organisational strategic cybersecurity management. The authors present a unique approach to analysing and strengthening cybersecurity tactics within enterprises. The authors underline that successful cybersecurity management requires a comprehensive, strategic approach that accounts for technical, organisational, and human dimensions. The M-TISM technique comprises multiple essential processes, including Element Identification, Interrelationship Assessment, Layering, and Model Refinement.

The paper explores the application of the M-TISM framework to organisational strategic cybersecurity management. The authors intend to uncover insights that could inspire more effective cybersecurity methods by examining the relationships and hierarchies among diverse variables. By integrating interpretative structural modelling with hierarchical classification, the authors propose a novel approach to visualising and understanding the relationships among cybersecurity tactics. In conclusion, the research provides a modified total interpretive structural model (M-TISM) for organisational strategic cybersecurity management. By utilising this new paradigm, the authors help establish an organised method for analysing and developing cybersecurity strategies within enterprises.

2.2.6 Challenges Faced by Digital Forensics

2.2.6.1 Technical Challenges

New digital technologies have opened many opportunities and introduced complex challenges to digital forensics. Because cybercriminals may exploit unsuspecting individuals and organisations, digital forensics has become increasingly critical as an investigative tool for establishing the reality of cybercrime. Experts and researchers in digital forensics have been hard at work studying and investigating a wide range of previously identified problems, but this has posed new challenges for the field. There are several problems and obstacles in the field of investigation, some of which relate to the introduction of new technologies. In contrast, others involve establishing new laws and regulations. Some of digital forensics' most significant technical hurdles include encryption, massive amounts of data, and incompatible tools.

In their research, (Lillis et al., 2016) discussed the evolution of communication systems, leading to user-friendly, widely accessible encryption products and services. As encryption technologies and standards evolve, decryption becomes increasingly difficult and time-consuming. This technique joins encrypted files so they can be read. In addition, criminals may cover their tracks by encrypting electronic data. This might impede a digital forensics investigator's investigation. According to studies, 60% of encryption cases are dropped due to difficulties decrypting the evidence. Therefore, the broad availability, low cost, and ease of installation of encryption systems substantially undermine the credibility and validity of digital forensics.

In their research, Lillis et al., (2016) identified a significant challenge for digital forensic investigations: the existence of massive volumes of data hidden in various software systems, such as enterprise resource planning systems. As data volumes grow exponentially, it becomes increasingly challenging for judicial systems and forensic investigators to keep pace with ever-evolving digital threats. Cloud computing has led to the replacement of a large portion of IT infrastructure, such as network switches, servers, and racks, with remote, on-demand, virtualised software that can be scaled up or down based on business needs. Also, the user or a third party might be located anywhere in the world to manage and host these services and data. As a result, the data and software may be stored across multiple physical locations. Because of this

dispersion, forensic experts have less access to and oversight over digital artefacts that may be relevant to an investigation.

The cost, complexity, and usefulness of digital forensic tools and methodologies may vary significantly. According to Karie and Venter, (2015), most digital forensic tools have different sections or pieces, which makes it more difficult for them to collaborate effectively. This is because most digital forensic instruments are heterogeneous. In addition, certain forensic technologies cannot handle the ever-increasing storage capacity of the devices under investigation. This indicates that digital forensic operations face a significant technological barrier when dealing with large targets, as they require more complex analytical approaches. As a result, it can be shown beyond a reasonable doubt that several technological obstacles constitute a significant risk to the efficacy and credibility of digital forensic procedures.

2.2.6.2 Operational Challenges

It is common knowledge that online criminal activity is always the result of a deliberate attempt. As a result, digital forensics faces various obstacles in its operational procedures. Among these difficulties, the prevention, reaction, and detection of incidents have received much attention.

According to Pandey et al. (2020), traditional on-premises information technology systems, which process data on-premises, have an integrated internal incident management procedure to ensure the highest possible level of security. Data loss prevention (DLP) systems, intrusion detection (IDS) systems, and log file analysis (log monitoring) are used in this process to detect data loss and security breaches. Consumers of cloud services may encounter frequent challenges due to these security incidents. This is because anti-forensics technology is embedded in these security events, making it easier for attackers to delete or hide any evidence they may have obtained.

Vincze (2016) said the evidence extraction and investigation process is also adversely affected by the lack of well-defined methods and procedures in digital forensics, which is concerning. It is common knowledge that there is now a lack of uniformity

in digital forensic models, which has made the procedure even more complicated. In addition, it argues that because no standard criteria exist, evaluating forensic specialists' expertise is highly challenging. The lack of established techniques was acceptable when digital forensics was considered a mysterious investigative process. Experts uncovered previously unseen evidence and data, leading to new insights into criminal behaviour. However, digital forensic investigation is no longer confined to low-powered computers due to advances in digital technology. Alternatively, it might occur in a virtualised setting that uses non-standard interfaces and a wide range of storage media.

Alghamdi, (2021) mentioned that digital forensics faces the dangers mentioned above and the forensics readiness challenge. To be forensically ready, a computer system or network must be able to record events in a trustworthy, detailed manner for later analysis. Due to the fast growth of cloud computing, businesses have been forced to execute, develop, and plan their IT strategies more efficiently. The lack of forensic readiness in cloud computing is another concern for digital forensic operations. The necessity for human scrutiny and involvement with physical hard drives is another potential operational difficulty for digital forensics. The process is straightforward when working with a single disc or partition, but RAID configurations make things much more difficult. Due to the intricate nature of digital forensics, manual inspection of hard disc images also presents a risk to digital artefacts. Validity, correctness, completeness, and dependability are all criteria that forensic analysis must satisfy.

Ariffin and Ahmad, (2021) found a significant obstacle in digital forensics: striking a balance between user privacy and the recovery of critical evidence. Despite improvements in storage capacity, only a small percentage of data is analysed before it is either forgotten or deleted. Because of the potential for a breach of the user's privacy, this adds another layer of difficulty to digital forensic investigations. The findings suggest that operational challenges pose a serious threat to digital forensic analysis.

2.2.6.3 Personnel-Related Challenges

The reliability of digital evidence is put at risk due to personnel issues. Several issues affect people, but the most important is the shortage of forensic staff with sufficient training.

According to Wazid et al., (2013) Despite the growing importance of digital forensics amid the prevalence of cybercrime, the field is threatened by a shortage of trained forensic officers. Since digital forensics demands technically skilled specialists certified and trained to provide scientifically sound evidence, a shortage of appropriately educated forensic investigators exists. The high standards in law enforcement and the intense rivalry among agencies have contributed to this scarcity. It is undeniable that the conventional forensic community, law enforcement, and the computer science community have increasingly focused on digital forensics in recent years.

In addition, Ravi et al., (2022) found that semantic differences influence the environment shaped by advances gained in this field. The possibility of a broken chain of custody also exists in the context of personnel issues. The term "chain of custody" refers to the chronological record of where and when evidence was gathered. Since digital evidence cannot be physically controlled, this presents one of the biggest obstacles to digital forensics investigations. Therefore, it is a significant issue to think about. Digital forensics must adequately manage the chain of custody despite the use of proprietary technologies, methods, and legislation across multiple jurisdictions. This is one of the industry's most significant challenges. Therefore, difficulties associated with people constitute a substantial obstacle to typical forensic procedures.

In addition to the issues, Vincze, (2016) highlighted in their research that digital forensics lacks a unified formal representation of methods and information for evaluating and acquiring digital artefacts. Because of this, incompatibilities and conflicts will undoubtedly arise among digital forensics technologies. The absence of a systematic or codified method for assessing, maintaining, and gathering digital evidence may lead to errors in interpreting and analysing digital artefacts. These errors can have serious consequences. Similarly, forensic professionals must use specialised skills and various forms of digital technology to handle large volumes of

data effectively during forensic investigations. On the other hand, these specialists often fail to document their work, making training and external evaluations more difficult. Prior expertise and experience must be leveraged to advance the training of future digital forensic specialists and to encourage information exchange across different detective groups. Unfortunately, digital forensic officers often fail to document their work or adhere to legal norms, posing a significant risk to the integrity of digital forensic investigations.

2.2.7 Application and Use of IoT in an Organisation and Home Applications

As current research on IoT infrastructures confirms, IoT use spans personal, work, health, and educational domains, among others. The related work in this section examines the use of IoT in organisational and home settings, focusing on security procedures and design from a DFR perspective.

Kim et al., (2020) explain that devices are more complex in intelligent home scenarios and during forensic investigations, posing challenges to the extraction of meaningful data for analysis. This is because IoT devices in smart homes use different storage methods and data formats. In this scenario, acquiring meaningful data for cybercrime investigation can be difficult. The authors focus on acquiring, classifying, and analysing data from various devices across smart home environments. The results were provided to show the data that can be acquired in a smart home environment for cybercrime investigation. This study highlights that IoT forensics is possible, though obtaining evidence from IoT devices remains difficult. IoT devices are common in smart living, manufacturing, automation, and healthcare. It is noted that IoT can improve people's quality of life; however, the exposure of personal data to cybercriminals undermines its benefits (Surange et al., 2021).

Do Valle et al., (2020) explain that in criminal investigation scenarios, the use of a Lambda architecture that involves frameworks such as HDFS (Hadoop Distributed File System), Kafka, Spark, and Docker was used to analyse big data volumes to identify digital traces from large datasets that involve IoT device data. Furthermore, the Lambda architecture was used to extract and process data for crime analysis. The

State Attorney of Rio Grande used the Lambda architecture in the state of Do Norte (Brazil) to investigate a crime and conducted test evaluations. The results were deemed good, but the effectiveness of this architecture must be verified across diverse real-time scenarios.

To implement DFR in an organisation, designers must incorporate a range of operational and operational planning strategies, such as risk assessment, employee training, implementation tools, and measurement tools (Ab Rahman et al., 2016). Acquiring digital evidence in a cybersecurity breach investigation is highly important. However, the complexities of IoT create questions and obstacles in IoT forensic investigations, especially in obtaining and analysing digital evidence from IoT devices (Atlam et al., 2020). Harbawi et al., (2017) argue that the sophisticated nature of IoT in its data exchange mechanism through the 'things' element in the device can undermine digital evidence trials. This creates the need for a new method or procedure for data acquisition. This new procedure is explained through a theoretical framework for the IoT forensic model. The issues in the model for evidence acquisition are discussed. The implementation results of real-time data acquisition can further verify the effectiveness of this theoretical framework.

Many authors provide frameworks for acquiring IoT data when exploring the literature. For example, Ngobeni et al. (2010) introduced the DFR wireless model, which focuses on monitoring, logging, and preserving wireless network traffic. Although this model is not based on IoT technology, the concept of wireless network traffic applies to IoT-enabled environments. However, this model does not comply with international standards or implement organisational and security processes.

Oriwoh and Sant, (2013) recommend the Forensic Edge Management System (FEMS) designed to provide security and monitoring for the home Internet of Things. FEMS is an innovative tool to help IoT owners secure their applications and deliver proven services. FEMS is designed for home IoT systems, not enterprise-wide systems. Therefore, the organisation's requirements, such as legal and forensic strategies and policies, are unmet. It also does not comply with international standards.

Kebande et al., (2016) proposed a Digital Forensic Investigation Framework for IoT (DFIF-IoT) based on the international standard ISO/IEC 27043. The framework comprises three modules: proactive, IoT forensics, and reactive. However, it needs to cover organisational-level processes as a significant part of the DFR process across the organisation.

Meffert et al. (2017) provided a general framework, Forensic State Acquisition from IoT (FSAIoT), to demonstrate in practice that relevant data from IoT devices can be extracted via three modes: controller-to-device, controller-to-cloud, and controller-to-controller. Although this research shows promising results in acquiring data from IoT devices during a forensic investigation, the framework does not address the readiness state. Therefore, further research is needed to address various challenges.

Hossain et al. (2018) present a forensic investigation framework (FIF) for IoT that uses a public digital ledger. This framework collects data from IoT, cloud, and user devices, then securely stores it on a blockchain network for public access. This framework ensures integrity, confidentiality, anonymity, and non-repudiation by storing data on a public digital ledger. A case study demonstrates effectiveness, and a prototype demonstrates performance. Probe-IoT is another framework that uses blockchain to store data acquired from IoT devices. This framework provides a mechanism for obtaining evidence from a digital ledger and further verifies the data for authenticity and integrity (Hossain et al., 2018). Additionally, these frameworks (FIF-IoT and Probe-IoT) do not address readiness states or international standards.

Kebande et al. (2018) propose adding DFR to the IoT's smart environment using the standard procedure specified in ISO/IEC 27043. This prepares the IoT-based environment for the ultimate cybersecurity incident. However, the authors acknowledge that more research is needed to enable organisations to develop standards that make the implementation process appropriate for their organisation.

Chi et al., (2019) proposed a framework for IoT data acquisition and analysis. This framework collected data from user devices and the cloud to illustrate the data acquisition process, but it does not address forensic readiness in organisations or

incorporate international standards. Furthermore, most of the research presented is not based on an approved standard, such as the ISO/IEC 27043 (ISO, 2015). Table 2 compares research findings that target organisations that have adopted readiness processes with standardised approaches.

2.3 IoT Security Process

Schiller et al. (2022) explain that electronic devices with sensing and communication capabilities have steadily replaced "ordinary" physical objects over the last two decades. Consequently, the Internet of Things (IoT) will quickly become critical in many fields of use. Smart objects are increasingly used in various settings, including businesses, public areas, households, and hospitals. About 30 years after the concept of the Internet of Things was first proposed, substantial security risks have emerged. Security breaches have far-reaching effects on many parties because of the interconnectedness and pervasiveness of IoT devices. In the past, we have seen how several vulnerabilities on the Internet of Things were exploited to cause material, financial, and health impairment. Despite these risks, manufacturers often lack the resources to adequately protect IoT devices.

The IoT has changed how people communicate and operate in our environments, from smart homes to factory automation; insecure Internet of Things (IoT) devices can compromise an entire network. Data and services inside the IoT ecosystem must be protected to maintain their confidentiality, integrity, and availability. Authentication, encryption, access restriction, and constant monitoring are cornerstones of IoT security. However, new security concerns have emerged as the number of connected devices grows. Given the nature of the information and infrastructure they manage, IoT assets must be protected. To better understand the threats that may affect IoT assets, this literature review examines current IoT security methods.

2.3.1 Understand Risks to IoT Assets

Effective cybersecurity methods for protecting Internet of Things (IoT) assets require a thorough understanding of the risks they face. Assets in the Internet of Things (IoT) include devices with an Internet connection and are therefore subject to cyberattacks.

Radanliev et al. (2019) provide an in-depth analysis of the complex landscape of risks associated with IoT devices. The authors discuss the crucial issue of protecting these networked assets in an age characterised by the rapid use of IoT devices across numerous industries. They highlight the growing interconnection of IoT systems, which enhances efficiency but also exposes them to greater risk. The research begins by recognising the pervasiveness and rapid expansion of IoT devices across settings ranging from smart homes to factories. It highlights the critical importance of security in these interdependent ecosystems and analyses the far-reaching consequences of vulnerabilities and possible attacks inside IoT contexts.

The unique security issues posed by IoT are a primary focus of the paper. The authors argue that a robust security architecture must be established for IoT systems due to the sheer scale of IoT deployments, the limited resources of many IoT devices, and the wide variety of communication protocols. The research also investigates the vital topic of risk assessment and management of the Internet of Things. It stresses the need for preventative measures to determine where cyberattacks are most likely to occur and where vulnerabilities exist in Internet of Things (IoT) networks and devices.

The authors also highlight the value of resilient IoT systems, guiding how to make devices more resistant to and responsive to cyberattacks. They highlight the need for continuous monitoring, anomaly detection, and effective incident response procedures to protect the usefulness and security of IoT assets. The essay also discusses the need for government and industry standards to establish baseline security measures for IoT producers. It touches on the role of policy and legislation in IoT security. This regulatory strategy aims to reduce the potential harm from IoT by promoting a safer environment for connected devices.

2.3.2 Evaluate IoT Risks

Despite the advantages to industry and business, the IoT is vulnerable from a security and privacy standpoint. Most IoT devices have low capabilities, their networks differ, and IoT-related standards are fragmented. The IoT's design provides a helpful framework for classifying the many security threats it faces. Security issues are categorised based on their location within the various IoT architectural layers.

IoT Layers	Security Risks
Sensing Layer	Unauthorised access
	Routing attack
	Transmission threats
	Denial of services (DoS)
	Malicious code
	Selfish threat
	Spoofing attack
	Availability
Network Layer	Data breach
	Transmission threats
	Routing attack
	Transmission threats
	Denial of services (DoS)
	Malicious code
Service Layer	Privacy threats
	Routing attack
	Replay attack
	Denial of services (DoS)
	Service information manipulation
Application Interface Layer	Remote configuration
	Security management
	Misconfiguration
	Management system

Figure 4: Security risks in the IoT architecture (Kim, 2017)

Kim, (2017) used a four-tiered architecture to outline the main security concerns, including a sensing layer built into IoT terminal components for detection and data collection. A network layer provides the framework for both wireless and wired communications. A service layer that facilitates necessary management operations for end-users and software programs. A layer for interacting with programs or the application interface. Figure 4 shows the Security risks in the IoT architecture.

Moreover, Jeyanthi, (2016) explains that the five phases of the IOT can be used to characterise the various types of attacks that can be started against it: (1) data collection, acquisition, perception (from devices); (2) storage (of these data); (3) intelligent processing (data analysis to provide intelligent services); (4) data transmission (between components); and (5) delivery (of the data to the things). In

terms of the Five Phases (Figure 5), the author depicts and discusses every conceivable assault or issue.

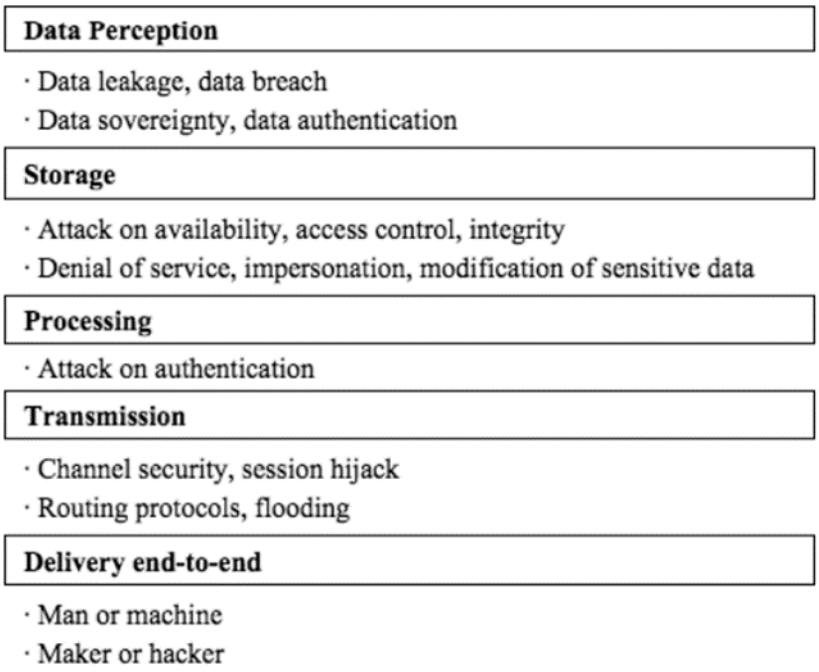

Figure 5: Attacks on phases (Kim, 2017)

According to Jeyanthi, (2016) when sensitive information is sent to unauthorised parties, it is known as a data leak or breach. A dishonest or disgruntled worker is usually the one who starts it. Data sovereignty refers to a country's legal jurisdiction over its citizens' digital data. The Internet of Things (IoT) is subject to international law since it connects devices worldwide.

A data breach may be seen as hostile to an organisation and its employees. Data authentication aims to confirm that information has not been tampered with in transit and has been accessed only by its intended recipients. For example, a distributed denial-of-service (DDoS) attack from multiple attackers across the network might reduce availability; a flash crowd forms when many users simultaneously attempt to access the server. Heavy traffic is caused by restless, legitimate users making multiple identical requests quickly, or by spoofing attackers pretending to be other devices or users committing attacks in secret. Lastly, there are three methods by which sensitive data might be altered in transit from sensors: (1) content alteration, (2) sequence manipulation, and (3) temporal modification.

Jeyanthi also showed IoT levels and potential dangers to each (Figure 6). The sensing layer, integral to IoT devices, is the focus of the following assaults.

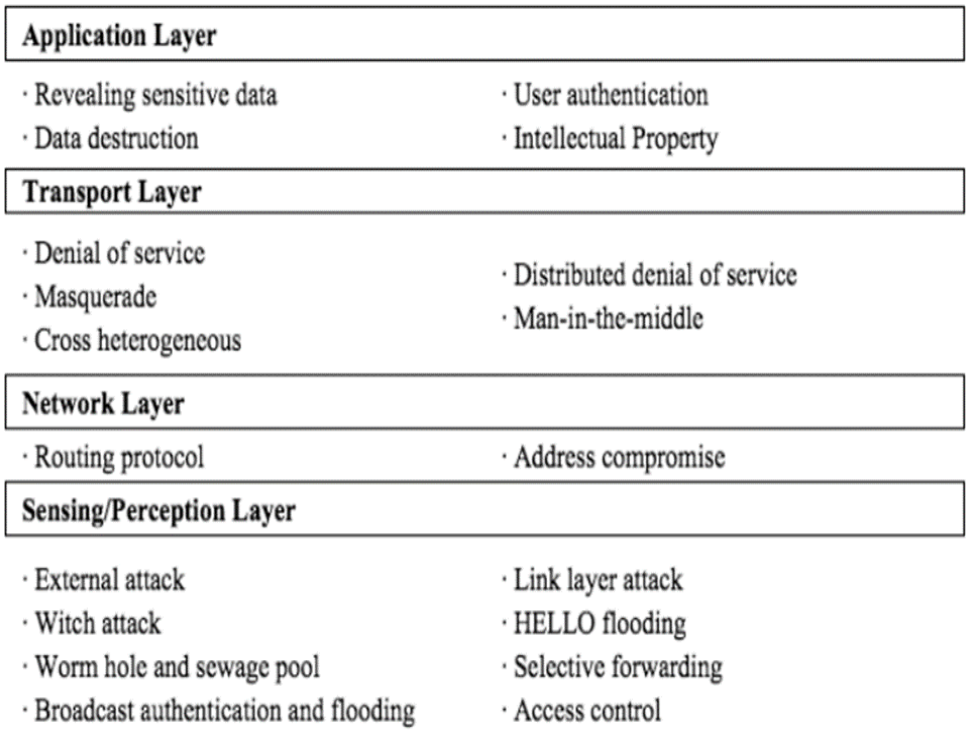

Figure 6: Possible attacks based on architecture (Jeyanthi, 2016)

When cloud companies sell or otherwise disclose their customers' data, they expose themselves to external attacks. Ad hoc networks are particularly vulnerable to wormhole attacks, in which hackers intercept communications between disparate systems and relay them to a third party through an improvised tunnel. A selective forwarding attack occurs when hostile nodes forward only certain packets, some of which may include private information. A sinkhole attack enables an attacker to post additional attacks, such as selective forwarding, falsification, and alteration, on a compromised node by drawing in information from all surrounding nodes. Malicious users in a sewage pool attack pull all communications from a targeted area, then switch to attacking the network's base station node. Data loss occurs when a legitimate node is compromised by a witch attack, allowing an adversarial node to assume control of the communication channel. A HELLO flood news attack may reduce the availability of a network if a malicious node acquires access to all other nodes in the network, broadcasts "Hello" requests across an extensive frequency range, and then floods them with "Hello" messages.

IoT risks are not limited to those that can be grouped by system design. According to (Abbass et al., 2019) several security flaws might be exploited to cause damage to users of Internet of Things devices by, for example, (1) allowing unauthorised access and abuse of personal information; (2) aiding attacks on other systems; and (3) posing safety issues. It elaborated on why these risks may be even more severe than cyber threats. First, hackers might intercept and alter sensitive information delivered to or from IoT devices due to inadequate security measures. For instance, information stored on smart TVs for online shopping might be compromised due to device security flaws. Second, if an IoT device has security vulnerabilities, it may be exploited in attacks against the network to which it belongs or against other systems. One possible use for a hacked IoT device is to launch a distributed denial-of-service (DDoS) attack. Third, unauthorised individuals may threaten physical safety by exploiting security flaws. For instance, a patient may be at risk if an insulin pump were hacked remotely.

Multiple security risks were outlined by Lin and Bergmann (2016) for IoT and smart home setups. For example, a loss of confidentiality in a home monitoring system might result in the unauthorised disclosure of private data. Unauthorised warnings about the state of a system, for example, might disrupt a home's controller and provide an intruder with a means of entry. Finally, access hazards can leave a system unsecured through unauthorised access to administrative functions.

2.3.3 Policies for IoT Devices

Although the IoT can enhance people's quality of life, there is also a risk of privacy and security issues arising from its widespread use. Organisations and other entities create policies for Internet of Things (IoT) devices to regulate their procurement, deployment, maintenance, and protection. Integrating IoT devices securely and responsibly into an organisation's infrastructure requires strict compliance with these regulations. When designing an IoT device, we must consider privacy concerns, even though there is currently no new legislation to set a precedent. If an IoT device intends to collect user information, it must obtain the user's consent to the Privacy Policy. The security, functionality, and ethical use of IoT devices within an enterprise or network depend on establishing proper regulations for their deployment and usage. Risks are

minimised, private information is protected, and device management standards are established with these rules.

ISO, (2015) "Information technology — Security approaches — Incident investigation concepts and procedures" is a standard that lays out a methodology and set of rules for investigating data breaches methodically and thoroughly(ISO, 2015). ISO/IEC (International Organisation for Standardisation/International Electrotechnical Commission) has developed several standards and recommendations for the administration of Internet of Things devices. The policies and security, interoperability, and compliance of IoT devices may all benefit significantly from these standards. The purpose is to help companies respond promptly and efficiently to information security incidents. The standard specifies the concepts and procedures for investigating events to reduce their impact, determine their causes, and prevent recurrence. It addresses various security problems, ranging from data breaches and cyberattacks to system flaws. Policy considerations for IoT devices are addressed by the following ISO/IEC standards and guidelines:

ISO/IEC 27000: This standard provides definitions and an overview of information security management systems. IoT device policies may benefit from a thorough understanding of key terms and concepts related to digital forensic preparation.

ISO/IEC 27001: ISO/IEC 27001 is a standard for establishing and maintaining information security management systems. Rules governing the safety of IoT devices are based on risk assessment and continuously improved using this framework. Using an ISMS enables the secure storage of data generated by IoT devices and the systematic management of their security (ISO, 2015).

ISO/IEC 27002: The benchmark for information security. It details installing security controls for Internet of Things (IoT) gadgets and infrastructure (ISO, 2015).

ISO/IEC 27019: ISO/IEC 27019 is sector-specific; however, it provides insight into security measures that may enhance digital forensics preparedness in Internet of Things (IoT) settings. It may help shape the Internet of Things (IoT) gadget regulations, especially in the energy and utility industries (ISO, 2015).

ISO/IEC 27035: Establishing and sustaining an incident management procedure that incorporates digital forensic operations is not possible without ISO/IEC 27035. Implement these standards for IoT devices to include digital forensics preparedness in incident response (ISO, 2015).

ISO/IEC 27037: This international standard offers guidance for locating, gathering, acquiring, and storing digital evidence. To ensure that all potential digital evidence is collected at the start of an investigation, these Recommendations detail the steps to follow during the initial response phase. These recommendations can be included in IoT device rules to ensure the systematic collection and preservation of digital evidence according to best practices and effective digital forensic preparedness (ISO, 2015).

ISO/IEC 27038: There may be sensitive material in particular papers that cannot be shared with the public. Once the original document has been appropriately processed, the revised version may be shared with these communities. Redaction refers to the procedure of omitting confidential material. New to the field of document management, digital redaction poses its own set of challenges and dangers. Redacted information in digital documents must remain unrecoverable. As a result, caution must be taken to ensure that the redacted content is permanently deleted from the electronic document (e.g., it must not be hidden in non-displayable portions of the document). Digital redaction procedures are outlined in the international standard ISO/IEC 27038. It also lays down the criteria for redaction software.

ISO/IEC 27041: The digital forensics community now has access to comprehensive, industry-specific standards. Businesses may use these recommendations to craft regulations on topics ranging from evidence handling to the communication of findings in digital forensic investigations in Internet of Things settings. Any inquiry techniques and procedures used must be justified. This paper aims to ensure that the methods and procedures used in an investigation are adequate and meet the necessary tests.

ISO/IEC 27043: While not specific to digital forensics, it provides a framework for incident investigation. It may be used in incident investigations to guarantee a systematic approach to digital forensic preparation for Internet of Things device rules.

ISO/IEC 15408: ISO/IEC 15408 is not an IoT-specific standard, but it can be used to assess the security measures of any product. It ensures IoT devices have sufficient security measures to support digital forensic readiness.

ISO/IEC 21823-1: While the primary emphasis of this standard is on data management, it may also inform IoT device policies regarding data that may be useful for digital forensics. A system's preparedness for digital forensics relies heavily on the quality of its data management.

Organisations may use these ISO/IEC standards and recommendations to create well-rounded, secure, and compliant policies for IoT devices. While IoT technology and the security landscape are constantly evolving, these standards must be adapted and integrated to meet unique industry requirements and organisational demands. Incorporating these ISO/IEC standards and recommendations into your organisation's IoT device rules ensures your business is ready for digital forensic operations, enabling more efficient incident response and security investigations.

2.3.4 Implementation of IoT Security Processes in an Organisation

Protecting IoT systems, data, and devices against threats and vulnerabilities requires implementing IoT security practices within an organisation in accordance with ISO/IEC standards. Establishing, maintaining, and improving security in IoT environments can be done in accordance with ISO/IEC standards. An outline of the operation is as follows:

2.3.4.1 Understanding the IoT Environment

To begin with IoT, it's essential to fully understand the company's current setup. Identify all connected devices, networks, and data streams. This knowledge is vital for developing a workable plan to keep things safe.

2.3.4.2 Risk Assessment

Conduct a risk analysis to discover weaknesses and dangers in the IoT infrastructure. Consider potential hazards such as information leakage, tampered devices, and unauthorised access. ISO/IEC 27001 and 27005 standards provide procedures for handling potential threats.

2.3.4.3 Security Policies and Procedures

Create and document security measures specific to the Internet of Things. Data encryption, access authorisation, device management, incident handling, and regulatory compliance are all vital. Information security management systems (ISMS) may be built using the guidelines ISO/IEC 27001, provided (ISO, 2015).

2.3.4.4 Access Control and Authentication

Implement robust access controls to limit interaction with IoT systems to approved users and equipment. It is recommended to use robust authentication techniques, such as two-factor authentication.

2.3.4.5 Data Encryption

Achieve end-to-end encryption of IoT data. Protect information from eavesdropping and tampering by using robust encryption. Information security guidelines are available in ISO/IEC 27002.

2.3.4.6 Device Management

Securely enrol, monitor, and decommission Internet of Things devices by establishing a device management system. Security fixes and firmware updates should be applied to IoT devices frequently.

2.3.4.7 Incident Response Plan

Create an IoT-focused incident response strategy that covers all bases. Establish measures to detect and address security breaches in the Internet of Things. The incident management guidelines are provided by ISO/IEC 27035.

2.3.4.8 Security Awareness and Training

All workers, contractors, and other stakeholders should be taught best practices for protecting the Internet of Things. Users should be educated about the risks of the Internet of Things and how to mitigate them through awareness initiatives.

2.3.4.9 Compliance and Audit

Conduct regular audits of the Internet of Things security mechanisms to verify that they align with the rules and standards set. Information security management systems are defined in ISO/IEC 27000.

2.3.4.10 Privacy Considerations

Given the sensitive nature of data processed by IoT devices, all privacy policies and procedures must comply with internationally recognised privacy standards, such as ISO/IEC 27552, Privacy Information Management System (PIMS).

2.3.4.11 Security Testing and Validation

Identify security vulnerabilities in IoT devices and infrastructure through penetration testing and other security audits. Maintaining a strong security posture requires regular testing. The implementation of ISO/IEC-based IoT security practices is underway. To safeguard a company's IoT infrastructure and keep pace with evolving risks, management must implement preventive measures. A business's security culture should include regular training, audits, and risk assessments to maintain a secure and reliable Internet of Things (IoT) environment.

2.3.5 Preventing and Managing Threats

Given the unique characteristics of IoT systems, it is important to familiarise oneself with existing risk management frameworks and IoT security technologies before developing an IoT risk management framework.

Security needs for IoT, as outlined by Kim (2017), include user authentication, secure execution, tamper resistance, secure data transfer, secure content, and identity management. The IoT is divided into four categories: architecture, devices, protocols, and technologies (Fig. 7). All users who want to interact with the IoT system must first authenticate. Internet of Things devices must be physically and logically secure to withstand hacking attempts and other hostile actions. For a program or application to run safely, the hardware or software on which it is running must be well-designed and secure.

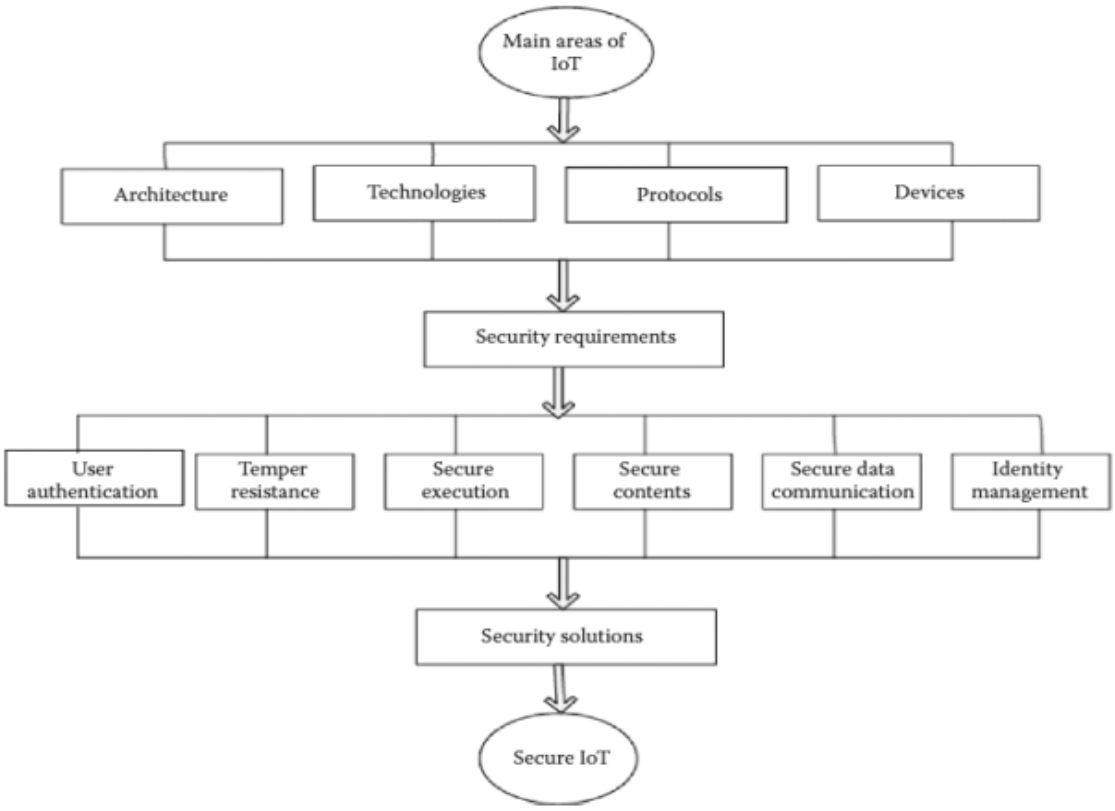

Figure 7: Security Requirements for the IoT (Kim, 2017)

Key management, authentication, identity, and security checks are essential to any data transmission system. Identity management's primary focus is safeguarding the identification of Internet of Things devices. Maintaining confidentiality requires limiting access to specific data to authorised parties only. To conduct an audit, the system must maintain user activity logs. Integrity guarantees that transmitted data remains unaltered. They also discussed methods to reduce the impact of IoT issues. From an architectural perspective, encryption, authentication, and key management can safeguard the perception layer. In contrast, an intelligent intrusion-detection system can protect the network layer (a common target of DDoS attacks) and the application layer (a key target of privacy breaches) by restricting user access.

2.3.6 Authentication Technologies in IoT

To prevent attackers from obtaining unauthorised access to IoT entities' data, such as devices and users, authentication methods are used (Shancang Li and Li Da Xu, 2017). All four Internet of Things (IoT) levels—interface, sensing, network, and service are vulnerable to compromise if authentication is inadequate. Researchers have developed various authentication mechanisms to enable secure communication across

disparate devices and systems. Internet of Things security is now dominated by studies on authentication methods. RFIDs and automobiles are only two examples of IoT devices for which authentication mechanisms have been created.

The scalable authentication methodology for RFID systems presented by Akgün and Çıalayan, (2015) applies physically unclonable functions with random physical changes to provide a higher degree of privacy while maintaining constant identification time. The authors propose using Physical Unclonable Functions (PUFs) to enhance the privacy and scalability of RFID systems. RFID tags use PUFs, hardware-based security features that generate random responses to requests, preventing tracking and the leakage of sensitive information.

The study investigates the use of PUFs in RFID systems, which offer a viable approach to addressing privacy and scalability concerns without sacrificing RFID's usefulness or efficiency. This study significantly advances our understanding of the convergence of security and RFID technologies, highlighting a potential strategy to enhance the confidentiality and scalability of such systems across a range of contexts.

Anonymous RFID authentication with untraceability and forward secrecy was proposed by CHIEN, WU, and HSU (2015), using a partially distributed server architecture in which only some authentication information is shared. Security concerns have arisen due to the widespread use of RFID technology for monitoring and identifying items. This study introduces a paradigm that uses a partly distributed server architecture to keep RFID identification systems secure and private.

The method described in the study improves untraceability, making it more challenging to monitor RFID tag holders and to maintain forward secrecy, while guaranteeing the integrity of previously authenticated data even in the event of a compromised encryption key. With potential applications across a wide range of sectors that require robust security protocols, the article offers valuable insights into enhancing the privacy and security of RFID authentication in remote systems.

2.3.7 Encryption and Key Management in IoT

Cybersecurity Services, networks, and sensors may all be compromised due to insufficient encryption. Encryption is essential for maintaining data confidentiality, which is critical for IoT security, as noted by (Lin and Bergmann, 2016). During transmission between IoT devices and servers, sensitive information, including data and the security key, is protected by encryption.

Although encryption safeguards the information in transit, it does not conceal its origin or destination. Key management systems were developed to address this need by restricting access to only those granted permission. Low-performance hardware and varying network conditions make it challenging to use traditional encryption and key management methods in IoT devices; thus, specialised solutions tailored to IoT devices have been developed.

Bokefode et al., (2016) used AES and RSA cryptographic algorithms to safely upload IoT data to cloud storage, allowing for secure communications in the cloud-based IoT ecosystem. The authors propose a secure cloud storage system that employs role-based encryption to restrict users' access to data based on their assigned roles. This method enhances cloud storage security for IoT data by deterring unauthorised access.

Reed-Solomon codes for error detection and correction were applied by Shah, Malik and Ahmad (2016) to safeguard smart home systems against errors caused by corrupted or damaged data. While Reed-Solomon codes are more commonly used to ensure data integrity during transmission, this research proposes using them to safeguard Internet of Things (IoT)-based home automation systems. Reed-Solomon codes provide an extra layer of security for IoT applications in the home by encoding and decoding data, enabling the system to detect and, if necessary, correct unauthorised or malicious changes.

This study contributes to the broader discussion on protecting connected devices and systems within the IoT framework by offering insights into tackling security challenges in IoT-based home automation. The study employs Reed-Solomon codes to propose a novel approach to Internet of Things (IoT) security.

2.3.8 Mechanisms to Detect Unknown Threats

A significant obstacle in cybersecurity is detecting unknown attacks, often referred to as zero-day attacks or advanced persistent threats (APTs). Standard security practices focus on thwarting known attacks, leaving businesses vulnerable to unknown threats. This literature overview provides insights into innovative methods to improve cybersecurity, covering numerous processes and tactics for identifying unknown threats.

According to (Tabassum and Lebda, 2019), numerous security threats posed by IoT devices to businesses have been proven. Organisations need an innovative system that automatically identifies suspicious IoT devices connected to their networks, given the growing use of these devices, their variety, the hurdles to standardisation, and their inherent mobility. It is essential to identify any Internet of Things (IoT) devices that aren't on the organisation's approved "whitelist." The study aimed to reliably identify IoT device types from the whitelist using the Random Forest supervised machine learning method to attribute network traffic.

The authors collected network traffic data from 17 distinct IoT devices across nine categories and manually categorised it to train and evaluate multi-class classifiers. Classification of 20 consecutive sessions using majority rule showed that 96% of test cases accurately recognised unknown IoT device kinds. In contrast, 98% of white-listed device types were correctly classified as their actual types. Not all categories of Internet of Things devices were immediately recognised. It took analysing 110 consecutive sessions to achieve 100% identification of unlawful IoT device types. In contrast, it took 346 sessions to obtain 100% categorisation of white-listed device kinds (with a success rate of 99.49%). Extensive testing showed that classifiers taught in one setting performed well when evaluated in another.

2.4 Forensic IoT Process

Cybersecurity Forensics for the Internet of Things (IoT) is increasingly vital as IoT systems and devices become more pervasive and, consequently, more vulnerable to cyberattacks and misuse. The Forensic IoT procedure outlined in the International Standard is deliberately abstract, applicable to various digital investigations and

forms of digital evidence. ISO/IEC 27043:2015 primarily focuses on incident investigation principles and processes rather than on comprehensive guidelines for the forensic Internet of Things (IoT) process (ISO, 2015).

However, it provides a general framework for digital investigations, which can be adapted to IoT environments. This approach is intended for designing and developing high-level processes, decomposing them into components (ISO/IEC 27041). In addition, the International Standards' procedures are meant to be all-encompassing, as they harmonise previously published digital processes. The investigative procedures are precisely laid out and described to ensure they can be followed. This procedure comprises four distinct phases, further subdivided into categories, as shown in Figure 8.

The Forensic IoT process, as defined in ISO/IEC 27043:2015, comprises a set of systematic steps for conducting digital investigations in the Internet of Things (IoT) context. In this approach, readiness processes help organisations define IoT scenarios and strategies, identify potential sources of digital evidence, and establish procedures for data collection, preservation, and analysis. The initialisation phase is critical for a prompt response to IoT incidents, followed by acquisition processes in which investigators securely identify, collect, transport, and store IoT data.

Digital forensic investigation in IoT-enabled organisational environments increasingly relies on integrating proactive monitoring systems and forensic readiness mechanisms. Intrusion Detection Systems and SIEM platforms can detect malicious activity and generate real-time security alerts, while Digital Forensic Readiness processes ensure that evidence-relevant data is preserved in a structured and legally defensible manner. The proposed research model, therefore, positions forensic readiness as an operational extension of cybersecurity monitoring rather than an isolated post-incident activity. This integrated approach supports continuous evidence generation, secure evidence preservation, forensic investigation preparedness, and compliance with ISO/IEC 27043 readiness principles.

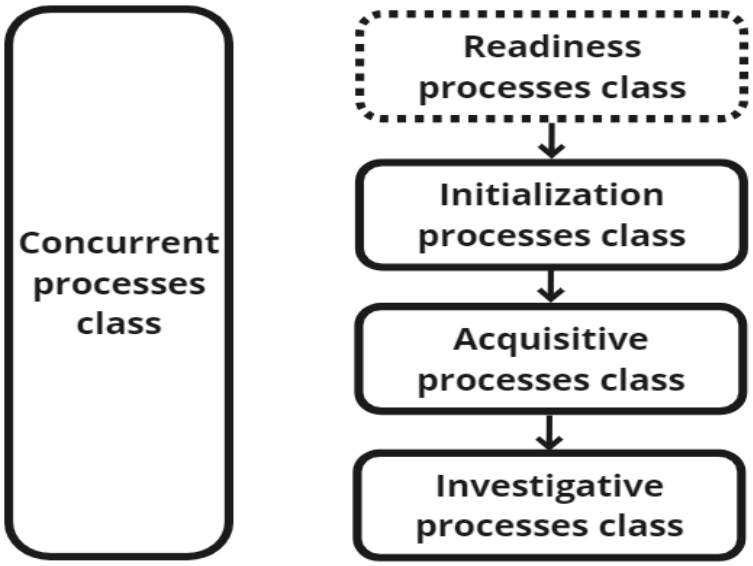

Figure 8: Digital Forensic Investigation process classes (ISO, 2015)

According to Kebande and Venter, (2018) the practices that ensure an organisation can make the most of Digital Forensic evidence in the event of an incident fall under the category of "readiness processes." Groups of processes that kick off the digital forensics inquiry are stored in the initialisation processes class. The acquisition method category provides instructions for collecting potential digital evidence. Digital incident investigation, analysis, interpretation, and presentation are all subclasses of the forensic investigation process. The process of concluding an investigation is also part of this. All process groups that happen simultaneously with a digital inquiry fall under the umbrella of "concurrent process classes." According to the authors, there are additional advantages to requiring the readiness process class as part of the digital investigative procedure.

According to ISO, (2015) organisations may maximise their use of digital evidence by preparing for the process and ensuring that relevant and usable forensic data is recorded and preserved in a manner that is investigation-friendly. In addition, the preparedness process team ensures that the organisation-wide definition, implementation, and optimisation of the technology, people, and processes involved in an investigation minimise business disruption during an actual incident. By outlining, implementing, and optimising procedures before an incident occurs, the

process group reduces the time and resources required to conduct a digital investigation.

ISO/IEC 27043 Digital Forensic Investigation Lifecycle provides a comprehensive international framework for digital forensic investigation and forensic readiness, defining standardised processes for the identification, collection, preservation, examination, analysis, interpretation, and reporting of digital evidence. Unlike traditional cybersecurity approaches that primarily focus on threat detection and incident response, ISO/IEC 27043 establishes a complete forensic investigation lifecycle that supports both proactive readiness and post-incident investigative activities within organisational environments.

The standard structures a digital forensic investigation into multiple interrelated process groups to ensure evidential integrity, repeatability, reliability, and legal defensibility throughout the investigation lifecycle. These process groups include readiness, initialisation, acquisition, investigation, concurrent, and assessment processes. Collectively, these phases establish a systematic framework for managing digital evidence before, during, and after cybersecurity incidents.

- **Readiness Process Group**

The readiness process group focuses on proactive preparation activities carried out before security incidents occur. The primary objective of forensic readiness is to ensure that organisations are technically, operationally, and procedurally prepared to identify, collect, preserve, and analyse digital evidence in the event of cyber incidents. In IoT-enabled organisational environments, readiness activities are particularly important because of the distributed, heterogeneous, and highly dynamic nature of IoT infrastructures.

Readiness activities include developing forensic policies, evidence retention procedures, logging strategies, chain-of-custody documentation, incident response integration, staff training, and infrastructure planning. The readiness process also involves identifying potential sources of digital evidence across IoT devices, cloud platforms, network infrastructure, endpoints, and security monitoring systems. This

proactive preparation enables organisations to minimise evidence loss, reduce investigation delays, and improve the efficiency of forensic investigations.

In this research, readiness processes were operationalised through continuous monitoring mechanisms using Wazuh and Splunk, secure log retention procedures, forensic evidence management workflows, and real-time alerting configurations to support proactive evidence acquisition and forensic preparedness.

- **Initialisation Process Group**

The initialisation process group is activated once a security incident or suspicious activity has been identified. This phase focuses on confirming the incident's existence, defining the scope of the investigation, authorising investigative procedures, and preparing the resources required for evidence acquisition and forensic examination. In organisational IoT environments, initialisation activities may include validating IDS or SIEM alerts, identifying affected IoT devices, establishing investigative priorities, and assessing the potential impact of the incident on organisational operations. This process also includes assigning investigative roles, defining legal authority for evidence acquisition, and ensuring compliance with organisational policies and regulatory requirements.

The integration of intrusion detection systems and forensic readiness mechanisms within the proposed framework supports rapid initialisation by enabling automated alert generation, event correlation, and preliminary incident classification.

- **Acquisitive Process Group**

The acquisition process group focuses on identifying, collecting, preserving, and securing digital evidence from relevant sources. Evidence acquisition in IoT-enabled environments poses substantial challenges because digital evidence may be distributed across devices, sensors, gateways, cloud services, virtual machines, edge nodes, and network infrastructure. This phase requires investigators to preserve evidential integrity while collecting logs, metadata, network traffic, system artefacts, memory captures, authentication records, and event traces. Preservation mechanisms such as hashing, timestamp validation, secure storage, and chain-of-custody

documentation are essential to ensure that evidence remains admissible and reliable throughout subsequent investigation stages.

In this research, acquisitive processes were implemented through continuous log collection, event preservation, secure evidence storage, and forensic data extraction using Wazuh and Splunk infrastructures. Real-time monitoring enabled the proactive collection and preservation of digital evidence during simulated cyberattacks.

- **Investigative Process Group**

The investigative process group focuses on examining, analysing, interpreting, and reconstructing digital events associated with a cybersecurity incident. During this phase, investigators analyse acquired evidence to identify attack vectors, determine attacker behaviour, establish timelines, reconstruct events, and assess the incident's impact on organisational systems. Digital forensic investigation in IoT-enabled environments is particularly complex because investigators must correlate heterogeneous evidence from multiple interconnected devices and systems. Investigative activities may include log correlation, anomaly detection, behavioural analysis, malware analysis, network traffic analysis, and evidence reconstruction across distributed infrastructures.

The proposed model supports investigative processes through integrated SIEM analysis, machine-learning-based attack detection, evidence prioritisation, and event-correlation mechanisms that identify suspicious patterns and reconstruct cyberattack activity.

- **Examination and Analysis Activities**

Within ISO/IEC 27043, examination and analysis are critical components of the investigative process. Examination involves extracting, filtering, and validating digital artefacts relevant to the investigation, while analysis focuses on interpreting evidential relationships and drawing conclusions from forensic findings.

This study employed machine learning models, including XGBoost, Random Forest, BaggingClassifier, and Extra Trees, to support evidence analysis and cyberattack classification. These models enhanced the ability to identify critical forensic indicators,

prioritise evidence sources, and improve the efficiency of digital investigations in complex IoT environments.

- **Reporting and Presentation Process**

The reporting process focuses on documenting investigative findings, evidential procedures, analytical results, and forensic conclusions in a clear, structured, and legally defensible manner. Effective forensic reporting is essential to ensure transparency, accountability, and admissibility in organisational investigations and legal proceedings. Reporting activities include documenting evidence-acquisition procedures, maintaining chain-of-custody records, presenting analytical findings, summarising attack timelines, and explaining investigative conclusions. The reporting process must demonstrate that evidence integrity was maintained throughout the investigation lifecycle and that all forensic procedures complied with recognised standards and organisational policies.

Within the proposed model, forensic reporting was supported by automated SIEM dashboards, log analysis reports, event visualisation, and forensic documentation processes integrated into the readiness workflow.

2.4.1 Readiness process groups in ISO/IEC 27043

ISO/IEC 27043 specifies four distinct process groups that comprise the readiness process, as shown in Figure 9. This section explains the readiness processes and accurately reflects the international standard ISO/IEC 27043.

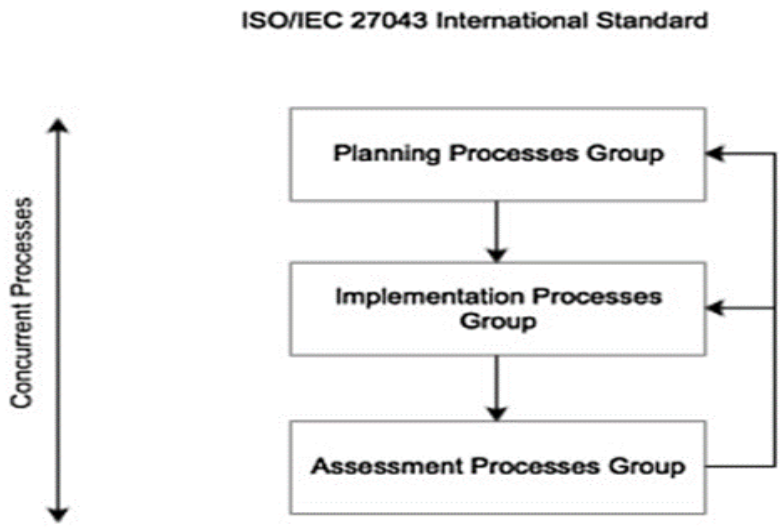

Figure 9: Readiness process groups (ISO, 2015)

2.4.1.1 Planning Process Group

ISO/IEC 27043 defines the planning process group as the set of actions that determine how Digital Forensic evidence will be collected, stored, analysed, and presented before an event occurs. Choosing what to do after discovering an occurrence is also part of this collection of processes. The DFR process is further ensured to consider legal and business-specific criteria by the planning process group (ISO, 2015).

2.4.1.2 Implementation Process Group

This process group implements the procedures outlined in the strategy phase. Systems and procedures are established, and the system architecture process is implemented to support digital forensic evidence collection. Software and hardware for recording incidents, storing data, and monitoring modifications might all fall under this category (ISO, 2015).

2.4.1.3 Assessment Process Group

The actions in this process group compare the outcomes of the implementation process group with the goals set for attaining DFR. The evaluation findings are included in the DFR process for improvement. For digital evidence to be admitted in court, the improvement must also evaluate whether it satisfies that jurisdiction's legal criteria and the Digital Forensic principle (ISO, 2015).

2.4.1.4 Concurrent Processes

Concurrent processes are operations that co-occur in digital investigations. These steps are not ordered and apply across various stages of the digital investigative process. One method to keep the chain of custody intact while digital evidence is passed between parties is to use the "preserving chain of custody" technique for most steps in the digital investigative process (ISO, 2015).

All prospective Digital Forensic data and other relevant data must be recognised, gathered, processed, and stored in accordance with organisational procedures; these processes are designed for this purpose. Critical data sources within an organisation must be identified and managed, as must forensic data, Digital Forensic tool adoption, incident response, and monitoring. In Figure 10, the preparedness steps are thus highlighted.

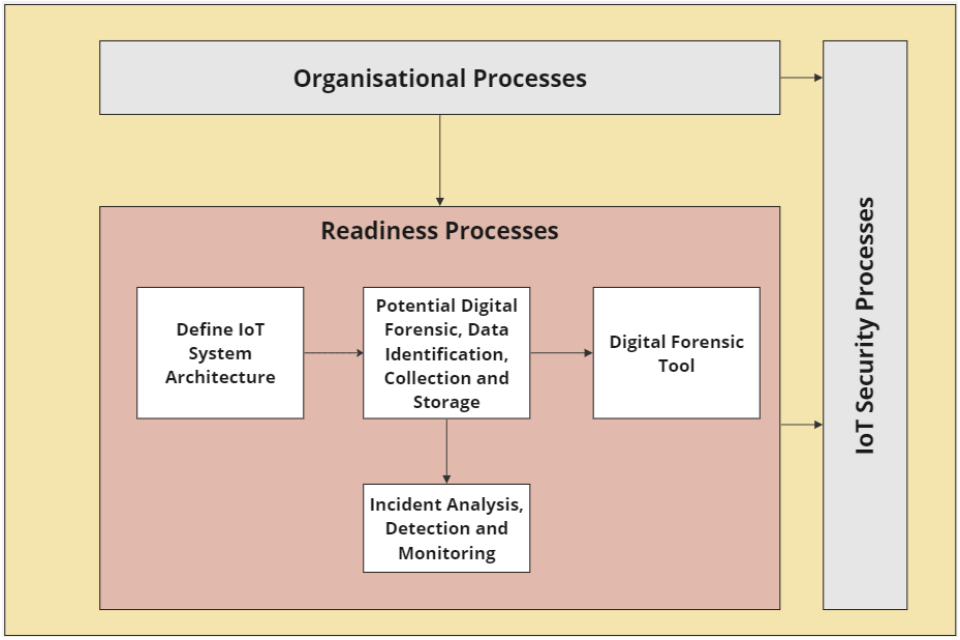

Figure 10: Readiness processes (Kebande et al.*, 2020)*

2.4.2 Defining IoT System Architecture

To gather, share, store, analyse, and process data, a network of physical objects, intelligent devices, cars, communication protocols, buildings, sensors, and software is necessary, as stated by Jabraeil Jamali et al., (2020). For the Internet of Things to work, sensors must provide a reliable link between the digital and real worlds. The term "Internet of Things architecture" refers to the complex arrangement of components that constitute IoT networking systems. These include sensors, Protocols, cloud services, actuators, and layers. In general, it's structured in levels that facilitate evaluation, monitoring, and upkeep by administrators. IoT data travels from sensor-equipped devices to the network and finally to the cloud, where it may be processed, analysed, and stored. There is much potential for the Internet of Things to continue expanding, bringing forth exciting new possibilities for its users.

Jabraeil Jamali et al., (2020) propose a three-layer model for IoT architecture. Typical IoT architecture is shown in Figure 11. Perception is the physical layer that includes sensors for gathering data about the surrounding world. Some physical parameters are detected, or other intelligent features are recognised in the surrounding environment. The network layer interacts with other layers, such as the transport layer, and with devices such as computers and servers. Sensor data transmission and processing are also made possible by its features. The application layer oversees the

delivery of the user's desired functionality. Smart homes, smart cities, and intelligent health are just a few examples of the many uses defined for the IoT. While the three-layer design is adequate for defining the big picture of IoT, it is not sufficient for research on IoT, which often focuses on the finer details of the concept. The five-layer design is specified.

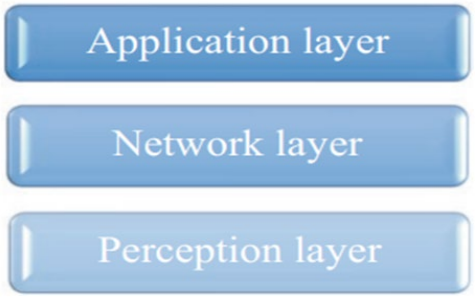

Figure 11: Conventional IoT architecture (Jabraeil Jamali et al.*, 2020)*

IoT technology has become increasingly popular in recent years and can be used in various contexts. Different Internet of Things applications function as intended and are designed for specific contexts. However, there is no universally accepted definition of architecture. Depending on the nature of the work, an appropriate number of architectural layers may be required.

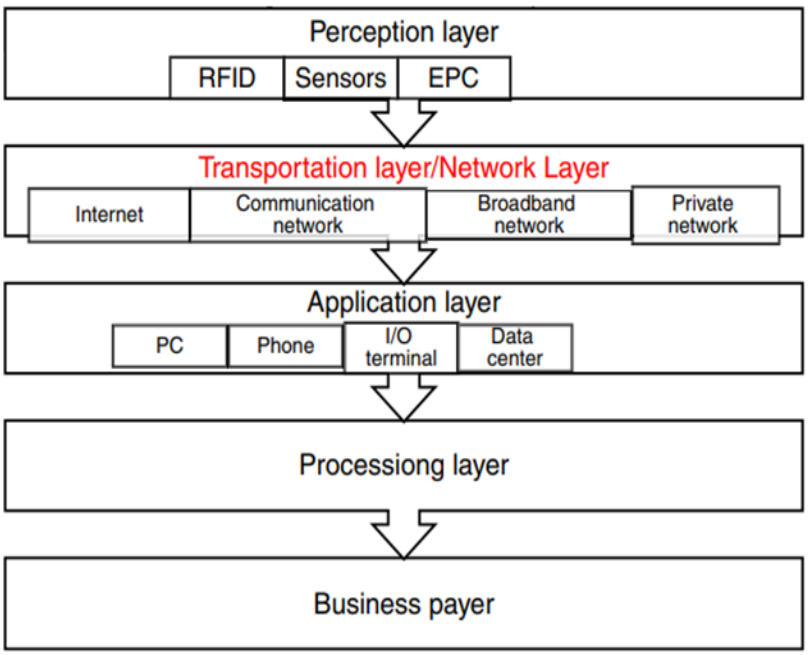

Figure 12: Five-layer architecture of IoT (Vishwakarma, Singh and Sharma, 2019)

According to Vishwakarma et al. (2019), the Five-layer design is the most common. This architecture has five layers: business, application, processing, transportation, and perception, as shown in Figure 12.

2.4.2.1 Perception/Sensing Layer

The "things," or endpoint devices, are the foundation of any Internet of Things system, serving as a bridge between the analogue and digital domains. Sensors and actuators that collect, receive, and analyse data across the network are part of the physical layer, referred to as "perception." Both wireless and cable connections may be used to link sensors and actuators. The architecture has no restrictions on the size or placement of its parts.

2.4.2.2 Network Layer

The network layer describes the overall flow of data in the program. Gateways to the Internet and other networks, as well as Data Acquisition Systems (DAS), reside here. A DAS is a data aggregation and transformation system (collecting and aggregating data from sensors, converting analogue data to digital data, etc.). Data acquired by sensors must be sent somewhere and processed. The network layer is responsible for this. These gadgets may now interact with one another, servers, and smart devices on the network. In addition, it manages all the gadgets' data communications (Vishwakarma, Singh and Sharma, 2019).

2.4.2.3 Processing Layer

The processing layer is the Internet of Things' central nervous system. Data is typically evaluated, preprocessed, and stored here before being sent to the data centre, where it is accessible to software programs that monitor, manage, and potentially act on the data. Here's where things get interesting: Edge IT and edge analytics.

2.4.2.4 Application Layer

The application layer is the user interface, providing services specific to the program. For example, consider a smart home app that lets users activate appliances, such as coffee makers, with a single tap. Smart cities, smart homes, and smart healthcare are among the many applications of the Internet of Things.

2.4.2.5 Business Layer

The system functions as an IoT manager. The business model-related applications are included. This layer is responsible for studying new business and profit models and overseeing the release and pricing of different apps (Vishwakarma, Singh and Sharma, 2019).

According to ISO/IEC 27043, a company's system architecture consists of its network, endpoints, data, and software. System architecture is defined so that the organisation's most valuable data and information sources may be located throughout the IT infrastructure (ISO, 2015).

Kebande et al., (2020) introduced the IoT data management cycle, which can be used at any time to identify prospective IoT data sources. The Internet of Things (IoT) data lifecycle includes creation, distribution, archiving, processing, integration, distribution, and consumption. At the Internet of Things (IoT) device layer, data is generated when sensors collect information from their environment and transmit it to the corporate network. These devices require a unique identifier to facilitate streamlined retrieval and querying across the company network. Local aggregation modules might be placed near the sensors to reduce the number of nodes responsible for data collection and storage.

2.4.3 Collect Digital Data, Identification, Detection and Storage

Yaqoob et al., (2019) state that the organisation's primary data sources serve as a map for locating suitable Digital Forensic data. Key data sources that handle crucial organisational data are among the possible Digital Forensic data sources. Prioritised business needs and situations, as emphasised in organisational-level procedures, are also potential sources of digital forensic data. It's worth noting that IoT gadgets often have very little storage space. As a result, they can store only limited information, particularly in Digital forensics.

To this aim, it is suggested that valid Digital Forensic data be sent to an IoT gateway or a remote Digital Forensic database for analysis and storage. In addition, each forensic record must include the "who," "what," "when," and "how" of an event when considering possible DF data acquisition. That is, forensic recordings must include as

many identifiers as possible, each uniquely identifying an IoT device, user, network device, location, or activity.

A high level of timestamp accuracy is required; therefore, it is essential that forensic data is accurately timestamped during collection to enable reliable correlation of events across multiple log sources. All devices participating in the IoT environment should maintain synchronised system clocks through trusted time sources and secure time management mechanisms. Techniques such as cryptographic timestamping and centralised network time synchronisation help preserve timestamp integrity and support the reconstruction of incident timelines across distributed systems.

Beyond technical data collection requirements, organisations must ensure that digital evidence remains legally admissible and forensically sound throughout its lifecycle. In IoT-enabled environments, evidence may originate from numerous interconnected devices, gateways, cloud platforms, and network infrastructures, increasing the complexity of evidence management. Consequently, it is not sufficient to collect data alone; organisations must also demonstrate that the evidence remains authentic, complete, reliable, and unaltered from collection through analysis and reporting.

To preserve evidential integrity, forensic-ready logging mechanisms should incorporate controls such as cryptographic hashing, secure storage repositories, access controls, audit trails, and integrity verification procedures. These controls help ensure that any modification, deletion, or unauthorised access to evidence can be detected and investigated. Furthermore, forensic-ready logs should capture sufficient contextual information, including device identifiers, user information, network addresses, event descriptions, and associated metadata, to support accurate interpretation and reconstruction of events during forensic investigations.

An equally important consideration is maintaining a robust chain of custody. Chain-of-custody procedures provide a documented record of how evidence was identified, collected, transferred, stored, accessed, analysed, and preserved throughout the investigation lifecycle. This documentation establishes accountability and transparency, enabling investigators, organisations, and legal authorities to

demonstrate that evidence has been handled consistently and under controlled conditions. Without adequate chain-of-custody controls, the evidential value and legal admissibility of digital evidence may be challenged.

Compliance and auditability also play a significant role in Digital Forensic Readiness. Organisations must ensure that evidence collection, storage, and analysis processes align with recognised standards and regulatory requirements. ISO/IEC 27043 provides guidance on forensic readiness and investigation processes by emphasising the systematic identification, preservation, integrity management, and documentation of evidence. In addition, organisations operating in jurisdictions subject to privacy regulations, such as the General Data Protection Regulation (GDPR), must ensure that forensic data collection activities remain lawful, proportionate, and accountable. This includes implementing appropriate controls for data retention, access management, data minimisation, and secure disposal of evidence.

Therefore, effective Digital Forensic Readiness requires a balance between operational monitoring, forensic evidence preservation, legal compliance, and privacy protection. By incorporating evidential integrity controls, chain-of-custody management, auditability mechanisms, and compliance requirements into evidence collection processes, organisations can improve their ability to generate reliable, legally defensible, and admissible digital evidence while maintaining alignment with ISO/IEC 27043 and applicable regulatory obligations.

2.4.3.1 Operational Logs versus Forensic-Ready Logs

Organisations routinely generate operational logs to support system administration, performance monitoring, troubleshooting, and security management. While operational logs provide valuable information regarding system activities, they are not necessarily suitable for forensic investigations without additional controls and safeguards.

Operational logs are primarily designed to support day-to-day operational requirements. Their purpose is to assist administrators in monitoring system performance, diagnosing faults, and identifying technical issues. Consequently, such

logs may not contain sufficient contextual information, may be overwritten after short retention periods, and may lack mechanisms to verify their integrity.

In contrast, forensic-ready logs are specifically designed to support digital investigations. These logs are generated, collected, and preserved to ensure their evidential value is maintained throughout an investigation. Forensic-ready logs typically contain richer contextual information, detailed metadata, reliable timestamps, device identifiers, user information, and event correlation data, enabling investigators to reconstruct incidents accurately.

A key distinction concerns evidential integrity. Operational logs can often be modified, deleted, or overwritten without generating audit records. Forensic-ready logs incorporate integrity verification mechanisms such as cryptographic hashing, secure storage, access controls, and audit trails to demonstrate that evidence has not been altered after collection.

Metadata preservation also represents a critical requirement for forensic readiness. Metadata, including file creation times, modification dates, source device identifiers, user accounts, network addresses, and event sequencing information, provides investigators with valuable context during evidence reconstruction. Loss of metadata can significantly reduce the evidential value of digital records.

Timestamp reliability is equally important in IoT-enabled environments, where evidence may originate from multiple distributed devices. Forensic-ready logging requires secure time synchronisation mechanisms, trusted time sources, and accurate timestamp recording to enable reliable event correlation across diverse systems and devices.

Furthermore, forensic-ready logs support chain-of-custody requirements by documenting how evidence was generated, collected, transferred, accessed, and preserved throughout its lifecycle. This provides accountability and supports legal admissibility by demonstrating that the evidence has remained authentic and untampered. Consequently, while operational logs assist system management and security monitoring, forensic-ready logs provide the evidential foundation required

to support Digital Forensic Readiness and enable effective investigation of cybersecurity incidents within IoT-enabled organisational environments.

2.4.4 Analysis (Detection and Monitoring)

According to ISO (2015), it is crucial to establish an incident detection and response mechanism so that, when suspicious behaviour is detected, the appropriate course of action can be taken. A list of triggers should be established and categorised by severity and event effect, as outlined in ISO/IEC 27043, based on the organisation's use cases and business plans. A predetermined, comprehensive response strategy must accompany these events. Depending on the needs of the business, incident monitoring may also be used to keep tabs on other quality of service indicators related to the Internet of Things. Organisational forensic preparedness may be affected by monitoring data quality, networks, and even energy networks, all of which are quality of service indicators.

2.4.5 Digital Forensic Process

The Digital Forensic Process can, therefore, be defined as a structural and systematic approach to identifying, acquiring, examining and demonstrating digital evidence within the context of computer crimes, criminal and civil offences, or breaches of policy to the satisfaction of the relevant legal standards (Aziz, et al, 2013). This is a relevant step in handling evidence that helps maintain its admissibility and credibility in the investigation. Identification is the process by which the scene is defined and the potential sources of evidence, including clients, servers, mobile devices, and cloud storage. This is followed by the Preservation step, in which measures are put in place to preserve the evidence in its form at the time of collection. This entails making duplicate copies of data admissible in court and documenting their transfer.

During the collection phase, structured data is extracted using specialised tools to ensure accuracy and prevent data from being harmed. This leads to the Analysis phase, in which evidence is scrutinised to identify crucial details. It can also include an analyst who might use specialised tools to detect viruses or hackers' attempts, track intruders, or restore chronological order. The following documentation details all outcomes, procedures, and checks and balances to develop a well-structured report

that may be useful to the relevant authorities or for legal action. Lastly, the Presentation phase entails communicating the evidence and conclusion in a convincing, easy-to-comprehend format, such as PowerPoint presentations, videos, or testimony in court if the case is in a court of law, to professionals such as lawyers, businesspersons, or police.

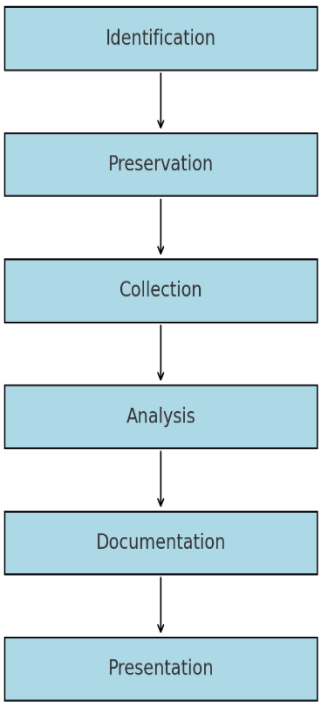

Figure 13: DFR Process

Digital forensic processes can also be cyclical, repeating as the situation demands. It is done to standardise the workflow, identify potential leads, process and collect evidence, report findings to support decision-making, and ensure a sound legal profile (Wang et al., 2023).

2.4.6 Forensic Tools Evolution

The field of digital forensics has developed numerous tools and techniques over time to match the increasing challenges in the modern digital ecosystem, characterised by the extensive proliferation of IoT devices. The evolution from traditional tool-based forensic measures to advanced, IoT-specific forensic solutions is addressing the unique challenges of real-time monitoring, large volumes of data, and diverse device types.

According to Kebande et al., (2020), inadequate technology raises doubts about the reliability of the Digital Forensic evidence collected, analysed, stored, and presented. For this reason, it's crucial to use a Digital Forensic tool that is adaptable to the needs of the IoT-enabled environment and can be adjusted to meet the organisation's preparation procedures. Identifying meaningful Digital forensic data is complicated by the massive amounts of data generated, analysed, and stored by IoT devices. As a result, a strategy must be developed to prioritise specific DF data, signal when an event occurs, and provide follow-up instructions.

Rather than monitoring the development of forensic technologies, ISO/IEC 27043:2015 concentrates on incident investigation concepts and methods (ISO, 2015). However, in the context of incident investigation and digital forensics, it is necessary to recognise that developing forensic tools is key to enabling investigators to conduct more in-depth, efficient investigations. The development of forensic tools has followed the steps outlined in ISO/IEC 27043 for incident investigation (ISO, 2015).

2.4.6.1 Early Digital Forensics Tools (Pre-ISO/IEC 27043)

Early digital forensics technologies laid the groundwork for digital investigations prior to the publication of the standard. These devices have enabled basic data recovery and evidence preservation, making them integral to incident investigation processes and, by extension, to the preparedness and acquisition procedures outlined in ISO/IEC 27043.

2.4.6.2 Data Recovery and Disk Imaging (Pre-ISO/IEC 27043)

The ability to make disk images that are accurate down to the last bit was a huge step forward. This feature is crucial for archiving evidence and conforms to the preparedness and acquisition procedures outlined in ISO/IEC 27043.

2.4.6.3 Keyword Searching and Registry Analysis (Pre-ISO/IEC 27043)

Finding digital evidence and patterns is consistent with the investigation procedures outlined in ISO/IEC 27043, aided by early keyword searching and registry analysis tools (ISO, 2015).

2.4.6.4 Mobile Device Forensics (Pre-ISO/IEC 27043)

Especially in instances involving smartphones and tablets, the introduction of mobile device forensic techniques has enabled investigators to broaden their focus. When dealing with digital evidence from several sources, this is pertinent to ISO/IEC 27043.

2.4.6.5 Network Forensics (Pre-ISO/IEC 27043)

Investigations into network intrusions and cybercrimes need forensic tools to examine network traffic. These resources satisfy the need for network analysis in forensics research.

2.4.6.6 Cloud and IoT Forensics (Post-ISO/IEC 27043)

Following the publication of ISO/IEC 27043, forensic tools have evolved to accommodate modern cloud and IoT environments. The importance of investigating cloud data and understanding interactions between IoT devices has increased. This fits nicely with the progress made in forensics equipment (ISO, 2015).

2.4.6.7 Traditional Tools

Most digital forensics relies on conventional forensic tools, which were fundamental and still applicable in many respects. Examples of case studies include EnCase and FTK, whose innovations enabled the creation of exact disk images and the preservation of complete evidence without modifying the original. Integrity was maintained, while investigators were enabled to perform thorough analyses. Keyword searching was another significant feature that enabled rapid retrieval of essential information from extensive data collections by narrowing the search to specific words or patterns. Moreover, registry analysis revealed most aspects of the user's activity, including installed software and probable security violations, which are significant for personal computer investigations. Traditional tools, despite their strong capabilities, often fell short of meeting the requirements of modern digital ecosystems, particularly the dynamic, heterogeneous environments introduced by IoT systems.

2.4.6.8 Advanced Forensic Tools

Modern ecosystems are now being addressed by progressive forensic tools that employ cutting-edge technologies and methods, incorporated into the toolbox for such purposes.

- Wazuh: Wazuh is a potent open-source security platform for real-time monitoring and log management, which proves to be very useful as a tool for protecting the IoT. Wazuh provides file integrity monitoring, which helps detect unauthorised modifications to the configuration or firmware of IoT devices, thereby ensuring their security and stability. Wazuh also includes a centralised management system for distributed IoT networks, improving visibility and control across a wide variety of devices. The centralised interface of this system facilitates monitoring and allows administrators to manage diverse IoT environments from a single platform.

- Splunk: Splunk, the most advanced analytics platform in existence, is well known for its ability to handle and process vast amounts of data generated by IoT-based devices. It would be best suited to data-rich investigations and decision-making in highly complex environments. Real-time visualisation and analysis are much more effective at quickly identifying trends, patterns, and anomalies in the collected data.

  Such capability is vital for identifying potential security risks and operational inefficiencies in today's IoT systems. Integrated with numerous IoT protocols and platforms, Splunk is agnostic to heterogeneous application-, network-, and device-level IoT environments. This is to ensure maximum flexibility and applicability for an organisation in combining data from various IoT-enabled devices, sensors, and networks to present a comprehensive overview of an IoT infrastructure. In this way, it can be seen that, through its analytical engine and extensive integrations, Splunk supports organisations in driving data-driven decision-making and maximising system performance and security across IoT ecosystems.

- Blockchain: Blockchain is a modern technology that plays a vital role in proof storage and validation in a tamper-proof way, making it particularly valuable in digital forensics. The two main features of a blockchain, immutability and transparency, are strong reasons to see it as the best method for protecting evidence integrity in almost all legal and investigative settings where data authenticity is crucial. Once information is entered into a blockchain, it can never

be changed or deleted. Therefore, device logs, transactions, and evidence are guaranteed to remain permanently intact and fully valid at a specific moment. This also highlights the importance of maintaining the chain of custody for digital evidence; any tampering or unauthorised modifications could compromise the investigation.

Blockchain can also be used to securely log device data from IoT systems, ensuring it remains as evidence in its original context throughout the investigative process. This security layer has potential in the IoT sector, where concerns about unauthorised modification or breaches are especially acute at the level of data generated by connected devices. Investigators can then verify the authenticity of evidence, make it admissible in court, and significantly improve the reliability of the investigation. These advanced forensic tools, including blockchain, work together to provide efficiency, trustworthiness, and security in digital forensics, especially within today's complex and often vulnerable IoT environment.

Advanced forensic tools are essential for tackling the challenges posed by a vast network of interconnected IoT devices. Real-time tracking and anomaly detection are crucial components of this technology because IoT devices constantly generate high-volume data. They enable ongoing monitoring of devices with integrated anomaly detection, helping to trace unusual behaviour or potential breaches as they happen. Quick intervention can sometimes prevent further damage, especially considering how long a threat might remain active before being addressed.

Moreover, IoT ecosystems produce an enormous variety of data, both in type and volume. Their functions are highly diverse, as are their communication protocols and data outputs. With versatile forensic technology, investigators can collect all types of data and integrate, analyse, and interpret multiple sources while maintaining a clear critical context. Automation also plays a vital role in accelerating investigations by minimising human errors. Automating simple tasks such as log collection, event correlation, and data analysis enables forensic tools to enhance investigation accuracy, allowing investigators to focus on more complex cases. This improves efficiency,

ensuring faster throughput and comprehensive coverage of extensive investigations involving numerous IoT devices, thereby increasing the overall speed and accuracy of forensic processes.

2.4.7 Interpreting Results

Organisations need to be able to interpret the findings of ISO/IEC 27043:2015 investigations to react to and manage digital events effectively (ISO, 2015). Here's how to make sense of the data and use it in your investigation:

2.4.7.1 Understanding the Incident

Understanding the event in its entirety is the first step in evaluating the outcomes. The guideline recommends a preliminary evaluation to determine what occurred and its severity. Assessing the incident's potential consequences, affected assets, and root cause is part of this process.

2.4.7.2 Results of Readiness Processes

Readiness procedures are among the incident investigation processes classified in ISO/IEC 27043. Organisational preparation for responding to events must be assessed when interpreting the outcomes of readiness activities. This process includes evaluations of personnel competence, issue detection, and infrastructure design.

2.4.7.3 Results of Initialisation Processes

Incident detection, first reaction, planning, and preparation are all part of the initialisation process. The success of incident detection, the timeliness of the response, and adherence to the investigative plan are all crucial considerations when interpreting the findings of these procedures.

2.4.7.4 Results of Acquisitive Processes

Finding and processing possible digital evidence is the focus of acquisitive procedures. Assessing the efficiency of evidence identification, gathering, transportation, and storage is essential for interpreting the outcomes of these procedures.

2.4.7.5 Results of Investigative Processes

Examining, analysing, interpreting, reporting, presenting, and finally wrapping up an inquiry are all steps in the process. In this last step, data are interpreted by evaluating

the accuracy of the analysis and interpretation, the thoroughness of the report, and the clarity of the presentation of the findings.

2.4.7.6 Concurrent Processes

The standard emphasises parallel procedures that operate in tandem to ensure the reliability of digital evidence. For this analysis, it's essential to consider if proper permissions were granted, whether the chain of custody was maintained, whether digital evidence was safeguarded and whether contacts with physical investigations were coordinated.

2.4.7.7 Assessment of Implementation

An evaluation of the efficacy of the incident investigation procedures is required after the findings of each procedure have been interpreted. This entails contrasting the achieved results with the desired objectives to spot discrepancies and provide solutions (ISO, 2015).

2.4.7.8 Continuous Improvement

Recognising that incident investigations should be an ongoing educational process is crucial for making sense of the findings. To better respond to future incidents, systems, procedures, and training should be refined based on the findings of each inquiry.

2.4.7.9 Action Plan

After analysing the data, businesses should develop a strategy to address problems or strengthen weak points. Training, resource allocation, and procedural modifications are among the methods that could be incorporated into this strategy to improve incident investigation.

2.4.8 Documentation

Documentation is the primary product of the digital evidence interpretation process, as it captures the investigators' interpretation. The Documentation should be printed on paper if cost-effective. Some digital investigations may produce a large volume of digital evidence artefacts. Therefore, care must be taken to ensure that no crucial digital evidence is overlooked by including all relevant digital evidence in the Documentation. The documentation must be prepared in clear, unambiguous

language. Those unfamiliar with the technical aspects of incident investigations should also be able to grasp it. Judges, juries, defendants, attorneys, prosecutors, company executives, stockholders, and staff are all examples of those who may hear such a speech (ISO, 2015).

Documentation authors should continually consider how their work may be used by the various stakeholder groups listed above in the event of legal action. Writers of such Documentation should also consider the consequences of their work being incorrect or misunderstood. Consequently, the documentation should include more details on subjects such as which potential evidence was collected/acquired, which analytical procedures were carried out, which assertions were considered, and from whom. Sometimes, there is insufficient evidence to draw any firm conclusions. Assumptions, associated probabilities, and inferences drawn from them should all be laid out explicitly in such Documentation. The speculativeness of these inferences cannot be overstated.

2.4.9 Presentation

According to ISO, (2015) the document produced throughout the documentation process must be made available to a broad audience. The primary goal of the presentation is to present the report's findings in real time. This presentation may take any form that is helpful to the case, including a question-and-answer session, an oral presentation, a multimedia presentation, or expert witness testimony. If the hypothesis is questioned, you must provide evidence to support it as part of your presentation. Therefore, the person making the hypothesis presentation should study the topic and the know-how report.

2.5 Critical Comparative Evaluation of Existing Digital Forensic Readiness Models/Frameworks

The reviewed Digital Forensic Readiness (DFR) models and frameworks, as well as IoT forensic models, have significantly advanced forensic investigations in distributed computing environments. However, despite their contributions, several limitations remain regarding scalability, automation, organisational integration, and practical applicability within modern IoT-enabled organisations.

The Forensic-Aware IoT (FAIoT) framework proposed by Zawoad and Hasan (2015) focused primarily on evidence preservation and provenance management within IoT ecosystems. The framework introduced mechanisms for protecting digital evidence through secure storage and controlled access. While this represented an important contribution to forensic evidence management, the framework largely focused on the preservation of technological evidence and did not address broader organisational readiness requirements, such as governance, policies, roles and responsibilities, and forensic planning processes. Furthermore, the framework was not aligned with ISO/IEC 27043 and provided limited support for large-scale organisational deployment.

Similarly, the Forensic Investigation Framework (FIF) proposed by Hossain et al. (2018) utilised blockchain technology to enhance the integrity, confidentiality, and non-repudiation of evidence. Although blockchain improves trustworthiness and tamper resistance, the framework primarily addresses evidence storage after collection and does not comprehensively address proactive readiness activities such as continuous monitoring, evidence identification, forensic planning, or organisational preparedness. In addition, the computational overhead of blockchain technologies may pose scalability challenges in large-scale IoT environments where thousands of devices continuously generate data.

Makura et al. (2021) proposed a Digital Forensic Readiness Framework aligned with ISO/IEC 27043. This work advanced the field by introducing standardised readiness processes and recognising the importance of pre-incident planning. However, the framework was developed primarily for cloud-based environments and did not fully address the complexities of IoT ecosystems, including heterogeneous devices, distributed evidence sources, real-time monitoring requirements, and dynamic network topologies. Moreover, the framework remained largely conceptual and lacked empirical validation within operational organisational environments.

The Ready-IoT framework, introduced by Sadineni et al. (2021), focuses on collecting provenance information and network traffic data for forensic investigations. While the framework improved visibility into network events and supported evidence

collection, its primary emphasis remained on network-level monitoring. The framework provided limited capabilities for attack detection, forensic automation, evidence correlation, and organisational readiness processes. Consequently, its ability to support comprehensive forensic investigations across complex IoT infrastructures remains constrained.

A common limitation identified across existing frameworks is the absence of an integrated approach that combines organisational readiness, technical evidence generation, security monitoring, and automated forensic analysis within a single architecture. Most frameworks focus on individual aspects of forensic readiness, such as evidence storage, provenance collection, or forensic process guidance, without addressing the complete forensic readiness lifecycle required by organisations operating IoT-enabled environments.

The proposed Adaptive Proactive Readiness Model (APRM) advances beyond these limitations in several important ways. First, APRM adopts a multi-layered architecture comprising Organisational Readiness, Technical Readiness, and Security Readiness. This enables the model to address governance, policy development, evidence management, monitoring infrastructure, and forensic investigation processes within a unified framework. Unlike previous approaches, the model explicitly incorporates organisational requirements alongside technical controls.

Second, APRM improves scalability by supporting distributed evidence collection across multiple IoT devices, endpoints, servers, and network infrastructures. Through the integration of Wazuh and Splunk, the model enables centralised aggregation, correlation, and management of forensic artefacts generated from heterogeneous environments. This capability is particularly important for modern organisations where evidence is generated by geographically dispersed, resource-constrained IoT devices.

Third, the proposed model introduces a greater degree of automation compared with existing frameworks. Automated evidence collection, real-time event monitoring, file integrity monitoring, log correlation, attack detection, and forensic data preservation

reduce investigator workload while improving the speed and consistency of evidence acquisition. The incorporation of machine learning techniques further enhances readiness by enabling automated threat identification and the prioritisation of forensic evidence.

Fourth, APRM is specifically designed for IoT-enabled organisational environments. Unlike many existing models that were developed for cloud systems, smart homes, or conceptual forensic scenarios, the proposed model addresses the unique characteristics of organisational IoT deployments, including device heterogeneity,, distributed data generation, evidence volatility, and operational complexity.

Finally, the proposed model distinguishes itself through practical implementation and experimental validation. While many existing frameworks remain theoretical or conceptual, APRM was implemented in a controlled organisational environment and evaluated against real-world attack scenarios, including brute-force attacks, denial-of-service attacks, and file integrity monitoring events. This empirical validation demonstrates not only theoretical compliance with ISO/IEC 27043 but also practical effectiveness in supporting digital forensic readiness. Therefore, the proposed APRM extends existing forensic readiness research by providing a scalable, automated, standards-aligned, and practically validated model that supports proactive digital forensic readiness in contemporary IoT-enabled organisations.

Table 3 demonstrates that although previous models/frameworks contributed important capabilities in evidence preservation, provenance collection, and forensic process guidance, none simultaneously provide ISO/IEC 27043 compliance, organisational readiness integration, automated evidence management, scalability, and empirical validation in IoT-enabled organisational environments. These combined capabilities constitute the primary advancement of the proposed APRM.

Table 3: Comparative Table of Previous Models / Frameworks vs Proposed APRM

Framework	ISO/IEC 27043 Alignment	Organisational Readiness	Automation	Scalability	IoT Suitability	Practical Validation
FAIoT (2015)	No	Low	Low	Medium	Medium	No
FIF (2018)	No	Low	Medium	Low	Medium	Limited
Makura et al. (2021)	Yes	Medium	Low	Medium	Medium	No
Ready-IoT (2021)	No	Low	Medium	Medium	Medium	Limited
Proposed APRM	**Yes**	**High**	**High**	**High**	**High**	**Yes**

2.6 The Gap in the Literature

Cybersecurity issues in IoT-enabled enterprises and forensic investigative analysis are both extensively covered in the literature study. Nonetheless, there may be opportunities for further research. There is a need for a more substantial inquiry into the overlap between IoT security issues and forensic investigation than the paper presents. It would be helpful to explore methods for developing IoT-specific forensic procedures that address the unique challenges posed by IoT devices and environments. The technological components of cybersecurity and forensics are the primary emphasis of the literature study. Further insight into the topic could be gained by incorporating legal and ethical factors, such as data protection legislation, the chain of custody, and the admissibility of digital evidence in court. The review briefly discusses emerging technologies such as blockchain and deep learning in the context of cybersecurity. Understanding how these tools can be utilised to enhance forensic analysis, threat identification, and incident response in IoT ecosystems would be incredibly beneficial.

However, the evaluation might benefit from a deeper examination of the human factors contributing to cyber risks, particularly by emphasising training and awareness initiatives. Examples include the psychology of successful cyberattacks, social engineering methods, and user behaviour. While this evaluation provides some insight into the value of cybersecurity education and awareness programmes, additional in-depth research that quantifies the impact of different training approaches on actual security improvements would be helpful for businesses. The assessment touches on several regional approaches to cybersecurity. Still, comparing their relative merits and shortcomings, along with the difficulties inherent in

implementing them, would help paint a more complete picture. A more comprehensive approach to the security of Internet of Things devices throughout their lifecycles is warranted, given the specific threats they pose at each stage: development, production, distribution, and eventual disposal. The literature study could be strengthened by exploring interdisciplinary methods that draw on knowledge from multiple disciplines to address the complex challenges of IoT security and forensics.

Although forensic investigation is highlighted in this assessment, greater attention should be paid to real-time forensic analysis methods that enable businesses to respond quickly to incidents and minimise damage from cyberattacks. Exploring human-centric approaches to IoT security, such as usability, user-centred design, and user-driven security settings, may help increase end-users' security knowledge and behaviour, given the growing prevalence of IoT devices in daily life. By addressing these potential gaps and delving deeper into these areas of study, future research may contribute to a better understanding of the challenges, solutions, and strategies in cybersecurity for IoT-enabled enterprises and forensic investigative analysis.

The literature review explores the complex web of cybersecurity threats facing IoT-enabled businesses and the crucial role of forensic investigative analysis. The digital age has ushered in unprecedented connectivity, but it has also increased vulnerability for individuals and organisations to various cyber dangers. The significance of strong cybersecurity measures has grown as the world becomes more interconnected. To safeguard private data, critical infrastructure, and stakeholders' confidence, this analysis underscores the importance of preventive cybersecurity strategies, IT security risk assessments, and the development of resilient cybersecurity policies. With the proliferation of IoT devices, security challenges and complexity have expanded. As the number of potential attack vectors increases with the proliferation of connected devices, understanding the specific risks of IoT ecosystems becomes essential. This review highlights the value of risk assessment in hybrid data centres, emphasising its vital role in maintaining the safety and reliability of time-sensitive operations. It also shows that, due to the dynamic and diverse nature of IoT environments, conventional security approaches may be inadequate and may require alternative risk-evaluation

techniques. The study further emphasises the importance of education and awareness in preventing cybercrime. To reduce risks stemming from human errors and negligence, training personnel within organisations and the wider public about cyber threats and best practices is crucial. Within e-commerce supply chains and IoT-enabled environments, the review emphasises the growing need for government involvement in addressing cybersecurity issues. Governments continue to face challenges in balancing regulation with innovation, striving to develop frameworks that promote cybersecurity without hindering technological progress.

The paper also highlights the importance of employing deep neural networks, blockchain, and other emerging technologies for cyber threat identification and monitoring. These innovations have the potential to dramatically improve the efficiency of detecting and countering cyber threats. Integrating technology, however, must continue to be guided by ethical and legal issues. The literature study illustrates the complex cybersecurity concerns IoT-enabled businesses face. It stresses the need for a comprehensive strategy that considers not just technology but also people, the law, and policy. The ever-changing nature of threats necessitates the development of novel preventative and reactive solutions. Organisations, politicians, and academics may all benefit from a more secure and resilient cyber environment if they invest in future research into the identified gaps and areas of inquiry.

Across all the models/frameworks explored, the proposed methods must be further tested in real-world applications to verify the theoretical claims made by different authors (Kebande et al., 2020; Makura et al., 2021). The brief literature indicates research activity on conceptual models and theoretical solutions for forensic IoT, with little emphasis on practical Digital Forensic Readiness (DFR) scenarios in organisations. However, it was noted that there is a need for readiness processes in IoT frameworks and IoT security mechanisms to support forensic processes in organisations. DFR processes have been discussed in the ISO/IEC 27043 international standard as readiness processes (ISO, 2015). This standard emphasises the importance of using standardised procedures when conducting readiness assessments. Therefore, this research will use the ISO/IEC 27043 standard to develop the Digital Forensic

Readiness Model. The existing literature provides extensive coverage of IoT security mechanisms, digital forensic investigation techniques, and a range of conceptual forensic-readiness models. Prior studies have examined IoT vulnerabilities, challenges in acquiring evidence, and post-incident forensic procedures in detail, while others have proposed theoretical readiness frameworks to improve investigative preparedness. However, these bodies of work remain largely fragmented, treating security, forensics, and organisational readiness as separate concerns rather than as integrated components of a unified forensic readiness capability.

Notably, few studies present a holistic Digital Forensic Readiness solution that is simultaneously aligned with an internationally recognised forensic standard, explicitly tailored to IoT-enabled organisational environments, and validated through practical implementation. Many existing models/frameworks lack alignment with ISO/IEC 27043, limiting their applicability to legally sensitive investigations, while others remain at a conceptual level and do not demonstrate how readiness processes can be operationalised within real-world organisational infrastructures. Furthermore, organisational dimensions such as governance, policy integration, and chain-of-custody management are often underrepresented, despite their critical role in ensuring evidential integrity and legal admissibility.

Additionally, current research provides limited support for real-time evidence generation and prioritisation within IoT environments, where evidence is highly distributed, dynamic, and potentially volatile. The lack of operational validation using realistic attack scenarios further hampers organisations' ability to assess the effectiveness, scalability, and practicality of proposed readiness approaches. These gaps collectively emphasise the need for a standards-aligned, organisationally grounded, and empirically validated Digital Forensic Readiness Model that integrates technical, security, and governance processes. Addressing these limitations, the present research develops and validates an ISO/IEC 27043–aligned Digital Forensic Readiness Model that supports real-time evidence handling, organisational integration, and operational evaluation within IoT-enabled organisational contexts.

2.7 Chapter Summary

This literature review analyses current Digital Forensic Readiness (DFR) models/frameworks and raises questions about the emergence of the Internet of Things (IoT) in relation to cybersecurity and forensic examination. It outlines the history of digital forensics, highlighting how the advent of IoT has introduced new technical and operational challenges, including diverse device types, varied data formats, and resource constraints. The review also examines the extent to which current forensic models address these challenges, particularly the incorporation of forensic readiness into IoT systems. To this end, it highlights the need for specific best practices that forensic practitioners can follow in response to incidents in IoT ecosystems and notes the lack of customisation of existing frameworks used to manage future incidents.

3.0 Research Methodology

3.1 Introduction

This chapter presents and discusses the research paradigm and methodology underpinning this study, with a focus on the rationale for the chosen approach. This section explains the methodology used to investigate the research aims and objectives. Research methodology is the practical approach to collecting, interpreting, and analysing data. It is defined as methods that describe objectives, manage data, and communicate research results within established processes and existing guidelines. These methods and techniques guide researchers on what to examine, how to conduct the research, and what inferences can be drawn from the collected data (Williams, 2007). The choice of research method also depends on the nature of the proposed research questions or problems, the researcher's personal experience, and the research's target audience (Creswell, 2009). There are three primary research methods: quantitative, qualitative, and mixed (Creswell, 2009; Williams, 2007). The author applies a quantitative methodology for this study. In addition, the literature review provides the necessary background for this study.

3.2 Research Paradigm

In selecting the appropriate methodology for this research, the author reviewed various paradigms and chose the most suitable. A paradigm is an essential collection of beliefs scientists share and agreements about how problems must be understood (Rahi, 2017; Cassell, Cunliffe and Grandy, 2018, pp. 17–32). These concepts include the beliefs and thoughts that guide the investigation of a particular topic. Given this, some suggest that the best way to interpret good research is to adopt a scientific approach. This is important because choosing a particular paradigm will not constrain the researcher by their current knowledge and will enable a better understanding of alternative approaches (Rahi, 2017). Paradigms can be categorised along several key dimensions, including ontology, which refers to whether "reality" represents the objective existence of personal experience or the product of one's subjective consciousness; epistemology, the study of knowledge about the world and how it came to be and how such knowledge can be transmitted among human beings; and methodology, which addresses whether the researcher focuses on identifying and

verifying the relationships and regularities between the various elements, or analysing individuals' subjective experience and interpretation, of the world (Cassell, Cunliffe and Grandy, 2018, pp. 17–32). Four main paradigms are commonly used in information system research: Positivism, Pragmatism, Constructivism, and Critical (Rahi, 2017). The author applies the Pragmatism paradigm for this study.

The pragmatism paradigm combines interpretivism and Positivism (Rahi, 2017; Žukauskas, Vveinhardt and Andriukaitienė, 2018). This paradigm aims to identify research weaknesses and strengthen them using a combination of methods. Proponents of this paradigm believe that actual knowledge can be achieved through a combination. The process is not essential; the problem is paramount, and the researcher must use all available methods to understand the problem context. Pragmatism does not involve any system or theory; scholars can use both quantitative and qualitative. The important thing is to find the best research and methods to solve the problem statement (Rahi, 2017; Žukauskas, Vveinhardt and Andriukaitienė, 2018). Pragmatism emphasises the importance of consequences and focuses on what works in the situation. When applied to qualitative methods, pragmatism recognises multiple scientific perspectives and aims to use the best methods to answer research questions and solve real-world problems (Žukauskas, Vveinhardt and Andriukaitienė, 2018). The pragmatism paradigm provides a pragmatic approach to studying Digital Forensic Readiness (DFR) in real-time scenarios. Pragmatism emphasises practicality and focuses on what works in real-world situations. In the context of DFR, this paradigm aims to develop actionable models and strategies that organisations can apply immediately during digital security incidents. The pragmatism paradigm seeks to create a DFR model in real-time scenarios by:

- Understanding the unique environment and real-time cybersecurity challenges organisations face. This includes questioning the subject when an event occurs. Working with emergency responders to understand the unique issues and challenges they face. Focusing on solving the immediate problem and creating a strategy that suits the current situation.

- Developing and testing prototypes of DFR models in real-time. This involves

designing a prototype DFR model based on real-time insights, implementing it during ongoing incidents, continuously gathering feedback from incident responders, and iteratively refining the model based on its effectiveness. This iterative process ensures the model evolves and adapts as real-time incidents unfold.

- Generating practical and actionable recommendations involves developing advice and best practices immediately after observing real-time incidents. Emphasise actionable steps to improve incident response effectiveness and provide real-time training and guidance to incident response teams based on these recommendations.

- Promoting collaboration between technical and non-technical teams. This encourages cooperation among IT, legal, HR, and management teams during incidents. It helps to understand how these cross-disciplinary efforts influence incident responses and to develop strategies that enable effective real-time communication and coordination among diverse teams.

- Using real-time data analytics for decision-making involves implementing data analytics tools to analyse incident data as it occurs. It assists in providing decision-support systems that deliver actionable insights to incident responders and emphasises real-time data visualisation to facilitate quick decisions. This also allows for the assessment of these tools' effectiveness during live incidents.

- Developing policies and procedures that adapt in real-time involves creating flexible guidelines capable of quick adjustments. This helps evaluate their effectiveness during live incidents, refine them based on outcomes, and establish dynamic protocols that respond to the constantly changing landscape of digital threats.

- Developing feedback mechanisms for ongoing improvement. This involves setting up feedback loops in which incident response teams provide real-time

feedback on the DFR model, which is then used to dynamically adapt it. It promotes adaptive learning within the organisation, where insights from live incidents guide future incident responses.

Applying the pragmatism paradigm in real-time DFR scenarios allows organisations to create models and strategies that are both theoretically robust and immediately practical. This approach guarantees that DFR efforts remain realistic, responsive to real-world challenges, and continuously adapt to the shifting landscape of digital security incidents.

3.3 Quantitative Research Methodology

Quantitative research methodology primarily involves the systematic collection and interpretation of numerical data. It explains, predicts, confirms, validates, or tests theories. Standard quantitative methods include experiments, numerical observations, and surveys with closed-ended questions. Quantitative research refers to the general techniques used when conducting research projects (Leedy and Ormrod, 2001). It emphasises objective measurements and the statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys or by manipulating pre-existing statistical data using computational techniques (Williams, 2007). It is a method for testing objective theories by examining the relationships among variables. These variables can often be measured on the device, allowing statistical methods to analyse the calculated data. The final report contains a solid structure, including an introduction, literature and theory, methodology, results, and discussion (Creswell, 2009).

Quantitative research is vital for creating a digital forensics model because it enables a deeper understanding of the complexities of digital forensics in real time. In real-time systems, digital forensic investigations are ongoing and dynamic, with new evidence and information constantly emerging. Digital forensics is a complex and rapidly changing field, and the opinions of those involved can be influenced by factors such as training, experience, and personal beliefs. Using quantitative methods to develop a digital forensic model helps identify the challenges and opportunities in the field. This provides insight into the factors influencing the success of digital forensics,

as well as potential obstacles and barriers. It ensures the model is based on the real experiences and perspectives of digital forensic investigators. It also helps pinpoint areas where additional training, resources, or support may be necessary. Quantitative research methods offer valuable insights for developing more effective models, tools, and techniques to investigate digital crimes and cyber incidents.

As mentioned earlier, this research will adopt a quantitative methodology for the DFRM in a real-time setting and collect sufficient data for analysis. It explores cybersecurity challenges faced by IoT-enabled organisations and analyses the forensic investigation process. The literature review has discussed and analysed cybersecurity and its organisational challenges; digital forensics and digital forensic readiness; and the process classes (Readiness, Initialisation, Acquisitive, and Investigative) according to the ISO/IEC 27043 Standard, as shown in Figure 16.

In this case, the research problem is to develop and evaluate a digital forensic model that meets the ISO/IEC 27043 security standard in real time. The terms "model" and "framework" are often used interchangeably, but there is a crucial distinction between them. A framework is a conceptual structure that provides a high-level view of a complex system or problem. It is a set of guidelines, principles, and best practices that can guide the development of specific rules, policies, and procedures within a particular domain. A framework provides a common language and shared understanding of the critical components and activities required to achieve a specific goal (Amin, 2013; Hogland, 2016). A model, by contrast, is a more detailed representation of a system or problem. It is a simplified, abstract representation of reality that can be used to explain and predict a system's behaviour. Models are primarily used to conceptualise, visualise, and communicate information technology concepts. They help stakeholders, including developers, designers, and analysts, better understand the system's structure, behaviour, or requirements. For example, a model may include equations, algorithms, or diagrams that describe the relationships among variables or components of the system (Amin, 2013; Hogland, 2016). A framework is a higher-level, more abstract concept that provides an overall structure

for understanding a complex system. At the same time, a model is a more detailed representation of the system that can be used to make predictions or test hypotheses.

In the context of digital forensic readiness, the Digital Forensic Readiness Model (DFRM) is a structured framework that defines the components, processes, policies, and procedures an organisation needs to effectively prepare for and respond to digital incidents and forensic investigations. It provides a systematic approach to enhance an organisation's readiness to handle cyber incidents, ensuring that digital evidence is appropriately collected, preserved, and analysed when necessary (Carrier, 2006). Organisations need a detailed security model to mitigate and prevent risks and attacks, including IT and IoT security processes. IoT device manufacturers do not adhere to standardised security measures or protocols in device design; therefore, additional security procedures and techniques must be implemented in IoT-enabled organisations. An IoT-FR model is developed to test the DFR and verify its performance in IoT forensics. The critical components of a digital forensic model will be analysed, with particular focus on its effectiveness in identifying and analysing digital evidence in real time. This research will analyse cyber threats, attacks, and vulnerabilities affecting IoT devices in organisations, and will help identify solutions to address them. Here, the practical issue of IoT forensics is addressed through a mechanism, DFRM, developed and implemented to demonstrate its effectiveness. The proposed solution will address the problems identified in forensic investigations in IoT-enabled organisations. Since IoT forensics is a challenging area, the proposed readiness model is demonstrated through a prototype to note its performance and effectiveness. The proposed readiness model and prototype will help cybercrime investigators easily acquire and analyse data from IoT devices in real time.

This research employed a quantitative, experimental methodology to design, implement, and evaluate an ISO/IEC 27043-aligned Digital Forensic Readiness (DFR) Model for IoT-enabled organisational environments. The quantitative approach was selected because the study required measurable evaluation of forensic readiness effectiveness, cyberattack detection performance, evidence preservation capability,

and investigation efficiency using experimental data and statistical analysis techniques.

The research methodology combined cybersecurity monitoring, forensic evidence acquisition, machine learning analysis, and controlled cyberattack experimentation within a practical organisational test environment. This methodological approach enabled the study to evaluate both the operational and forensic effectiveness of the proposed model under realistic attack conditions.

The experimental process consisted of four major stages:

1. Design and implementation of the Digital Forensic Readiness Model.
2. Deployment of security monitoring and forensic tools within an IoT-enabled organisational infrastructure.
3. Execution of controlled cyberattack scenarios and forensic evidence acquisition.
4. Evaluation of forensic readiness performance using machine learning analysis and forensic metrics.

The proposed model was operationalised by integrating organisational readiness processes, technical monitoring infrastructure, forensic evidence management procedures, and automated attack detection mechanisms. The implementation environment enabled continuous monitoring, log collection, event correlation, evidence preservation, and forensic investigation support aligned with ISO/IEC 27043 principles.

A controlled organisational laboratory environment was established to simulate realistic IoT-enabled organisational operations. The environment included endpoint systems, network infrastructure, monitoring servers, virtualised systems, and forensic repositories configured to support real-time evidence generation and forensic analysis. Simulated cyberattack scenarios were then executed to evaluate the proposed model's ability to detect attacks, preserve evidence, maintain chain-of-custody integrity, and support forensic investigations.

The quantitative methodology enabled an objective assessment of forensic readiness performance using measurable indicators, including attack detection accuracy, precision, recall, F1 Score, false positive rate, evidence preservation capability, and response efficiency. These evaluation metrics provided empirical evidence regarding the effectiveness of the proposed Digital Forensic Readiness Model.

3.4 Research Tools

To achieve the research objectives outlined in Section 1.3, a quantitative research methodology was adopted for each objective, thereby increasing the likelihood of achieving the required results. The first objective examines current DFR models through an extensive, critical evaluation of the available literature. While conducting the literature review, gaps were identified to accomplish the second and fourth objectives: developing a comprehensive forensic readiness model and a readiness model that incorporates the organisation's IoT applications. To assess the models and verify the effectiveness of the other objectives, the tools below were used:

- **Experimental Design:** The experimental design systematically manipulates variables and assesses their impact on digital forensic readiness outcomes. This involves controlled experiments conducted in real-world environments. It also consists of implementing specific DFR protocols, introducing simulated cyberattacks, or varying the resources allocated to digital forensic readiness.

- **Forensic Tools and Software:** Digital forensic tools (Wazuh and Splunk) were used to gather digital forensic data by experimenting with different configurations and protocols to evaluate their efficiency in handling various types of digital evidence. This includes log files, system snapshots, network traffic data, and metadata collected during forensic examinations. Several security monitoring, forensic analysis, and machine learning tools were utilised throughout this research to implement and evaluate the proposed Digital Forensic Readiness Model.

    - ✓ **Wazuh Security Monitoring Platform:** Wazuh was selected as the primary security monitoring and Host-based Intrusion

Detection System (HIDS) platform because of its real-time monitoring, log collection, file integrity monitoring, threat detection, and forensic event preservation capabilities. Wazuh agents were deployed across organisational endpoints and monitored systems to collect security events, authentication logs, system activities, and Indicators of Compromise (IoCs). The platform also provided automated alert generation and centralised event management required for forensic readiness implementation.The Wazuh environment consisted of four major components: Wazuh Server, Wazuh Indexer, Wazuh Dashboard, Wazuh Agents. These components collectively supported continuous monitoring, event correlation, forensic log preservation, and incident response integration.

- ✓ **Splunk SIEM Platform:** Splunk was implemented as the Security Information and Event Management (SIEM) platform to support advanced log analysis, forensic investigation, evidence correlation, and attack visualisation. Splunk enabled the aggregation and indexing of logs generated from monitored systems and provided investigators with search, analysis, dashboard visualisation, and reporting capabilities. The integration between Wazuh and Splunk strengthened the forensic readiness workflow by enabling real-time event analysis, timeline reconstruction, and evidence examination during cyberattack investigations.

- **Statistical and Machine Learning Analysis:** Statistical and Machine learning analysis was implemented using Python-based data science libraries to evaluate cyberattack detection performance and forensic evidence prioritisation. This involves analysing digital forensic datasets to identify patterns, trends, and statistical correlations. It also examines case resolution time, evidence collection types, and forensic analysis success rates. These

enable descriptive and inferential statistics to test hypotheses and draw conclusions. The experimental environment utilised: Python, Scikit-learn, XGBoost, Pandas, NumPy, Matplotlib.

Four machine learning classification models were selected for comparative evaluation:

- ✓ XGBoost (XGBClassifier)
- ✓ Random Forest
- ✓ Extra Trees Classifier
- ✓ BaggingClassifier

These models were selected for their high classification accuracy, feature importance analysis, robustness to overfitting, and suitability for cybersecurity intrusion detection applications.

- **Experimental Infrastructure:** The experimental environment was configured within a controlled organisational IoT testbed consisting of:
  - ✓ Windows-based endpoint systems.
  - ✓ Monitoring servers.
  - ✓ Organisational network infrastructure.
  - ✓ Virtual machines.
  - ✓ Centralised forensic repositories.
  - ✓ Simulated attacker systems.

  The environment enabled the realistic generation of authentication logs, attack traces, event records, and network activity associated with cyberattack scenarios. This infrastructure supported continuous monitoring, preservation of forensic evidence, and controlled experimental evaluation of the proposed model.

The research methodology adopted in this study is deliberately aligned with the technical, process-driven, and evaluative nature of Digital Forensic Readiness (DFR) in IoT-enabled organisational environments. A quantitative and experimental research approach was selected because the primary objective of the study is not to explore perceptions of readiness, but to design, implement, and empirically evaluate a forensic readiness model under controlled yet realistic conditions. The use of real-

world security monitoring and forensic tools enables objective measurement of forensic readiness capabilities, including evidence generation, preservation, integrity, traceability, and investigative efficiency.

Alternative research approaches were considered during the design phase. Qualitative methods, such as interviews, surveys, or observational case studies, were deemed valuable for understanding organisational attitudes and policies but insufficient for validating the technical effectiveness of forensic readiness mechanisms. Similarly, purely conceptual or simulation-based approaches were not adopted, as they do not demonstrate how forensic readiness processes perform during actual cyber incidents. Given the need to validate the proposed model through operational evidence and measurable outcomes, a quantitative experimental approach was considered the most appropriate and defensible choice.

To ensure validity, the experimental design employs repeatable, well-defined cyberattack scenarios that reflect the realistic threats faced by IoT-enabled organisations. Consistent system configurations, predefined attack parameters, and standardised evaluation metrics are applied across all experiments to ensure that observed outcomes are directly attributable to the proposed DFR model rather than environmental variation. Construct validity is supported by mapping evaluation metrics directly to the research objectives and readiness processes defined in ISO/IEC 27043.

Reliability and reproducibility are addressed through tool-based and automated evidence-collection mechanisms, standardised logging configurations, and documented experimental procedures. These measures ensure that experiments can be repeated under identical conditions and that results can be independently verified. The reliance on widely used, industry-recognised security and forensic tools further enhances the reproducibility and practical relevance of the findings.

Ethical considerations are carefully addressed throughout the research process. All experiments are conducted within controlled laboratory environments, ensuring that no live production systems or external networks are affected. No personally

identifiable information is collected or analysed, and datasets used in machine-learning-based analyses are anonymised where applicable. The research complies with organisational security policies and established ethical research practices.

Finally, the study acknowledges certain methodological limitations. The experimental evaluation is conducted in a controlled environment, which, while necessary for repeatability and safety, may not capture the full complexity of large-scale or highly heterogeneous organisational IoT deployments. Additionally, machine learning techniques are used to support forensic readiness evaluation rather than legal decision-making, and their results should be interpreted as assistive rather than determinative. These limitations are recognised and discussed to ensure transparency and to identify areas for future research.

3.5 Chapter Summary

This chapter has presented the research methodology adopted to investigate Digital Forensic Readiness within IoT-enabled organisational environments. A quantitative research approach was selected to enable objective evaluation of the proposed model through controlled experimentation, data collection, and statistical analysis. The chapter also outlined the research design, experimental strategy, data collection methods, and evaluation procedures used to ensure the reliability and validity of the findings.

Having established the study's methodological foundation, the next stage of the research focuses on the practical implementation of the proposed Digital Forensic Readiness Model. Chapter 4 translates the methodological principles discussed in this chapter into a deployable architecture by presenting the design, components, and implementation of the proposed Adaptive Proactive Readiness Model (APRM). It further describes the organisational, technical, and security layers of the model, together with the experimental environment used to support subsequent forensic readiness evaluation.

4.0 Research Design

4.1 Introduction

The research methodology presented in Chapter 3 established the foundation for the development and evaluation of the proposed Digital Forensic Readiness Model. Building upon that methodological foundation, this chapter focuses on the practical implementation of the research by transforming the identified requirements, design principles, and readiness objectives into a functional model.

The chapter therefore serves as a bridge between the study's theoretical and methodological aspects and the experimental evaluation presented later. It introduces the Adaptive Proactive Readiness Model (APRM), explains its organisational, technical, and security components, and describes the system architecture and implementation environment developed to support forensic readiness within IoT-enabled organisational settings.

In an era dominated by the Internet of Things (IoT), where connected devices communicate and exchange information seamlessly, organisations face unprecedented business and innovation situations. However, this interaction presents new challenges, particularly in cybersecurity. As the digital environment evolves, there is an increasing need for digital forensics to ensure the security and integrity of data in IoT-enabled organisations. This research aims to explore and develop a comprehensive approach to digital forensics design, specifically for organisations within the IoT ecosystem. Digital forensics readiness encompasses an organisation's preventive measures and strategies for responding to cyber incidents, reducing risk, and preserving digital evidence for investigative purposes.

Integrating IoT devices presents unique challenges and disadvantages that require specialised methods for preparing digital certificates. The large volume and variety of data generated by IoT, coupled with the high standards of these devices, demand new methods and techniques for forensic investigations. This research seeks to bridge the current gap in understanding and application by offering a model for developing effective digital forensic planning strategies within the IoT environment. Investigating this issue is crucial to safeguarding critical information within organisations and

maintaining trust across the wider ecosystem. Organisations can strengthen their cybersecurity by establishing a robust digital forensics framework, ensuring regulatory compliance, and reinforcing their defences against emerging threats.

In the next section, we will describe the main aspects of our proposed model, research design, and experiment, including identifying IoT-specific digital forensics challenges, developing a preparation plan, and validating our findings through real-world applications and a data mining strategy. Through this research, we aim to offer insights into the development of digital forensics and foster a safer environment for organisations managing complex IoT systems.

4.2 Proposed DFR Model for IoT Environments

The proposed model, which integrates various processes, is shown in Figure 16. It will involve the organisation's and the IoT system architecture's readiness to develop security policies and procedures. The management of the IoT architecture will include policies and procedures for monitoring data flow during application operation, incident detection, data breach monitoring, and comprehensive risk identification and mitigation, all of which will be incorporated into the organisation's overall cybersecurity and forensic readiness model.

As an initial step towards a DFR model, the organisation must ensure that IoT architecture processes adhere to the ISO/IEC 27043 standards. The IoT architecture includes the organisation's system architecture, information systems, infrastructure, and the network perimeter, endpoints, software, and data. The architecture details will identify information sources within the organisation's Information System (IS). The data component of the IoT architecture is crucial to supporting the readiness processes outlined in the ISO/IEC 27043 standard. The Digital Forensic Readiness Model is based on processes such as readiness, initialisation, acquisition, and investigation. Each of these key processes will incorporate steps for the organisation to follow, as shown in the model diagram (Figure 16).

In digital forensics within IoT environments, preparing for potential incidents in advance is crucial for effective response and mitigation strategies. Several techniques

have been identified for achieving digital forensics readiness (DFR) in IoT-based environments. These forensic techniques focus on collecting past information using tools to trace data, which can provide clues about the attack or damage. Many digital forensic tools are available, including EnCase, FTK Imager, and Autopsy.

Digital forensic tools trace data across all devices compromised by a breach. The forensic process involves identifying devices for investigation, preserving all relevant data from these devices, and analysing, documenting, and reporting the findings. For example, techniques used in environmental monitoring are considered. Systems such as ZigBee are employed. ZigBee is an IoT sensor monitoring protocol that uses sensors to record light, humidity, and temperature levels. This environmental data is collected by wireless sensors, transmitted, and incorporated into the organisational network for use in applications. The received data is then used in further processing or to analyse environmental conditions. In this scenario, if any IoT device is compromised, data security can be at risk, especially in the absence of sufficient security measures. Digital forensics will identify compromised devices and utilise this information to gather additional evidence about the breach. Since IoT devices transmit data packets, monitoring these devices is of paramount importance. The data sent or received can offer insights into device interactions with other devices (such as Wi-Fi routers, IoT devices, and computers) and may highlight potential attacks.

Monitoring IoT network protocols and services is essential for detecting potential issues early and gathering evidence. By overseeing Wireless Sensor Networks, investigators can collect detailed data on IoT network functions, which aids in digital forensic analysis. An Intrusion Detection System monitors IoT devices and networks, alerting administrators promptly when a possible intrusion occurs. Additionally, the False Alarm Detection technique can optimise incident detection. These methods help organisations enhance their preparedness and respond effectively to cyber incidents, thereby reducing the impact of cyber threats.

The readiness process involves several functions that prepare for forensic investigations. These functions include forensic logging, log parsing, preservation, storage, analysis, and characterisation. Forensic logging gathers digital information

for analysis. Log parsing extracts key events from the logs. Log preservation ensures information integrity by creating hash values. This data is stored in a forensic database for verification and analysis. Log analysis helps detect security incidents within the collected data. Log characterisation categorises the logs. The readiness report supports achieving outcomes by implementing readiness processes. These guidelines, techniques, processes, and reporting stages aim to prepare IoT-based environments for forensic investigations.

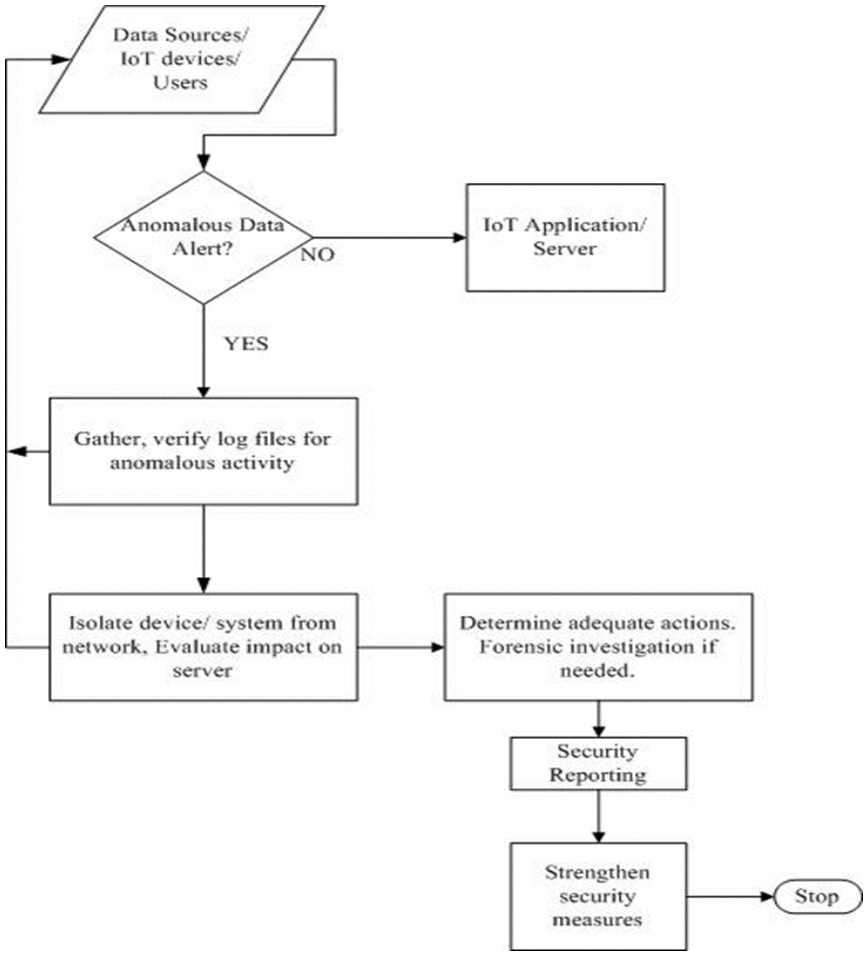

Figure 14: Flowchart of the forensic IoT process.

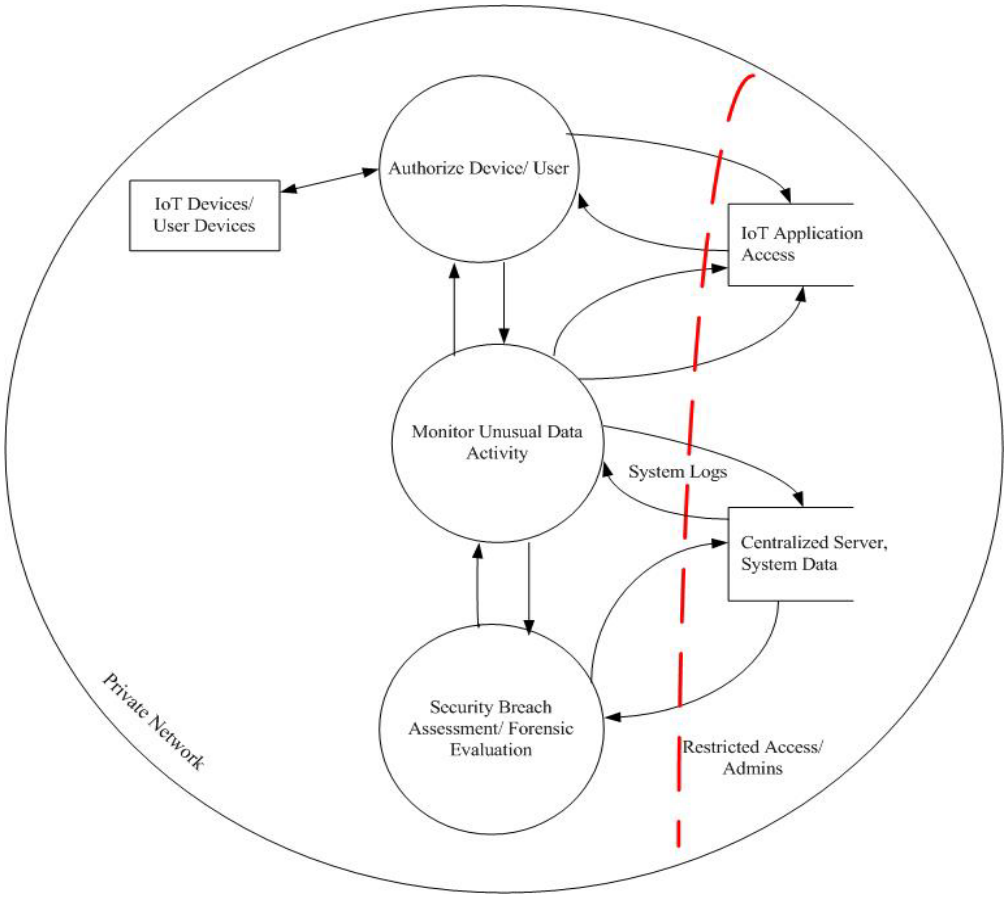

Figure 15: Data Flow Diagram

Data is collected from the DFRM; logs are monitored in real time by the forensic tool for anomalies or unusual activity (incidents); alerts are generated for incident response; observations are made during the scenario; and relevant documents, such as legal or regulatory guidelines, are followed. Given these aspects, a forensic readiness model for IoT-enabled organisations is conceived and developed. The model's process flowchart is shown in Figure 14.

The data flow diagram in Figure 15 depicts the IoT data flow. Initially, IoT devices must undergo authentication and authorisation to access the IoT application and database. During authorisation, all incoming data is monitored for anomalies or unusual activity that could prompt a series of investigative actions. The digital forensic readiness processes facilitate monitoring in accordance with ISO/IEC 27043. When any anomaly or breach is detected, forensic assessment processes are triggered to perform a comprehensive investigation. Any unusual activity is reported to the administrators during the authorisation phase. Common breach scenarios include

brute-force attacks, man-in-the-middle (MITM) attacks, or distributed denial-of-service (DDoS) attacks.

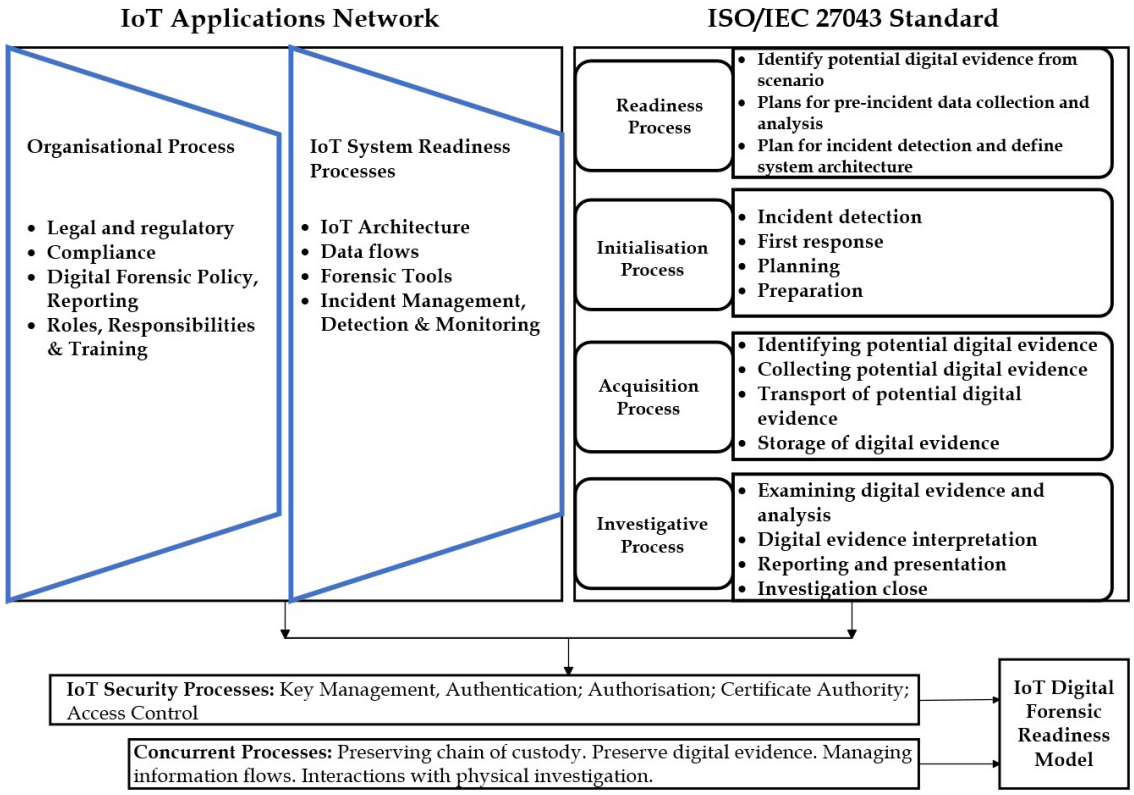

Figure 16: Proposed IoT Digital Forensic Readiness Model

The model, which shows how different processes connect, is shown in Figure 16. The proposed model will include the organisation's and IoT system's readiness processes to develop security procedures and policies. Managing the IoT architecture will involve policies and procedures for monitoring data flow during application operation, incident detection, data breach monitoring, and overall risk detection and mitigation, all integrated into the organisation's cybersecurity framework. The organisation must ensure IoT architecture processes follow the ISO/IEC 27043 standards. The IoT architecture includes the organisation's system architecture, information systems, infrastructure, as well as the network perimeter, endpoints, software, and data. These details will provide information sources within the organisation's information systems. The data aspect of the IoT architecture is crucial for enabling the readiness processes specified in the ISO/IEC 27043 standard. The Digital Forensic Readiness Model covers readiness, initialisation, acquisition, and

investigation. Each of these key processes will have steps for the organisation to follow, as shown in the readiness model diagram in Figure 16.

The Digital Forensic Readiness (DFR) model for IoT environments is designed to address the complexities of interconnected IoT ecosystems across organisational, technical, and security layers, as shown in Figure 17. The organisational layer establishes a platform for incident readiness, covering risk identification, incident planning, communication standards, and ISO/IEC 27043 practices for globally accepted evidence handling and documentation, with a focus on preparedness and prevention. The technical layer concentrates on integrating specific IoT mechanisms, such as device monitoring, data authentication, traffic analysis, and forensic tools, to automate the collection and processing of evidence from large, diverse datasets.

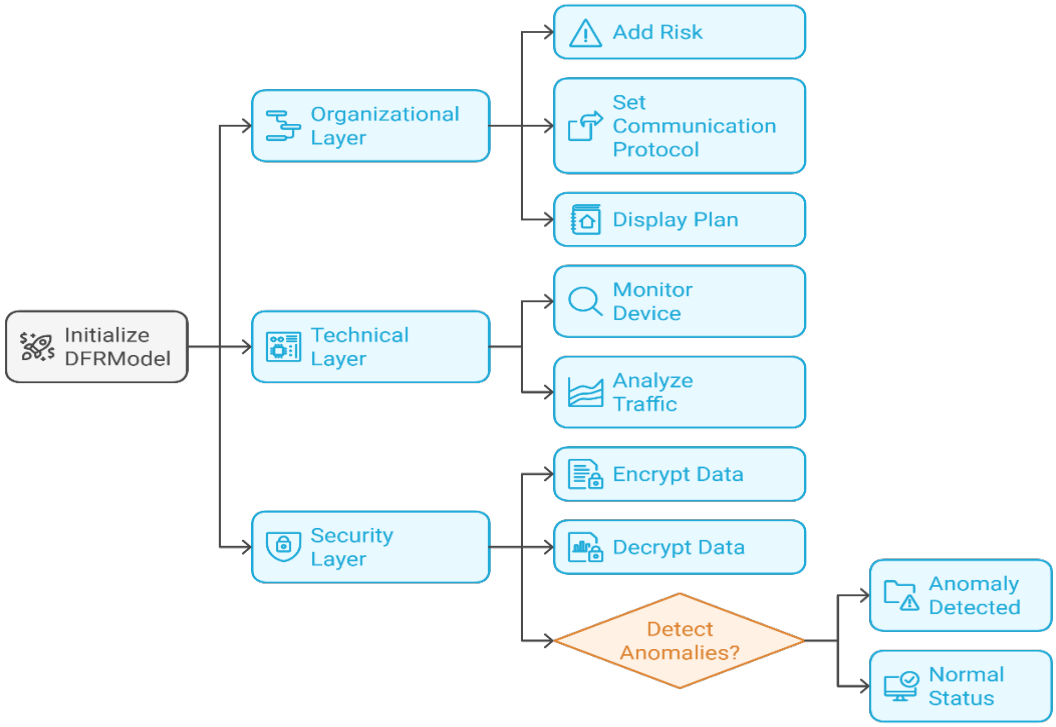

Figure 17: Architecture of DFR Model

Complementing this is the security layer, which enhances the ecosystem through encryption, integrity verification, and automated anomaly detection via machine learning, proactively reducing vulnerabilities and maintaining data integrity. Together, these three layers form a scalable and robust framework that provides an environment prepared for forensic examination in highly complex scenarios, supports

effective evidence management, and optimises timely responses to cyber incidents in challenging IoT environments.

4.2.1 Organisation Layer

The organisational layer represents the governance and management foundation of the proposed Digital Forensic Readiness (DFR) model. Its primary role is to ensure that forensic readiness is embedded within organisational policies, procedures, and responsibilities rather than treated as an ad hoc technical activity. This layer addresses challenges in accountability, legal compliance, and decision-making by defining roles and responsibilities, escalation procedures, and evidence-handling policies aligned with ISO/IEC 27043. In IoT-enabled organisations, where evidence sources span multiple departments and systems, the organisational layer ensures coordination among technical teams, management, and legal stakeholders, thereby supporting consistent, defensible forensic processes.

The organisational level of the proposed Digital Forensic Response (DFR) model assesses an Internet of Things (IoT)- based organisation's readiness to respond to cybersecurity incidents. Incident readiness is achieved through pre-incident planning, during which risks within the internet-connected ecosystem are identified and assessed. Potential threats to connected devices, networks, and data, as well as vulnerabilities that could be exploited, must be identified and studied. Risk identification also includes identifying potential attack vectors and how the conceived threats would affect various IoT devices and systems. Once these risks are understood, organisations can develop refined communication protocols to facilitate quick, efficient coordination among internal teams, external stakeholders, and law enforcement in the event of an incident. It streamlines the response process, ensuring everyone is aware of the protocols being followed.

Furthermore, this layer ensures that the organisation's forensic procedures comply with the international standard ISO/IEC 27043, which provides a framework for the collection, handling, and documentation of evidence in forensic investigations. These global standards must be followed to maintain an unbroken chain of evidence, ensuring that it is not faulty, unalterable, or inadmissible in a court of law. Properly

documented, this evidence comprises a chain of collection, preservation, and custody to ensure tamper-proof reconcilability, thereby securing its worth in investigations and prosecutions. If standards for evidence handling align with incident readiness, the organisational layer ensures that responses to any IoT-related incidents are effective, synchronised, and legally sound.

4.2.2 Technical Layer

The technical layer operationalises forensic readiness by enabling the systematic generation, collection, and preservation of evidence across IoT devices, networks, and supporting infrastructure. This layer addresses the challenge of heterogeneous and distributed evidence sources commonly found in IoT environments. By integrating monitoring agents, logging mechanisms, and evidence storage processes, the technical layer ensures that potential digital evidence is captured in a structured and forensically sound manner. It supports the preservation of evidence integrity and traceability, enabling timely forensic analysis while minimising disruption to organisational operations.

The proposed technical aspects of the DFR address a relatively new dimension of issues: the investigation and security of IoT environments. The DFR addresses its IoT-specific mechanisms, in which security is not merely about monitoring devices, data, or traffic, but also extends to networked devices by fine-tuning device monitoring to detect abnormal behaviour, unauthorised access, or malicious activity. This further underscores the importance of monitoring and tracking IoT device activity. It provides a means to ensure that every device is continuously monitored, enabling early detection of tampering, malfunctions, or security breaches. IoT device data is authenticated at a much greater scale than the data generated and transmitted by IoT devices, and must be verified against specifications for accuracy and integrity. It ensures that data recorded during an incident is genuine and has not been altered or compromised, making it the most critical step in preserving the integrity of the evidence. Another factor that enhances security is traffic analysis, which involves analysing network traffic to detect anomalous or suspicious patterns that may indicate cyberattacks, such as distributed denial-of-service (DDoS) attacks or data exfiltration

attempts. Since this enables the construction of a data flow model, investigators can analyse it to detect anomalies and, consequently, trace potential security breaches.

It has built-in advanced tools for efficient evidence collection and analysis, which, along with IoT-specialised mechanisms, form the technical layer. These tools are designed to manage enormous and diverse datasets generated by IoT devices, thereby improving the efficiency and thoroughness of forensic processes. For example, specialised forensic software can automatically gather logs, device data, and network traffic, reducing human error and ensuring timely, systematic evidence collection. Advanced analysis tools will enable investigators to quickly scan data for patterns, correlate events, and identify critical data points that can provide insights into the incident after data collection. These tools will support professional analysis of both structured and unstructured data to assist complex investigations in IoT systems. All of these mechanisms and tools, as depicted here, constitute the technical framework of the DFR model, ensuring that evidence remains unchanged during IoT incident investigations and is accurately addressed.

4.2.3 Security Layer

The security layer focuses on real-time detection, monitoring, and response, serving as the trigger for forensic readiness processes. It addresses the challenge of identifying security incidents early enough to preserve volatile evidence in IoT environments. Through continuous monitoring and alerting mechanisms, this layer ensures that suspicious activities are detected promptly and that forensic processes are activated in accordance with predefined readiness procedures. Importantly, the security layer is not limited to attack detection; it also enables forensic readiness by ensuring that detected events are recorded, contextualised, and preserved for subsequent investigation. The DFR model proposed here has at its core a security layer with special provisions to address the exceptional vulnerabilities and risks consistently raised in IoT settings. An essential policy in this layer is the encryption policy to protect against malicious parties exploring IoT-generated and communicated data, as well as IoT devices. IoT ecosystems are of most concern, as a single device compromise may endanger an entire network. While encryption is somewhat less critical, integrity

verification, the process that ensures data has not been altered during its lifecycle, is much more significant. The use of hash functions and digital signatures in data integrity verification provides a means of demonstrating, in forensic investigations, that the information used was not manipulated and thus remains admissible in court. Another element of the layer is automated anomaly detection, which applies machine learning to identify potential abnormal or malicious activity on IoT devices and networks. One IoT device generates such vast amounts of data that no amount of automated monitoring can adequately capture. Malware and other potential attacks on the device, unauthorised access by the offender, or device malfunctions can also be detected by machine learning models that recognise patterns of typical device usage. These models are self-developed and learn in parallel in real-world environments, resulting in improved detection of initially ignored or underreported threat types. When combined with ADS, the security layer also becomes more preventive, increasing the speed and accuracy of threat detection and incident response times. These strategies, in their own right, form an impressive framework for messaging and managing IoT-specific threats. Together with encryption and integrity verification, they secure data confidentiality and reliability and improve automated, real-time anomaly-based identification and responsive remediation of security threats. This approach therefore represents a general enhancement to the security framework of IoT spaces, in addition to forensic analysis.

Digital forensic readiness (DFR) is an emerging requirement and urgent necessity for IoT-based enterprises. Besides managing cyber threats, it helps safeguard valuable assets and comply with the ITRs of multiple agencies. The increasing complexity and size of IoT ecosystems introduce unique challenges, such as high-volume data, diverse device types, and more advanced cyber threats. In this context, a DFR strategy can assist organisations in detecting, responding to, and investigating incidents with minimal disruption to their operations. Incorporating internationally recognised standards, such as ISO/IEC 27043, into DFR processes ensures a more standardised approach to handling and documenting evidence. These standards offer proven, structured approaches for collecting, preserving, and presenting digital evidence, ensuring its admissibility in court and enhancing organisational accountability.

Advanced forensic tools, such as Wazuh and Splunk, along with blockchain technologies, can further enhance forensic capabilities by facilitating real-time monitoring and anomaly detection, secure evidence storage, and more effective management of distributed IoT networks.

The proposed Digital Forensic Readiness Model explicitly addresses the unique challenges of IoT. This model is comprehensive and can be easily expanded to include additional layers, as it already encompasses an organisational layer for establishing the general firewalls and plans of an organisation, a technical layer specific to Iot mechanisms, and a security layer that employs encryption for data encoding and machine learning for anomaly detection. The DFR assists IoT-enabled organisations in better understanding and managing the complexities of digital forensics in current ecosystems through tools and methodologies. When strategically planned and best practices and emerging technologies are integrated, they offer significant opportunities to improve organisational forensic readiness, protect against cyber threats, and maintain the integrity of the digital environment.

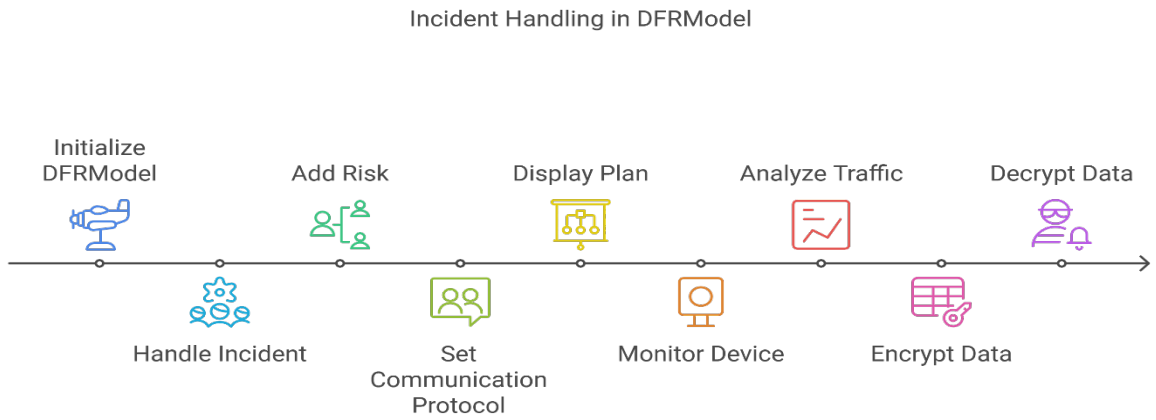

Figure 18: Incident Handling in DFR Model

Each layer of the proposed Digital Forensic Readiness (DFR) model addresses a specific yet interconnected challenge in preparedness within IoT-enabled organisational environments. The organisational layer ensures governance, policy alignment, and accountability; the technical layer facilitates the systematic creation, preservation, and traceability of evidence; and the security layer supports real-time detection and response, including forensic processes. Collectively, these layers ensure

evidence integrity, chain-of-custody compliance, and ongoing forensic readiness, enabling organisations to shift from reactive investigations to proactive, compliant forensic preparedness within complex IoT ecosystems.

4.2.4 Incident Response

Incident response is a structured process that enables a firm to detect, contain, and mitigate the effects of a cyber threat on its business interests, reputation, and tangible assets. It provides a strategic framework for addressing an organisation's security threats, including, but not limited to, data leakage, malware attacks, and internal threats. The main goal of incident response is to reduce the impact of incidents, restore affected systems, and prevent future occurrences(Nugroho et al., 2023).

4.2.4.1 Key Phases of Incident Response

The initial stage of the incident response process is preparation, where key elements of the incident response plan, roles and responsibilities, and the tools and methods required to detect and manage the incident are established (ManageEngine, 2024). This stage also involves training staff through education, tabletop exercises, and drills, as well as updating relevant documents. The following stage is detection and analysis, which entails continuously monitoring systems to identify activities that might indicate security threats. In this stage, the scope, types, and impacts of attacks are identified using tools such as IDS, log analysers, and forensic tools. The containment stage involves efforts to stop the incident from spreading to other systems or networks. Solutions may be applied temporarily during this stage while evidence is collected for further investigation. The eradication stage involves removing the source of the incident. This includes deleting the virus or closing the vulnerability that the threat exploited, ensuring the threat is fully eliminated. Afterwards, the recovery stage involves restoring systems to normal operation, replacing damaged components, and applying necessary patches and updates. It also includes verification to confirm there are no signs of the attack, followed by monitoring to prevent recurrence. Finally, a post-incident review is conducted, during which important data on the event, its origins, and the effectiveness of the response are recorded. The insights gained during

this phase help to enhance the incident response plan for future incidents (Manning, 2023).

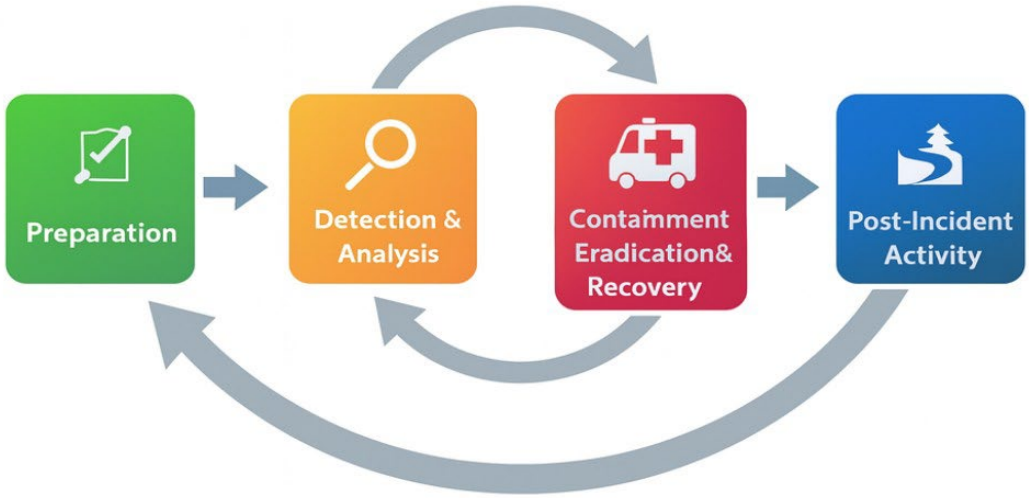

Figure 19: Phases Of Incident Response

The Digital Forensic Readiness (DFR) program includes an Incident Response component that helps organisations recognise, contain, and address cybersecurity incidents while maintaining the admissibility of collected digital evidence (Felipe Diaz Lopez, 2017). In the DFR approach to incident response, an organisation's active and reactive strategies are integrated, enabling it to respond appropriately once a breach or anomaly is detected. Forensic readiness in incident response means that, during planning, a system, process, and team are designated to support an efficient, lawful response to an incident within the stipulated legal and regulatory framework.

4.3 System Configuration for Experiment

This experimental study aims to address the current gap in understanding and application by providing a model for developing effective digital forensic readiness in IoT environments. Figure 20 illustrates the network structure of the proposed Digital Forensic Readiness Model experiment. The experiment involves creating a realistic organisational scenario within a confined environment, including various digital evidence, 50 user devices (desktops, laptops, and two network devices), and potential attackers or other malicious actors, to mimic real-world digital forensic investigations.

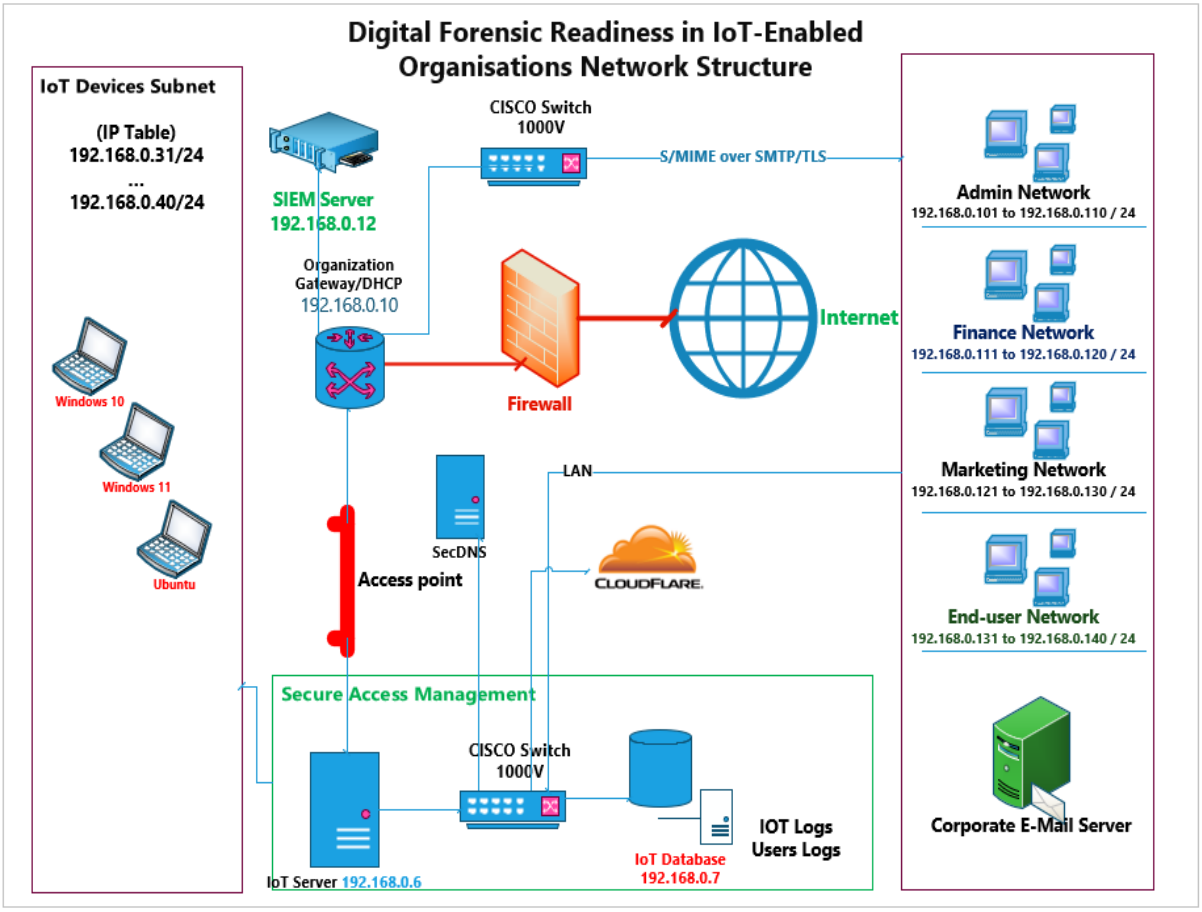

Figure 20: Network Structure of DFR in IoT-enabled Organisations.

The user devices include a variety of Windows 10, Windows 11, and Linux machines, each posing distinct security risks and shaping organisational perceptions of these devices. These devices are located in a data centre and accessed remotely. The open-source digital forensic tools Wazuh and Splunk were used to gather digital forensic data (identification, detection, and storage) and to conduct analysis (detection and monitoring). All system, network, and application logs are stored in a dedicated database (the forensic data store).

The proposed Digital Forensic Readiness (DFR) model operationalises forensic processes by integrating continuous monitoring, evidence acquisition, secure preservation, integrity validation, and structured chain-of-custody management within the organisational IoT environment. Unlike conventional security monitoring approaches that focus primarily on attack detection and operational response, the model ensures that security events and system artefacts are collected and preserved in a manner suitable for forensic investigation and for evidential admissibility.

The operationalisation of forensic processes begins with the monitoring stage, deploying Wazuh agents across organisational endpoints, servers, and IoT-connected systems. These agents continuously monitor system activities, authentication attempts, network events, changes in file integrity, and security logs generated across the infrastructure. Once suspicious activities or Indicators of Compromise (IoCs) are detected, the system automatically generates alerts and forwards the associated evidence to the centralised Wazuh server and Splunk SIEM platform for correlation and preservation.

To ensure forensic reliability, all collected logs and security artefacts are preserved with associated metadata, including timestamps, device identifiers, event sources, log categories, and system context information. Timestamp synchronisation mechanisms were implemented across monitored devices to maintain temporal consistency and support accurate event reconstruction during forensic investigations. This process ensures that evidence collected from distributed IoT devices remains correlated and traceable throughout the investigative lifecycle.

The model further operationalises evidence handling through structured workflows for evidence acquisition. Security logs, authentication records, event traces, file integrity monitoring outputs, and system activity records are automatically aggregated and securely stored in central forensic repositories. Access to forensic data is restricted via role-based access controls to prevent unauthorised modification or deletion of evidential artefacts.

Additionally, forensic preservation mechanisms were implemented to maintain the integrity of evidence throughout the collection and storage. Collected evidence is preserved in read-only formats where possible, and integrity verification mechanisms, such as cryptographic hashing and secure timestamping, are applied to detect potential tampering or unauthorised alterations. These measures strengthen evidential reliability and support compliance with digital forensic investigation standards.

4.3.1 Wazuh Implementation

Wazuh is an open-source, integrated XDR and SIEM protection for endpoint and cloud operations. It is designed to be an enterprise-ready security platform that imposes no licensing constraints and provides a global enterprise vision.

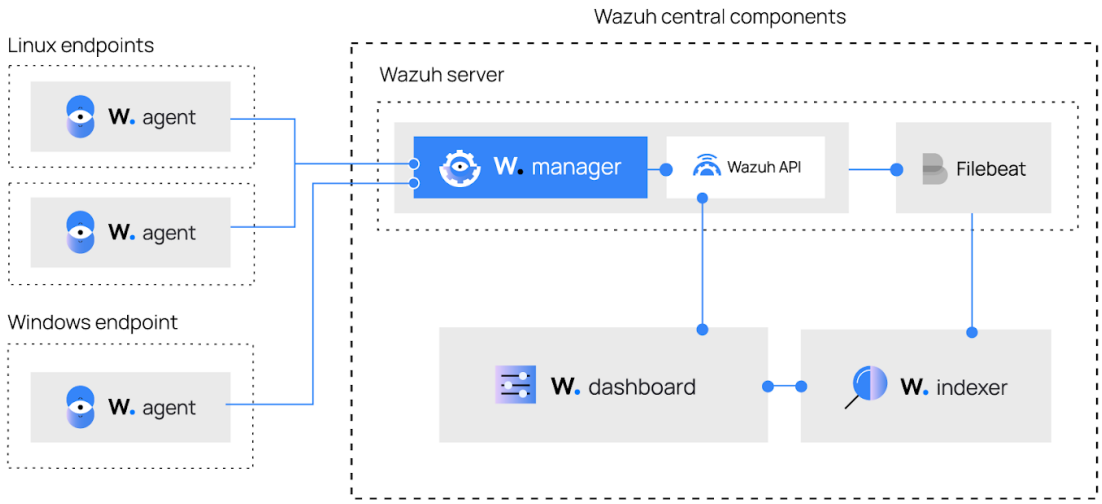

Figure 21: Wazuh Architecture (Wazuh Inc., 2024)

Wazuh is an SIEM tool for security analysts that offers capabilities in log analysis, file integrity monitoring, host-based intrusion detection, root check, and regulatory compliance support. It provides detailed information on security incidents and can be used for preventative analysis. Its advanced capabilities make it a valuable tool for analysts to conduct comprehensive forensic analysis (Wazuh Inc., 2024).

This thesis proposes a DFR solution based on the open-source product Wazuh. It aims to address problems and related questions, such as how to separate essential alerts from noise (i.e., distinguishing useful from non-useful data) and how IoT-enabled organisations can be digitally forensic-ready to detect and prevent cyberattacks more effectively and conduct comprehensive forensic analysis. This is relevant to modern organisations, as cyber-attacks are becoming more frequent and more severe, and traditional risk management strategies are becoming less effective.

4.3.1.1 Overview and Importance of Wazuh Implementation

Using an open-source package, Wazuh provides security detection, visibility, and compliance capabilities. Wazuh is a fork of OSSEC HIDS that provides ease of use and security maintenance by combining OSSEC's advantages with a new tool that offers

additional features, advanced functionality, and a user-friendly interface, all of which are easy to install and use. Wazuh supports data analysis with an ELK stack, a user-friendly UI, and multiple integrations with other tools. At this point, data analysis with the ELK stack is performed via Wazuh Manager and Filebeat. Wazuh Manager comprises four essential components: an API, an analysis engine, a notification engine, and a new visualisation module. The core of Wazuh consists of a single universal agent and three components: the Wazuh server, Wazuh indexer, and Wazuh control panel (Wazuh Inc., 2024).

4.3.1.2 Wazuh Indexer

Wazuh Indexer is a full-text and analysis engine. This central component measures and stores data generated by Wazuh servers and provides data logging and search capabilities. Wazuh indexers can be installed individually or grouped, providing flexibility and ease of use.

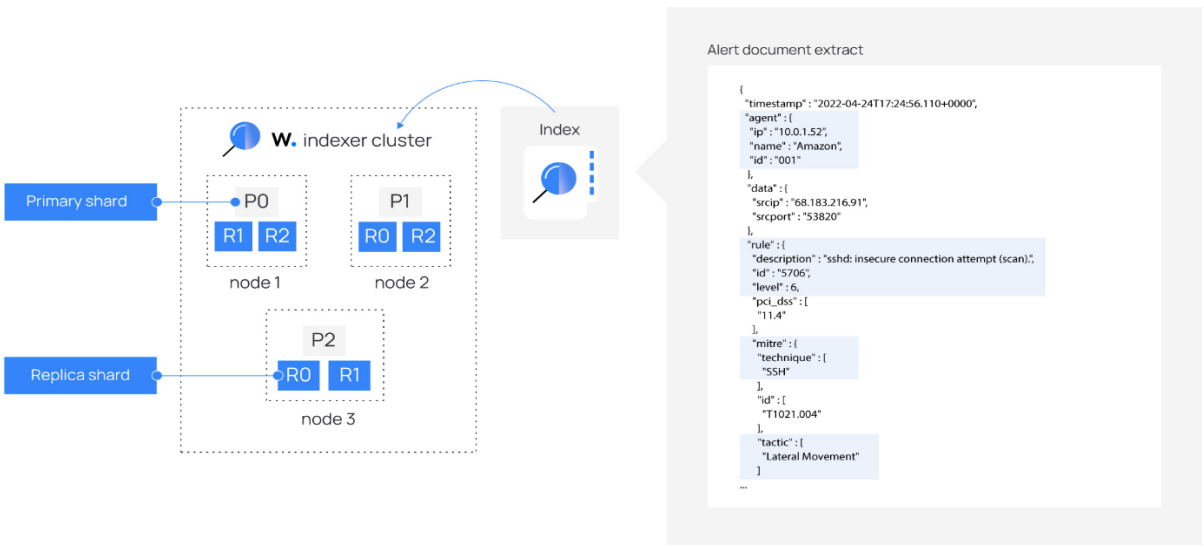

Figure 22: Wazuh Indexer (Wazuh Inc., 2024)

Each database consists of keys, fields, or attributes and their corresponding values, which may be strings, numbers, Boolean values, dates, variable values, addresses, or other data types. An index is an interrelated set of books; data stored in the Wazuh indexer is divided into shard containers. Wazuh indexer performs replication by spreading data across multiple shards and distributing shards across nodes. This protects your system against hardware failures and increases query capacity when you add nodes to the cluster. Wazuh uses four different indicators to capture various

events: wazuh-alerts, wazuh-archives, wazuh-monitoring, and wazuh-statistics (Wazuh Inc., 2024).

4.3.1.3 Wazuh Server

Wazuh server verifies the received data. It does so through discretion and authority, using threat intelligence to identify indicators of known compromise. A single server, when configured as a cluster, can analyse data from hundreds or thousands of agents and scale horizontally. This core is also used to manage, configure, and remotely install agents if necessary (Wazuh Inc., 2024).

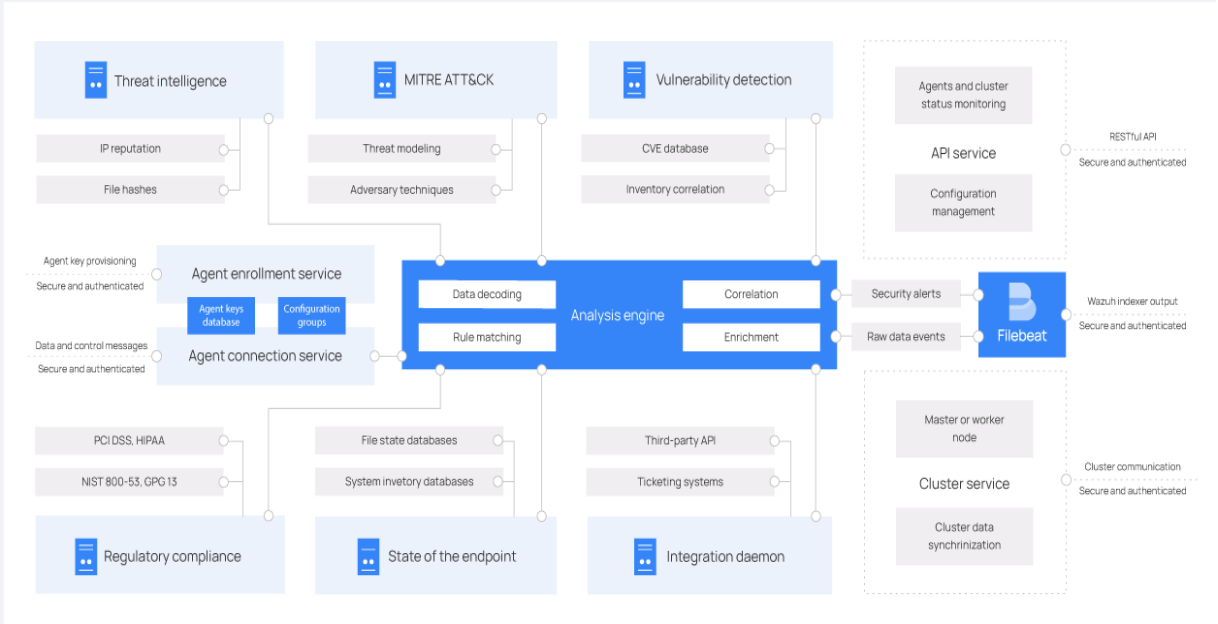

Figure 23: Wazuh server architecture (Wazuh Inc., 2024)

The Wazuh server comprises multiple components with distinct functions, including agent registration, agent authentication, and communication between Wazuh agents and the Wazuh server. These components are the agent enrolment service, Connection Manager, Search Engine, Wazuh RESTful API, Wazuh Cluster Daemon and Filebeat.

4.3.1.4 Wazuh Dashboard

Wazuh Dashboard is a web user interface for data visualisation and analysis. It includes various forms of data for security incidents, compliance (e.g., PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), malicious application detection, data display control integrity, test results, and over-the-air monitoring of out-of-the-box control panel status, etc. It is also used to manage Wazuh configurations and monitor their status.

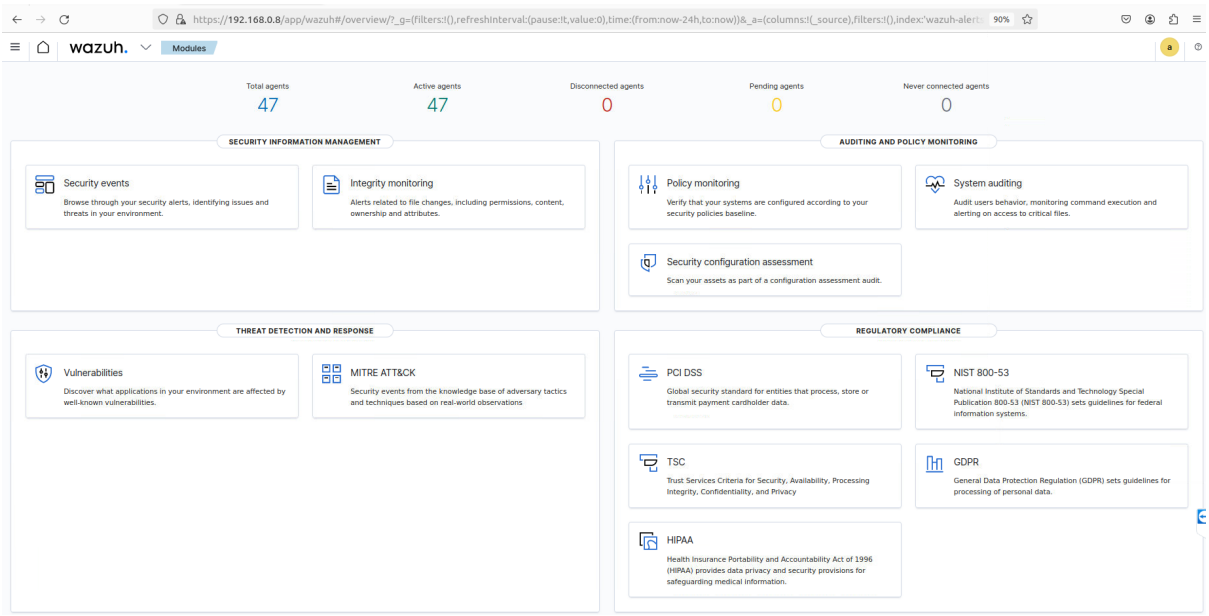

Figure 24: Wazuh Dashboard

4.3.1.5 Wazuh Agent

Wazuh agents are installed on endpoints such as laptops, desktops, servers, cloud-based systems, and virtual machines. They provide capabilities for threat prevention, detection, and response. They run on Windows, Linux, macOS, Solaris, etc. The platform can also monitor vulnerable devices, such as routers, firewalls, and switches. For example, Syslog files can be collected by Syslog, and their configuration can be monitored via SSH or API by periodically checking the files. The following shows Wazuh data flow and components.

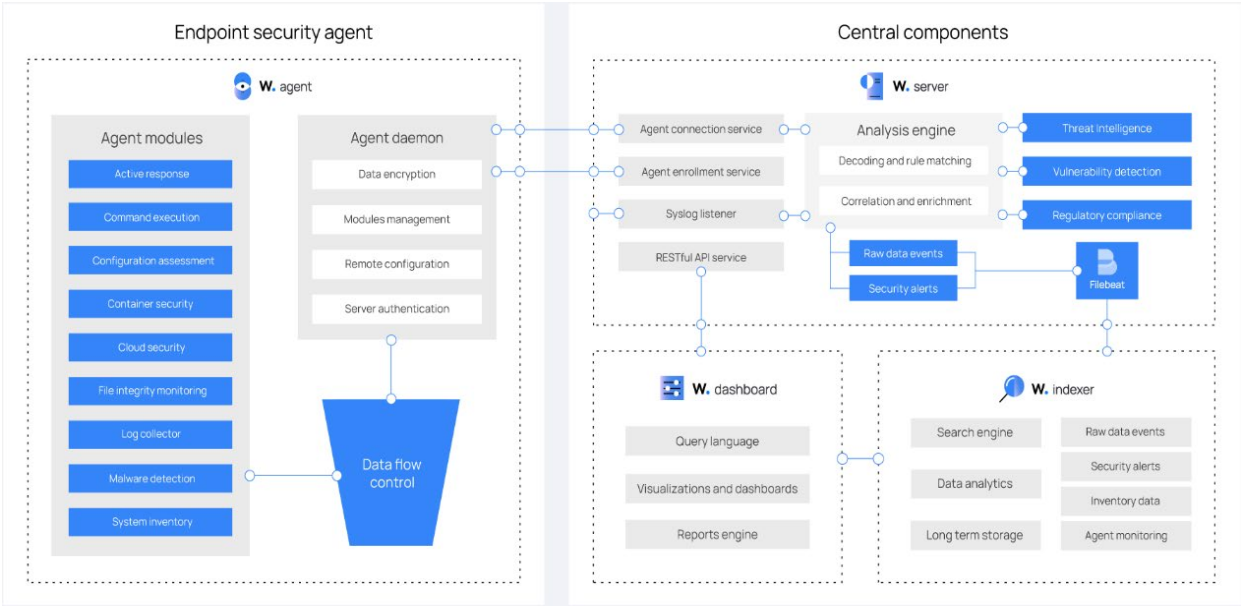

Figure 25: Wazuh components and data flow (Wazuh Inc., 2024)

Wazuh uses a typical client-server model. Wazuh agent is a program that needs to be installed on a machine to be monitored. A typical agent comprises four components: a configuration manager, a system check, a root check, and an API.

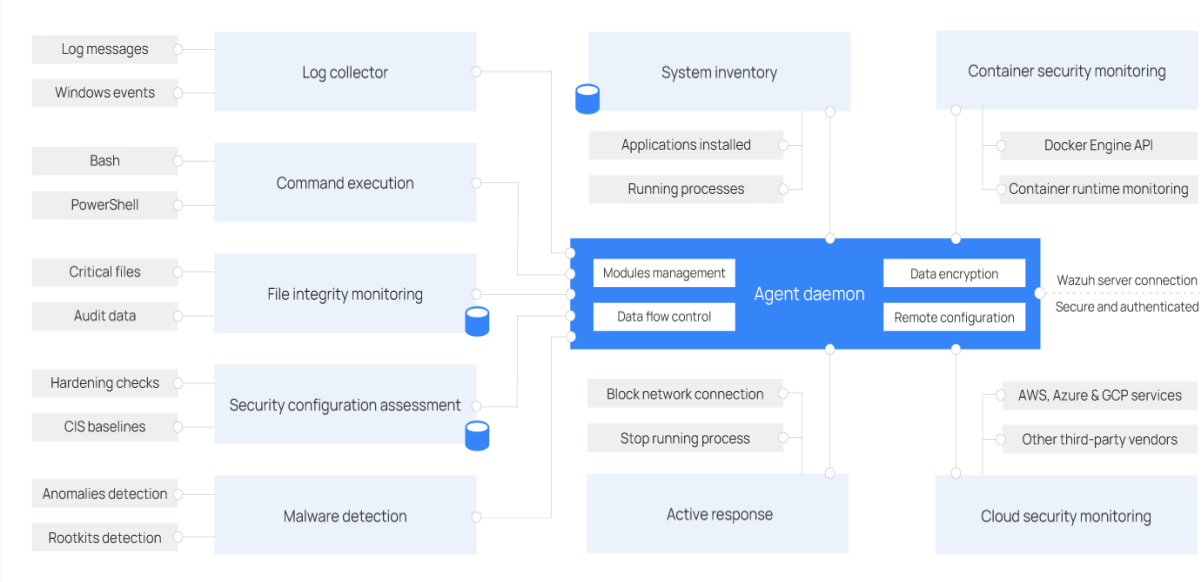

Figure 26: Wazuh Agent architecture (Wazuh Inc., 2024)

The Wazuh agent reads the configuration file from the Wazuh manager and retrieves the modules defined therein. The syscheck module detects changes to the file system. Rootcheck is a set of tests that verify system integrity and audit system rules. Results obtained by the agent are sorted by the Wazuh manager's analysis engine, and the notification engine notifies the administrator based on predefined rules. System and agent status can be checked in the Wazuh manager user interface. Logs monitor events on servers, network devices, and other IT systems. Log data is aggregated and searchable. If an anomaly is detected in the log data, an alert containing analysis information will be triggered.IoT-enabled organisations face an ever-changing security landscape. They worry about network security, misconfigured systems and software installations, insider threats, and the ever-increasing threat of attack. Non-compliance can also lead to significant losses for organisations, as many IT requirements are enforced through security controls. Implementing Wazuh offers a cost-effective approach to security monitoring without compromising on features or effectiveness, making it accessible to organisations of all sizes.

4.3.1.6 Wazuh Configuration Parameters and Implementation Justification

The Wazuh platform was configured as the primary Host-based Intrusion Detection System (HIDS) and forensic monitoring infrastructure within the proposed Digital Forensic Readiness Model. Several configuration parameters were carefully selected and optimised to support real-time monitoring, forensic evidence preservation, alert generation, and incident investigation within the organisational IoT environment.

1. **Wazuh Agent Configuration**

   Wazuh agents were deployed across monitored systems to collect authentication logs, event records, file integrity events, and security activities. The following configuration parameters were implemented:

   - Real-time log monitoring enabled.
   - Windows Event Channel integration activated.
   - File Integrity Monitoring (FIM) enabled.
   - Rootcheck and malware detection modules activated.
   - Active response disabled during forensic testing to preserve evidence integrity.
   - Centralised log forwarding enabled.

   Real-time log monitoring was configured to continuously capture authentication failures, successful login attempts, process execution events, and system activity records associated with cyberattack scenarios. File Integrity Monitoring was enabled to detect unauthorised file modifications and preserve system artefacts relevant to forensic investigations.

2. **Alert Threshold Configuration**

Alert thresholds were configured to reduce excessive false-positive alerts while maintaining effective attack detection capability. The configuration included:

- Brute-force login threshold limits.
- Repeated authentication failure detection.
- Suspicious process execution monitoring.
- High-severity event prioritisation.

These thresholds were selected after initial experimental testing to balance operational monitoring efficiency and the preservation of forensic evidence.

3. **Log Retention and Preservation Settings**

Log preservation settings were configured to support long-term forensic investigation requirements. Centralised log storage and indexing mechanisms ensured that collected evidence remained accessible and traceable throughout the investigation lifecycle. Timestamp synchronisation was also enabled to maintain temporal consistency between distributed IoT systems and monitoring platforms.

4.3.1.7 Alternative Monitoring Tools Considered

During the implementation phase of this research, several alternative intrusion detection and security monitoring tools were evaluated to determine their suitability for supporting Digital Forensic Readiness (DFR) within IoT-enabled organisational environments. The tools considered included:

- OSSEC
- Snort
- Suricata
- Security Onion

These solutions are widely recognised within the cybersecurity community and have been successfully deployed in various threat detection and incident response scenarios. However, each tool presents different strengths and limitations when assessed against the forensic readiness requirements of this study.

OSSEC was considered for its strong capabilities in host-based intrusion detection, log analysis, file integrity monitoring, and active response. As the predecessor of Wazuh, OSSEC provides effective security monitoring; however, it offers fewer advanced features, limited scalability, and less comprehensive integration than modern security monitoring platforms.

Snort is one of the most widely adopted network-based intrusion detection systems and is particularly effective at identifying known attack signatures and suspicious network activities. Its real-time traffic analysis and packet inspection capabilities make it valuable for network security monitoring. However, Snort primarily focuses on

network-level visibility and lacks the extensive host-based monitoring and forensic evidence collection capabilities required for a comprehensive forensic readiness solution.

Suricata was also evaluated due to its high-performance network monitoring capabilities and support for multi-threaded processing. It offers enhanced protocol analysis, intrusion detection, and network traffic inspection. While Suricata performs exceptionally well in detecting network-based threats, it lacks some of the integrated host monitoring and forensic evidence preservation features necessary to support a complete Digital Forensic Readiness Model.

Security Onion provides a comprehensive security monitoring platform that combines multiple open-source security tools for network monitoring, intrusion detection, log management, and threat hunting. Although Security Onion offers extensive security visibility and investigative capabilities, its deployment and management can be challenging, particularly in resource-constrained environments and smaller organisations seeking a more streamlined forensic-readiness solution.

Following a comparative evaluation, Wazuh was selected as the primary monitoring and detection platform for this research. Wazuh provides a comprehensive security monitoring solution that combines host-based intrusion detection, file integrity monitoring, vulnerability assessment, log analysis, security configuration monitoring, and incident detection within a unified platform. These capabilities closely align with the objectives of Digital Forensic Readiness by enabling organisations to proactively collect, preserve, and analyse digital evidence before security incidents occur.

A significant advantage of Wazuh is its ability to support continuous evidence collection across multiple endpoints while maintaining detailed audit trails and event records that can be utilised during forensic investigations. Its built-in file integrity monitoring capability helps identify unauthorised modifications to critical files, while its centralised log management functionality enables efficient aggregation and correlation of security events across distributed IoT devices and organisational systems.

Furthermore, Wazuh offers seamless integration with Security Information and Event Management (SIEM) platforms such as Splunk and Elastic Stack, facilitating advanced event correlation, visualisation, and forensic analysis. This interoperability simplifies evidence aggregation and supports the reconstruction of attack timelines, which are essential activities during digital forensic investigations.

Given its comprehensive monitoring capabilities, forensic evidence preservation features, scalability, and compatibility with the proposed Digital Forensic Readiness Model, Wazuh was identified as the most suitable monitoring solution for this research's implementation and evaluation. Its ability to bridge cybersecurity monitoring and forensic readiness requirements made it particularly effective for supporting proactive incident preparedness within IoT-enabled organisational environments.

4.3.2 Planning and Design

Wazuh Manager can mainly be a server appliance that accumulates and analyses data from Wazuh agents. It examines regulatory and policy information and generates alerts for the configured policies. While Network Intrusion Detection System (NIDS) setup is available on many systems today, NIDS deployments can be expensive when attempting to match the capabilities of commercial-grade solutions. Wazuh integrates Suricata for NIDS and benefits from using agents on hosts to analyse accumulated data, reducing the need to forward logs to a central analyser and saving on storage and performance costs at the NIDS server. Wazuh offers a cost-effective alternative to other NIDS solutions.

4.3.2.1 Assessing Security Requirements

The security requirement assessment is the first important step in implementing Wazuh. There are two critical aspects to this step. They are:

- Identify the assets in the environment: Wazuh is a host-based IDS with some IPS capabilities. Hence, before deploying Wazuh, it is essential to list the assets that need to be protected so that appropriate agents can be installed on them.

- Define the protection needs of each asset: The extent of monitoring required for each asset varies. Long-term log monitoring is helpful for servers but not for network devices. Some assets may require real-time alerts for security incidents. This step tries to determine the type of monitoring needed for the asset. This will also help build the correlation rules in the latter part of Wazuh.

4.3.2.2 Designing the Wazuh Architecture

After completing the hardware and software requirements, it's time to design the Wazuh architecture. Before designing the architecture, I suggest understanding the three components of the HIDS. It would help them to design the architecture that suits their requirements.

The critical components of the Wazuh HIDS are the Manager, Agents, and Analysis Engine. The Wazuh server serves as the manager and the central, complete component for sharding. The Wazuh agent program must be installed on the server to be monitored. Since it will monitor servers and potentially router/firewall devices, it must be installed on those devices.

The first check run by the agent registers the specific machine with the manager and then creates an encrypted key for it. The agent and the manager constantly communicate, and the agents are queuing items for the manager. Agents will retrieve information from the hosts they monitor and, using various built-in analyses, will analyse logs (comparing to known attack signatures), filesystems, changes to system tables, routers, firewalls, and other network devices. They will report any identified security concerns back to the manager.

The analysis engine performs all correlation analysis. This involves collecting logs and security alerts from agents and determining whether a security breach has occurred. This is done by creating rules and searching for rule matches or predefined pattern matches, e.g., if/else conditions. An automated response can then be initiated. For example, if a security concern matches a predefined pattern, an email notification can be sent to the network administrator.

4.3.2.3 Installation and Configuration

Wazuh architecture is based on a manager and agent. The Wazuh manager collects and analyses data from deployed agents using policy rules and reports and alerts on the collected data. Data collection occurs in the manager, and different analysis, correlation, and data enrichment processes are performed. The Wazuh API is a RESTful interface for interacting with the manager and agent. This API is used to query and report on data collected by the manager and agent.

4.3.3 Preparing the Environment for Wazuh

This section will prepare the environment for installing the Wazuh indexer and server dashboard. Wazuh can run on a physical or cloud server, but we'll use a PC. Below are the minimum PC requirements.

Table 4: Wazuh Minimum PC Requirements

Components	Minimum RAM (GB)	CPU (Cores)	Recommended RAM (GB)	Recommended CPU (Cores)
Wazuh Indexer	4	2	16	8
Wazuh Server	2	2	4	8
Wazuh Dashboard	4	2	8	4

For this experiment, Wazuh was installed on a 64-bit Ubuntu Linux operating system with the PC specifications below. The Wazuh dashboard can be installed on a dedicated node or along with the Wazuh indexer (Wazuh Inc., 2024).

Table 5: Implemented Wazuh PC Specifications

Components	RAM (GB)	CPU (Cores)
Wazuh Indexer / Dashboard	32	8
Wazuh Server	16	8

4.3.3.1 Installing and Configuring Wazuh

According to Wazuh, the Indexer and dashboard can be installed on the same server. Wazuh indexer and server can be deployed as a single cluster or multiple clusters. The Wazuh Server is the core component, including the Wazuh Manager and Filebeat. The Wazuh Manager collects and analyses information from Wazuh agents and triggers

an alert when a threat or vulnerability is detected. Filebeat securely sends notifications and logs events into the Wazuh indexer. For this experiment, a Wazuh single-node indexer and server were installed.

4.3.3.2 Configuring Wazuh Agents

The Wazuh server runs in manager mode, so agents can only communicate with it. Here, they have provided an initial configuration for testing on the server, including the server IP and authentication keys.

From the interface, we can add an agent that will execute a shell script as root on the client machine. The shell script includes the server information and the authentication key. The authentication key is similar to an SSH key. Wazuh agents communicate with the server using the authd process. The agents initiate all communication, and the authd process on the server creates a thread for each connection and processes it. All communication is encrypted using TLSv1.3. An optional server parameter is "--force", which resets the keys and agent connections.

By default, all agents are loaded with configuration profiles. This behaviour can be customised during the agent registration process and post-registration by updating an agent's active configuration when using version 3.7 or later. After adding the agent, we can see its status in the next window; it may take a moment to configure. We now have the list of agents and their status. From here, we can see the agent ID, name, IP address, and OS version to quickly identify agents.

4.3.4 Integration with Organisation Network

Hardening a system is a delicate process that can break existing functionality, whether through traffic blocking, corruption, or data deletion. Wazuh will help you identify which Wazuh agent users are experiencing issues and which rules are triggering them. This can be done by searching for user@hostname in the compliance monitor under the specific committed rules, then changing the time range to see how many times the rule was triggered. Clicking the graph button shows how often the rule was triggered during that time range. This information will help administrative users understand the impact of a specific rule and tune it to better suit the environment. The more detailed graph is available in the monitor option, which displays when the rule was

triggered for the agent user and the rule ID mentioned earlier, pinpointing the exact time and date. Maintaining a specific rule can be achieved by creating a custom rule policy. These packages will include newer versions of existing decoders and rules that work with the most current version of Wazuh, as well as new rules/decoders for changes to the security environment, e.g., points of weakness, potential attacks, and new malware types, to maintain and improve the level of security within an organisation.

4.3.5 Monitoring and Alerting

Monitoring is essential in our environment for real-time analysis. Wazuh offers a feature that enables effective, real-time monitoring. It also provides system health monitoring by analysing system messages, logs, and file changes. This is important because it helps us identify when and why something occurs in our system. For example, it detects when someone maliciously alters system files. Wazuh also monitors system and application authentication by tracking successful and failed user logins. Additionally, you can receive real-time alerts based on correlation rules to detect active incidents.

4.3.5.1 Configuring Log Monitoring Rules

The log monitoring module correlates events and their status to fine-tune the system's responses. It does so by generating alerts about policy violations and system status. Log monitoring rules are created by analysing multiple log events and their statuses to identify specific conditions. When a condition is met, an alert is raised. Log monitoring is a feature of the Wazuh agent that scans and analyses system and application logs. Log data can be imported from files and Windows Event Logs, making integration straightforward. Wazuh has developed rules to detect security policy violations. These rules are used to identify particular behaviours or applications that threaten the system's security. Wazuh rules are easy to customise and adapt to an organisation's needs.

4.3.5.2 Setting Up Real-Time Alerts

Wazuh enables the setup of real-time alerts, including immediate notifications of security incidents. It facilitates the implementation of real-time alerts based on existing

FIM, PCI DSS, or other security policy requirements. Expanding Wazuh rules is a common method for creating new security alerts. When adding FIM monitoring rules, it is best to target a specific file or directory. File identification can be easily done using the file properties window. Comparing the MD5 checksum and computing head and tail checksums of the file content are effective ways to detect file tampering. If checksums do not match the baseline data, an alert will be generated for the manager, and the affected file will be recorded in an alert incident. File checksum testing is efficient, and data can be stored for possible IOC or forensic research.

4.3.6 Incident Response and Remediation

Incident response refers to the process an organisation uses to identify and mitigate the impact of a security breach. Incident response plans are pre-prepared documents that detail the organisation's response to a security breach. They should also specify the procedures for management involvement, customer communication, and public relations, and include sample notices for customer and public release. The primary objectives of an effective incident management plan are to minimise the impact of the security event and to prevent further damage. The ability to monitor and respond to incident-causing activities in real time is vital for controlling the extent of damage from a security breach.

Wazuh can be utilised to enhance incident response in several ways. It monitors system and application activity by comparing it against a set of rules, which help identify malicious activity or threats to system security. Wazuh rules are valuable for incident response because any activity that triggers a rule is logged and an alert is generated. These alerts help identify security breaches, as they can be sent instantly to administrators via email and used to centralise logs of specific threats. This makes it easier to compile reports and statistics related to security events. Each Wazuh alert is assigned a severity level from 0 to 12. The severity is determined by an equation that considers the activity type and its potential impact on the system. High-severity alerts are easy to recognise and crucial for real-time incident response, as they highlight the most serious threats to system security.

4.3.6.1 Developing an Incident Response Plan

This is an essential element of an organisation's security. An incident response plan is a proactive strategy for preventing and managing incidents. It involves preparation for such events. Wazuh already has this in place, which can serve as a guide for an organisation's incident response plan.

The first phase of the Wazuh incident response plan involves the preparation stage. The main goal of the plan is to recognise that being transparent and ready can minimise loss and downtime during a security incident. Wazuh states that a proper preparation stage will enable organisations to identify what needs protection and detect security breaches. This approach helps to significantly lessen the cost and impact of an incident.

Some key tasks in the preparation phase of an incident response plan include developing a security policy that integrates with the infrastructure Wazuh will configure to assess and report on security levels. A security incident handling policy is also essential, as it will serve as the primary guideline for actions when a security incident occurs. Additionally, Wazuh emphasises that raising public awareness of security is crucial to minimise the number of security-related events. These can range from phishing scams to attempts at gaining unauthorised access. This creates a standard for comparing the policy's security level. It will evaluate the severity of incidents and notify relevant parties of any security breaches.

4.3.6.2 Investigating and Responding to Security Incidents

Wazuh is used to monitor, investigate, and respond to security incidents. In the event of a server intrusion, the organisation will be notified. The incident could be caused by a virus or an unauthorised user, and it will then be assessed, with a report generated. Wazuh analyses the report and provides the necessary information to address the issue. For example, if the problem is a virus, Wazuh will suggest steps to mitigate and resolve it. When an incident occurs, the Wazuh Manager is notified and retrieves the relevant data from the Wazuh agents. This data is stored in the Incident Escalator and analysed by security personnel. They then determine an appropriate response to the incident. If the response is approved, an event file containing instructions for the agents to resolve the incident is created. These instructions are

extracted and executed by the Impacted Host, which is subsequently assessed by security personnel. If the event resolves the incident, feedback is provided, and the incident status is closed.

4.3.7 Reporting and Compliance

Reporting is an essential part of network management. It is designed for human understanding, and filtered, condensed, graphical representations of Wazuh data are the most effective way to present it. Usually, non-technical management needs to review such reports. Wazuh reports can be accessed via the web interface, and limited user accounts can be created to allow users to view specific predefined dashboards. For example, the compliance officer could have an account that grants access only to PCI DSS reports. It is now common for organisations to comply with specific industry security standards. This may stem from an audit conducted by a new business partner or simply demonstrate good practice to clients. Wazuh includes built-in compliance templates that map to technical controls from various security standards. For instance: PCI DSS, AWS Foundational Security Best Practices, GDPR, ISO 27001, CIS Amazon Web Services Benchmarks, and others.

In recent years, there has been a rise in regulations and laws governing how organisations conduct their business. Due to the ethical and security-sensitive nature of much of its work, the UK Ministry of Defence is subject to many of these regulations. These systems must be implemented securely and robustly to prevent and mitigate potential security incidents. Wazuh can provide and monitor security and threat exposure in line with applicable security standards and regulations. It offers out-of-the-box security policies for tools such as the CIS benchmarks, PCI-DSS regulatory compliance, the US DoD policy auditing framework, and more. By implementing Wazuh and configuring it to these standards, organisations can more effectively identify and rectify problematic areas in their security and compliance with minimal effort and investigation.

This is all monitored and accomplished through an intuitive web interface and requires minimal effort to set up and maintain. In summary, Wazuh policy monitoring will ensure that the organisation's systems comply with security and policy standards

by alerting when requirements are not met, enabling corrective action, and comparing and measuring the security and compliance status against desired states. This information would be vital to a security and systems administrator tasked with maintaining high security within the organisation.

4.4 Splunk Implementation

Splunk is a real-time operational intelligence engine that enables us to conduct live searches and send alerts when specific conditions are met. The Splunk architecture comprises three main components: forwarders, indexers, and search heads. The forwarders are responsible for capturing and transmitting relevant logs to the indexers. The indexers handle the indexing of data sent by the forwarders. The search head is responsible for searching and reporting on the indexed data. (Ghosh et al., 2022).

Splunk enables digital forensics researchers to quickly access and refine logs, rather than working with raw text logs and low-level file-system techniques. Splunk is primarily designed to search, index, and analyse logs. It also interprets system behaviour from logs and, through Splunk, believes that including forensic evidence will help explain how the system works in real time. Splunk optionally allows one to split logs into fields through a process called extraction. Splunk can label events during the search and create an event type that can later be referenced (Du, Le, and Scanlon, 2020). It requires examination of procedural and primitive data to produce findings about the events. A handler in the digital artefact that can give evidence that will be used in the court of law. Splunk is a solution for log management, security, information, and event management, and it helps build cool stuff from data (Dimitriadis et al., 2020).

4.4.1 Chain-of-Custody and Evidence Integrity Management

A critical component of the proposed Digital Forensic Readiness Model is the operationalisation of chain-of-custody (CoC) procedures to ensure that digital evidence remains authentic, traceable, and legally defensible throughout the investigation lifecycle. Chain-of-custody management refers to the documented process for recording how evidence is identified, collected, transferred, preserved, accessed, analysed, and stored during forensic investigations.

Within the implemented model, chain-of-custody procedures begin immediately after suspicious events are detected by the monitoring infrastructure. Once an event is identified, the associated logs and digital artefacts are automatically preserved within the forensic evidence repository. Each evidence object is assigned a unique identifier and accompanied by metadata that documents the source system, acquisition timestamp, evidence type, acquisition method, and the responsible investigator or automated process.

To maintain evidential integrity, all evidence transfers and access activities are logged continuously within the system. Any modification, duplication, retrieval, or analysis of forensic artefacts generates corresponding audit records, thereby ensuring complete traceability throughout the evidence lifecycle. These audit mechanisms support accountability and minimise opportunities for evidence tampering or unauthorised access.

The model also incorporates integrity verification mechanisms to preserve the authenticity of collected evidence. Hashing algorithms were applied during evidence acquisition and storage processes to generate integrity validation values for forensic artefacts. These hash values are periodically revalidated during investigative procedures to confirm that evidence has not been altered after collection. The integration of hashing, secure storage, timestamp synchronisation, and audit logging collectively strengthens the reliability and admissibility of digital evidence within organisational investigations.

Furthermore, Splunk dashboards and Wazuh monitoring interfaces provide investigators with structured visualisation and retrieval capabilities for forensic artefacts while preserving the underlying integrity of the evidence. This operational workflow enables organisations to maintain continuous forensic readiness while supporting efficient evidence handling and investigation procedures in IoT-enabled environments.

4.4.2 Splunk Configuration and Evidence Indexing Parameters

Splunk was implemented as the Security Information and Event Management (SIEM) platform to support forensic evidence indexing, event correlation, security analysis, and investigation reporting. Several configuration parameters listed below were optimised to improve the efficiency of evidence retrieval, forensic visibility, and event analysis capabilities.

1. **Log Indexing Configuration:** Dedicated indexes were created within Splunk to separate authentication logs, security events, forensic artefacts, and monitoring alerts. The indexing strategy improved search efficiency and enabled structured forensic analysis across multiple evidence sources. This structured indexing approach improved evidence correlation and enabled investigators to reconstruct attack timelines more effectively. The following indexing configurations were implemented:
    - ✓ Security event index
    - ✓ Authentication event index
    - ✓ File integrity monitoring index
    - ✓ Wazuh alert index
    - ✓ Forensic investigation index
2. **Data Input and Log Forwarding Configuration:** Splunk forwarders were configured to ingest logs generated by Wazuh agents and monitored systems. These configurations ensured that forensic logs retained their original metadata and contextual information during evidence transfer and indexing processes. Log ingestion settings included:
    - ✓ Real-time event forwarding
    - ✓ Timestamp extraction
    - ✓ Source type classification
    - ✓ Log parsing rules
    - ✓ Event field extraction
3. **Search and Correlation Settings:** Custom search queries and correlation rules were implemented within Splunk to identify Indicators of Compromise (IoCs), repeated authentication failures, suspicious network activities, and attack patterns associated with brute-force and denial-of-service attacks. Correlation

searches enabled the aggregation of distributed evidence across multiple systems and improved forensic investigation efficiency by automating the analysis of event relationships.

4.4.3 Alternative SIEM Platforms Considered

During the implementation phase of this research, several Security Information and Event Management (SIEM) solutions were evaluated, including Elastic Stack (ELK), IBM QRadar, AlienVault OSSIM, and Graylog. Each platform offered valuable security monitoring and log management capabilities; however, Splunk was ultimately selected as the most suitable solution for the study's objectives.

The decision to adopt Splunk was based on several key advantages. Splunk provides powerful search and analytics capabilities, enabling investigators to rapidly identify, filter, and analyse large volumes of security events generated across IoT-enabled environments. Its scalable indexing architecture enables efficient handling of growing datasets, which is particularly important in distributed IoT ecosystems where devices continuously generate large volumes of log data.

In addition, Splunk offers real-time monitoring and analysis, enabling security teams to detect suspicious activity and respond promptly to potential incidents. Its intuitive dashboards and visualisation features also support forensic investigations by presenting complex event data in an easily understandable format. Furthermore, Splunk integrates seamlessly with Wazuh, the security monitoring platform used in this research, enhancing the collection, correlation, and analysis of forensic evidence.

Another important factor was Splunk’s ability to support forensic event correlation and timeline reconstruction. These capabilities enabled the tracking of attack progression, the identification of affected systems, and the reconstruction of incident sequences, all of which are critical to achieving effective Digital Forensic Readiness in distributed IoT environments.

4.5 Chapter Summary

This chapter has presented the design and implementation of the proposed Adaptive Proactive Readiness Model (APRM), including its organisational, technical, and security layers, as well as the supporting system architecture and monitoring

infrastructure. The implementation demonstrates how Digital Forensic Readiness principles can be operationalised in an IoT-enabled organisational environment through the integration of evidence collection, monitoring, preservation, and analysis mechanisms.

While Chapter 4 established the framework and implementation environment, the effectiveness of the proposed model must be validated through practical experimentation. Consequently, the next chapter evaluates the model's operational capability through a series of realistic cyberattack scenarios. These experiments assess the model's ability to detect malicious activities, preserve forensic evidence, support incident investigation, and maintain forensic readiness throughout the investigation lifecycle. Through this evaluation, the research seeks to determine whether the proposed model can effectively address the forensic readiness challenges identified in the literature review.

5.0 Preparation and Setup for Experiments

5.1 Introduction

Building upon the implementation environment developed in Chapter 4, the experiments presented in this chapter were designed to evaluate the practical effectiveness of the proposed APRM under realistic attack conditions. The selected scenarios assess the model's ability to generate, preserve, and analyse digital evidence while supporting real-time detection and forensic investigation activities. These experiments provide the empirical basis for evaluating the Digital Forensic Readiness capabilities of the proposed model. It presents the implementation, detection, and forensic investigation of four security scenarios designed to evaluate the effectiveness of the proposed Digital Forensic Readiness (DFR) model within an IoT-enabled organisational environment. The selected scenarios include brute-force attacks, File Integrity Monitoring (FIM) events, unauthorised process execution, and Denial of Service (DoS) network attacks. These scenarios were deliberately chosen because they represent common, realistic cyber threats faced by modern organisations and provide opportunities to evaluate the model's ability to detect, preserve, and analyse digital evidence throughout the forensic investigation lifecycle.

The selected attack scenarios reflect different stages and objectives of cyberattacks commonly observed within organisational networks and IoT-enabled infrastructures. Brute-force attacks are attempts to gain unauthorised access to systems through credential compromise and remain among the most frequently reported attack techniques targeting remote access services such as SSH and RDP. In IoT environments, weak authentication mechanisms and poorly managed credentials often increase susceptibility to such attacks. Successful brute-force attacks may lead to unauthorised system access, privilege escalation, data compromise, and further lateral movement across organisational networks.

File Integrity Monitoring (FIM) scenarios were selected because unauthorised file modification is a common indicator of malicious activity, malware infection, insider threats, or post-compromise actions. In forensic investigations, monitoring changes to critical system files provides valuable evidence of attacker behaviour and helps investigators identify when and how systems were compromised. The inclusion of

FIM therefore supports the assessment of evidence preservation and forensic traceability within the proposed model.

The unauthorised process detection scenario was included because attackers frequently execute malicious processes following successful system compromise. Such processes may be used to establish persistence, exfiltrate data, disable security controls, or facilitate further attacks. Detecting unauthorised processes is particularly important in IoT-enabled environments where malicious software may operate unnoticed due to limited device visibility and monitoring capabilities. This scenario enables the evaluation of the model's ability to identify suspicious activity and generate forensic artefacts that support subsequent investigations.

Denial-of-Service (DoS) attacks were selected for their relevance to both traditional organisational networks and IoT ecosystems. IoT devices have frequently been exploited to participate in large-scale Distributed Denial of Service (DDoS) attacks due to their widespread deployment, limited security controls, and continuous network connectivity. Such attacks can disrupt critical services, affect operational continuity, and generate significant volumes of network activity that require forensic investigation. Evaluating DoS attacks, therefore, provides insight into the model's capability to detect network-based threats, collect relevant evidence, and support attack reconstruction.

Collectively, these scenarios provide a representative set of threats affecting confidentiality, integrity, and availability within organisational environments. They were selected not only because of their prevalence in real-world cyber incidents but also because they enable comprehensive evaluation of the proposed Digital Forensic Readiness Model across multiple dimensions, including attack detection, evidence generation, evidence preservation, forensic analysis, and incident investigation. By using realistic attack scenarios, the study aims to demonstrate how Digital Forensic Readiness can improve organisational preparedness for cyber incidents and strengthen forensic investigation capabilities within IoT-enabled infrastructures.

To study and analyse these attacks in a controlled environment, a realistic network architecture comprising attacker and victim systems was developed. Wazuh was deployed as the primary security monitoring platform to detect malicious activities, generate alerts, and collect forensic artefacts, while Splunk was utilised to support evidence correlation, visualisation, and forensic analysis. Detailed configuration steps and supplementary screenshots are provided in Appendix B to maintain the focus of this chapter on implementation, detection results, and forensic investigation findings.

5.2 Scenario - Detecting and Forensic Investigation of a Brute-Force Attack

Brute-force attacks are carried out by threat actors to gain authorised access to endpoints and services. Services such as SSH on Linux and RDP on Windows are often vulnerable to brute-force attacks. Wazuh detects a brute-force attack by intercepting multiple authentication failures.

5.2.1 Infrastructure and Configuration for Attack Scenario

The table below shows the infrastructure and configuration used for this attack scenario.

Table 6: Infrastructure for Brute-Force Attack

Endpoint	Description
Ubuntu 22.04	WAZUH Server Machine
Windows 11 192.168.0.10	Attacker endpoint that performs brute-force attacks. It's required to have an SSH client installed on this endpoint.
RHEL 9.0	Victim endpoint of SSH brute-force attacks. It's required to have an SSH server installed and enabled on this endpoint.
Windows 11 192.168.0.50	Victim endpoint of RDP brute-force attacks. It's required to enable RDP on this endpoint.
Kali	Attackers' tools

The following steps were performed to configure the Ubuntu endpoint. This allows authentication failure attempts to be performed on the monitored RHEL and Windows endpoints(Wazuh Inc., 2024).

1. On the attacker endpoint, install Hydra and use it to execute the brute-force attack:
2. $ sudo apt update
   $ sudo apt install -y hydra

The following steps were performed during the brute-force attack. In this scenario, the attacker launches the attack from the 192.168.0.10 (DC01) machine. To install Kali Linux in VMware, the attacker must first install VMware on the 192.168.0.10 (DC01) machine.

- The attacker uses KALI Linux to attempt brute-force logins at 192.168.0.60 if its Remote Desktop Connection (RDP) service is left ON by mistake. The attempt is made through the **192.168.0.10** (DC01) machine.

- Kali Linux is set up at VMware with IP: **192.168.0.20** over the **192.168.0.10** machine. The attacker prepared 11 password list files and stored them in the \Desktop\Password.txt folder for later brute-force searches. In this password list file, 10 of the passwords are wrong, and 1 of them is the right one, so 10 times it will be a failure to log in to the 192.168.0.20 machine, whereas there is a correct password inside the password list file, so 1 time the attacker will be successful in logging in to the **192.168.0.20** machine.

- This attack attempt shall be appropriately recorded on the Wazuh client running at 192.168.0.20. Then, it shall be sent to the Wazuh server machine to alert and identify the attack scenario.

- Therefore, the attack scenario is adequately communicated to the Wazuh server and can be easily seen. Ten attempts will fail and be noticed by the Wazuh server, and one attempt will be marked as successful.

- This attack scenario can be quickly identified by the Wazuh server through a forensic audit of the 192.168.0.50 machine using the Wazuh server.

- Using this log forensic audit, the attack scenario can be identified and reconstructed easily, from which setup this attack was made.

Figure 27: Brute-Force Attack on Host 192.169.0.50

Immediately, the brute-force attack is launched across the network at any endpoint (e.g., 192.168.0.50), and the Wazuh Server (i.e., 192.168.0.8) displays it. To see this on the Wazuh Server, click Agents and select the agent machine from the list of clients (e.g., 192.168.0.50). Then click Security Events to see any incidents on the Wazuh client (e.g., 192.168.0.50). The evidence screenshot is shown below:

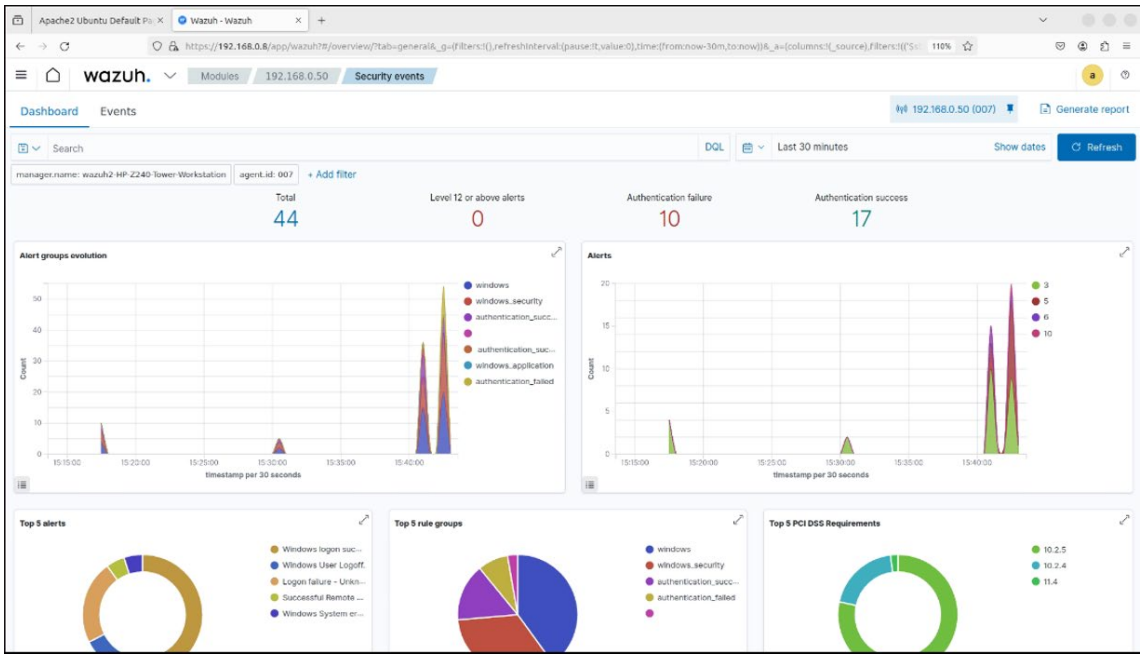

Figure 28: View of Security Events on the Wazuh Dashboard

As one password from the passwords list file was correct, it can be seen below in the highlighted screen that a successful logon happened and was identified:

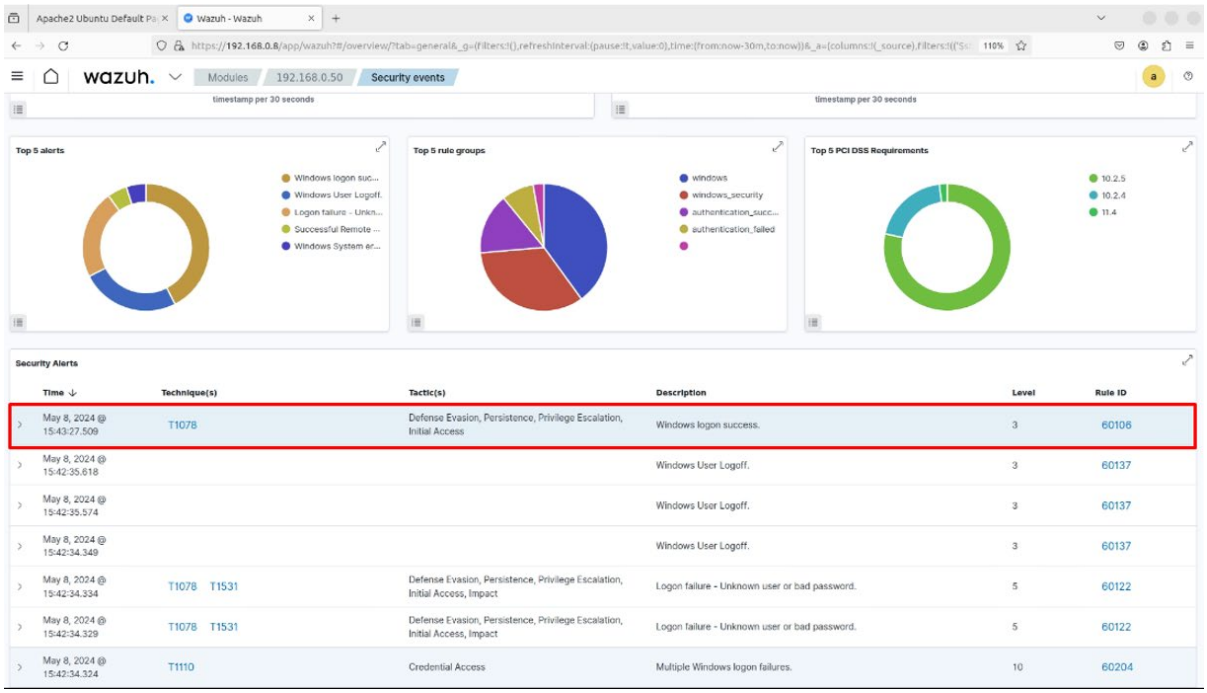

Figure 29: Identified Successful Logon Security Events on the Wazuh Dashboard

VICTIM machine/ Wazuh client IP (192.168.0.50) can be seen as evidenced by the screenshot below.

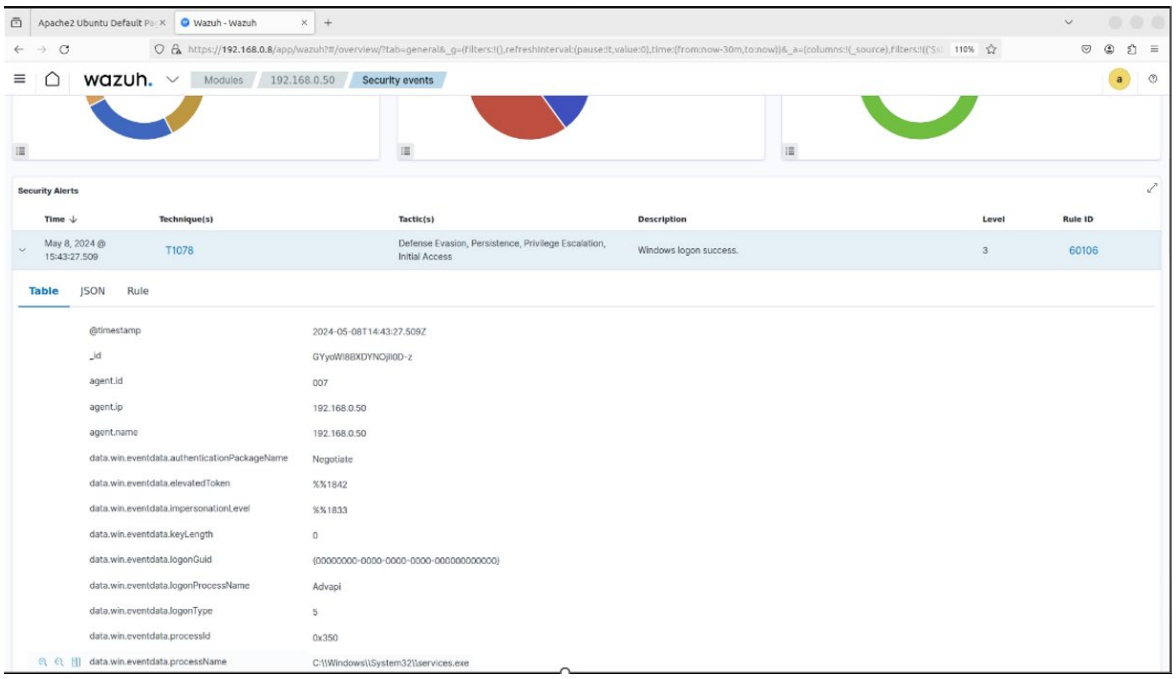

Figure 30: Victim Machine Security Events on the Wazuh Dashboard

The following steps were taken to conduct further forensic analysis of this brute-force attack scenario.

1. Go to the Wazuh Client machine with IP 192.168.0.50 for further forensic investigation.
2. Run Events Viewer Activity to cross-verify whether any login attempt is made on this machine with Event ID 4624.
3. Event ID 4624 means that a remote user made a login attempt, which can only happen if the user leaves the remote desktop connection open unintentionally.
4. The attacker can scan any connections opened at any desired IP using an Nmap scan.
5. The screenshot of the forensic evidence is shown in Figures 31 and 32 below.

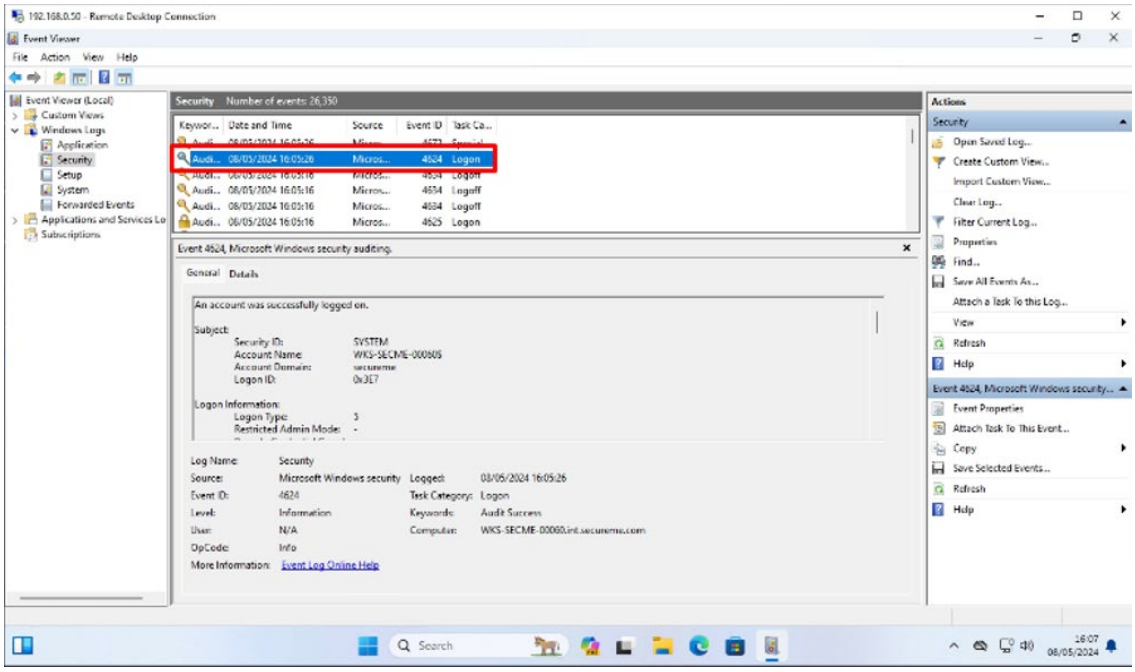

Figure 31: Event Viewer Activity Showing Attacker Login

6. For Event ID 4624, all the Event data can be seen, including the attacker's login name, machine name, and other details. The screenshot is shown below.

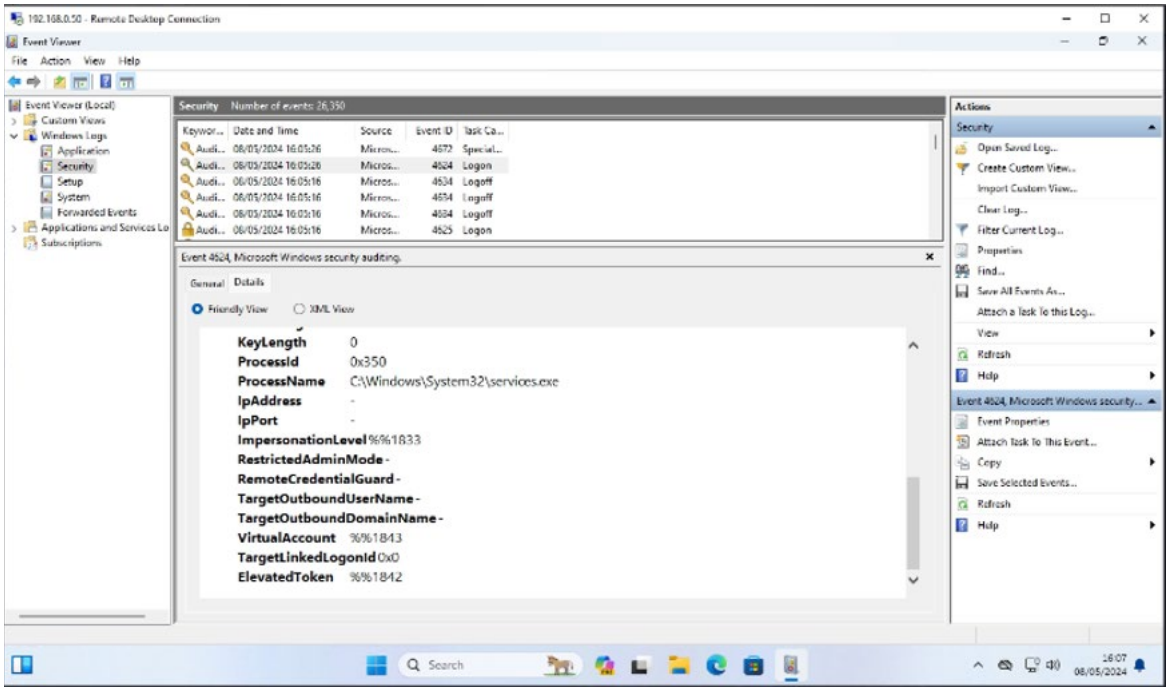

Figure 32: Event Viewer Data Confirming Attacker Login Information

5.2.2 Digital Forensic Analysis of Brute Force Attack Logs Using Splunk

To analyse the logs using Splunk, the Event Viewer logs need to be extracted from the victim machine at 192.168.0.50. The steps below were followed, and the figure below shows the log extraction process from the victim machine via the Event Viewer.

1. Open the Event Viewer on the victim's machine.
2. Select Windows Logs and then Security, as we are only concerned about the network events.
3. Save the event logs from the Event Viewer on the desktop, or choose any path you want, as shown in Figure 37.

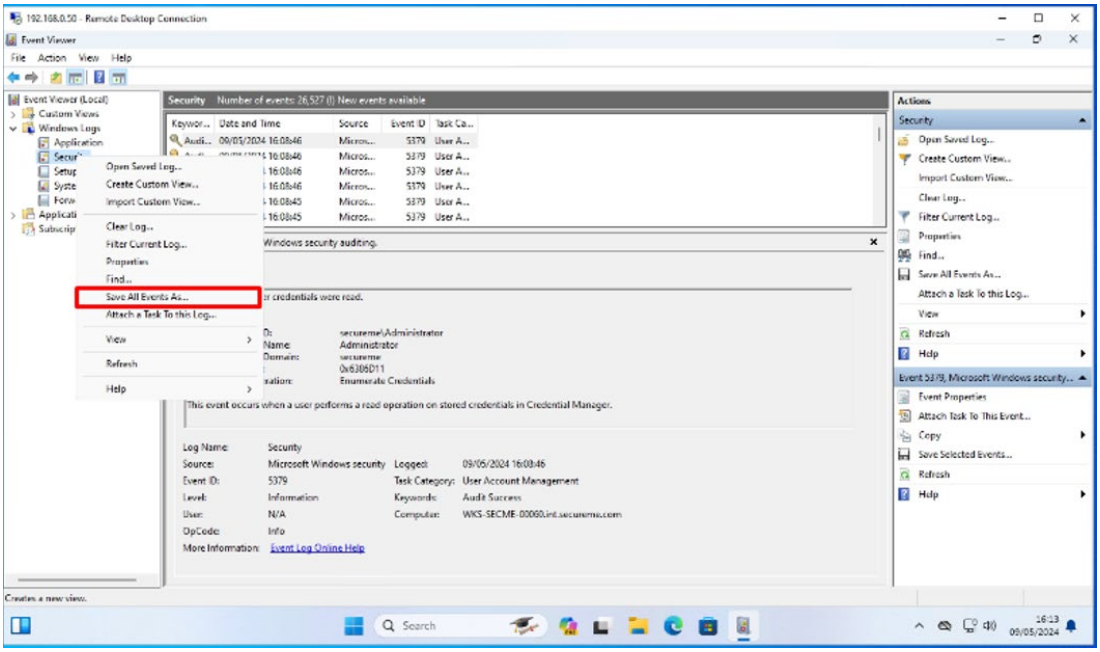

Figure 33: Extraction of Event Logs Using Event Viewer

4. Securely copy the logs into the Splunk machine and import the logs into Splunk Enterprise.

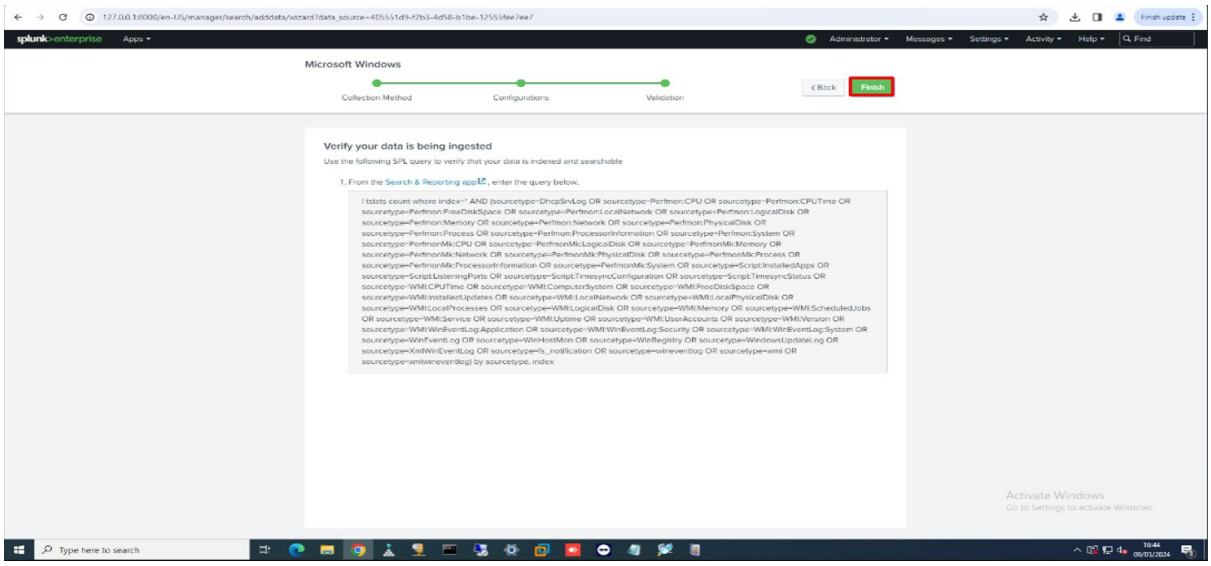

Figure 34: Logs Successfully Uploaded to Splunk

5. The log analysis begins after the logs have been successfully uploaded to Splunk.

6. The following figures illustrate that we have utilised a query that filters all logs of failed login attempts.

7. As shown in Figures 39 and 40, a significant number of failed login attempts were made by attackers.

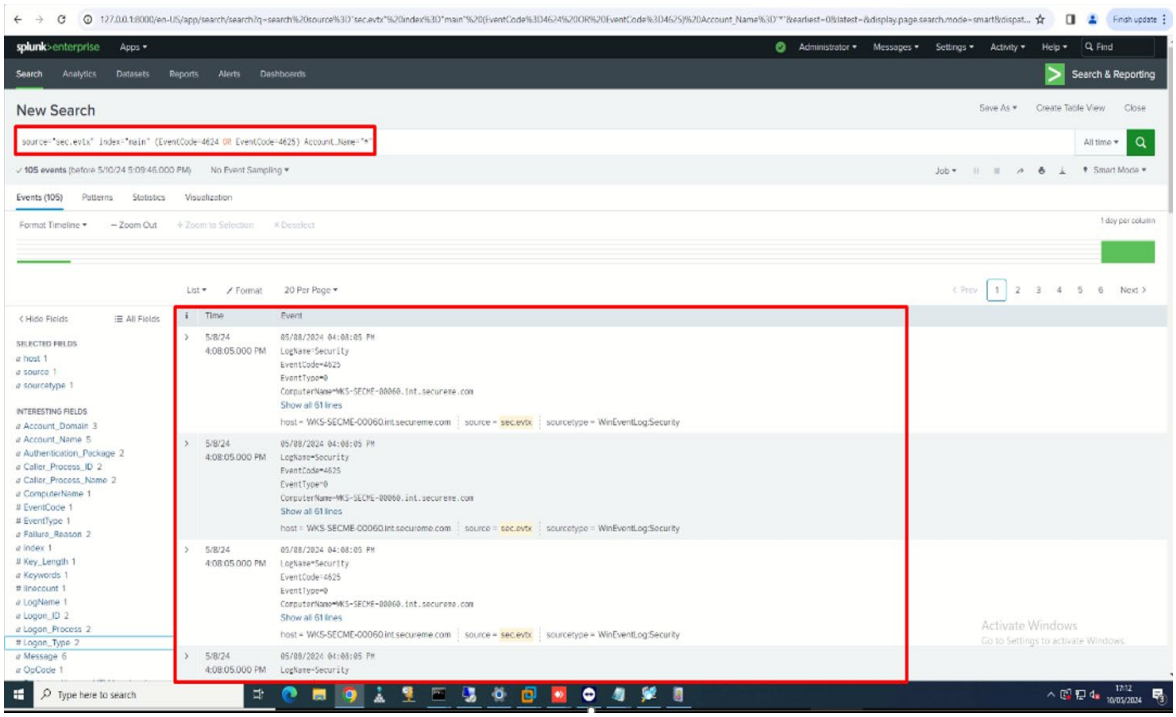

Figure 35: Digital Evidence of Failed Login Attempts (1)

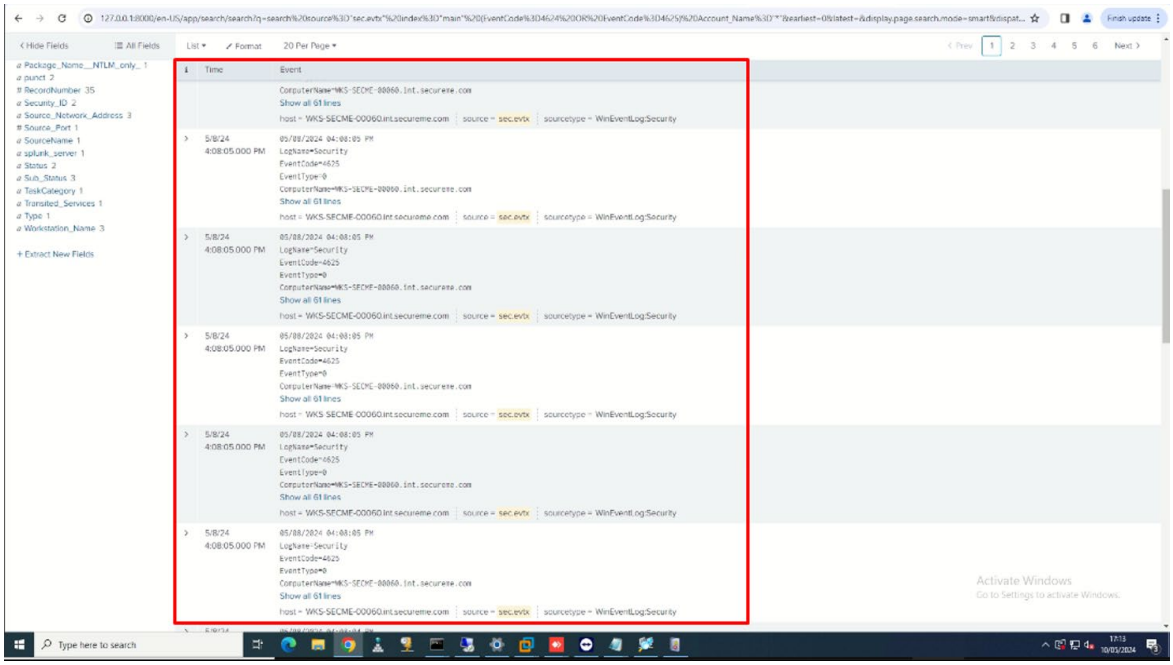

Figure 36: Digital Evidence of Failed Login Attempts (2)

8. We can also see successful login attempts and forensic evidence, as shown in Figure 41 below.

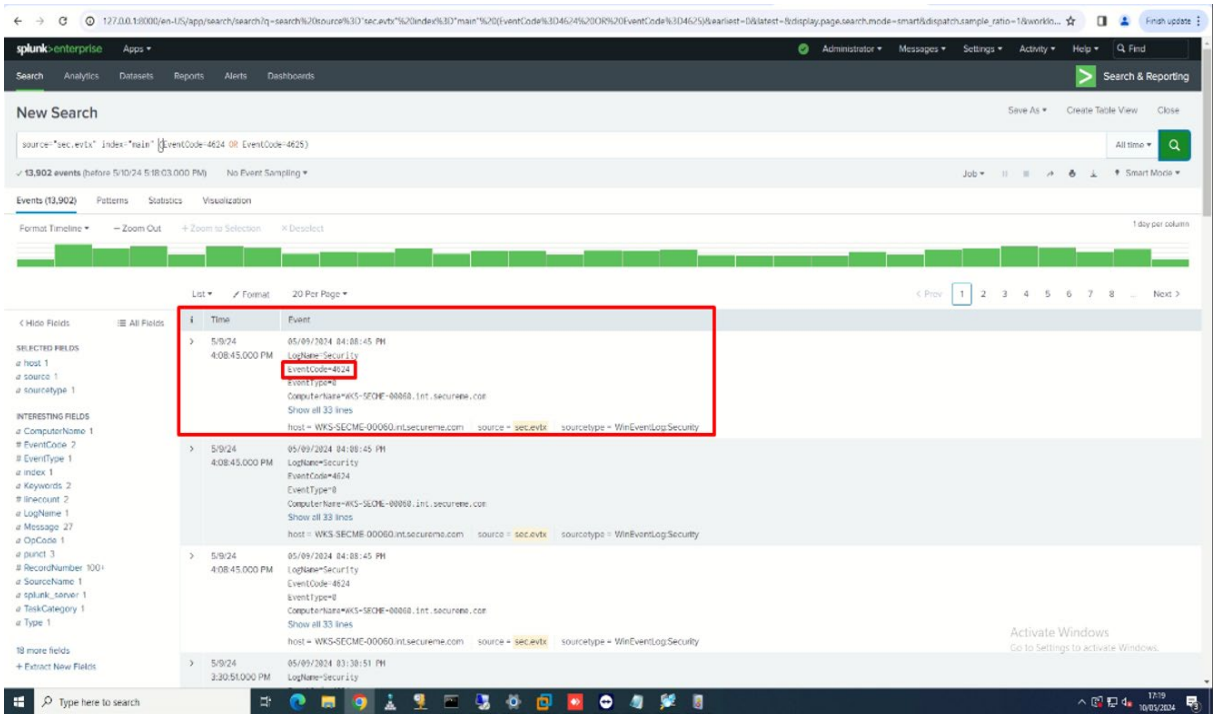

Figure 37: Digital Evidence of Successful Login Attempts

5.3 Scenario - Analysis and Forensic Readiness Implications

This scenario demonstrates the effectiveness of the proposed Digital Forensic Readiness (DFR) model in supporting proactive evidence generation, preservation, and traceability within an IoT-enabled organisational environment. While the detection of malicious activity confirms the functionality of the underlying security mechanisms, the primary contribution of this scenario is to illustrate how security events are systematically captured, correlated, and preserved in accordance with forensic readiness principles. The results show that potential digital evidence is automatically generated at the time of the incident, reducing the risk of data loss, contamination, or delayed acquisition.

From a forensic readiness perspective, this scenario highlights the model's ability to ensure the timely availability of relevant forensic artefacts, maintain chain-of-custody integrity, and minimise manual intervention during incident response. The structured logging and evidence correlation mechanisms enable investigators to efficiently and consistently reconstruct attack timelines, supporting both technical analysis and organisational decision-making. By embedding evidence-handling processes into routine security monitoring, the model demonstrates a shift from reactive, post-incident investigation to continuous forensic preparedness.

In addition, the scenario illustrates how the proposed DFR model supports coordination across organisational, technical, and security layers. Organisational policies and predefined procedures guide the activation of forensic processes, the technical layer ensures reliable evidence capture and preservation, and the security layer provides real-time alerts that trigger readiness workflows. This layered interaction confirms that forensic readiness is achieved not through isolated tools, but through an integrated organisational capability.

Overall, this scenario validates the practical applicability and robustness of the proposed DFR model by demonstrating how real-time monitoring and structured evidence handling improve investigative efficiency, reduce response time, and enhance organisational preparedness. Beyond confirming attack detection, the scenario provides empirical evidence that the model enables forensically sound, standards-aligned readiness, thereby supporting reliable investigations and strengthening organisational resilience in IoT-enabled environments.

5.3.1 Operational Workflow for Forensic Evidence Acquisition

The experimental attack scenarios implemented in this research operationalised the proposed forensic evidence acquisition workflow within a controlled organisational IoT environment. During the brute-force attack simulation, Wazuh agents continuously monitored authentication events, failed login attempts, system activities, and network communications generated by both attacker and victim systems.

Once abnormal authentication behaviour exceeded predefined thresholds, the Wazuh monitoring infrastructure generated real-time alerts and automatically preserved associated security logs within the central evidence repository. These logs included authentication timestamps, source IP addresses, user account activity, failed login sequences, event identifiers, and operating system security events relevant to the attack scenario.

The preserved forensic artefacts were subsequently exported and ingested into Splunk for advanced forensic analysis and event correlation. Splunk enabled investigators to examine attack timelines, correlate suspicious events across multiple systems, identify

Indicators of Compromise (IoCs), and reconstruct attacker activities using preserved log data. This process demonstrated how the implemented model supports the transition from intrusion detection to formal forensic investigation within organisational IoT infrastructures.

To maintain forensic integrity during evidence acquisition, all exported logs were preserved in their original format, accompanied by timestamp metadata and event context information. Access controls and audit logging mechanisms ensured that evidence remained protected against unauthorised modification throughout the investigative process.

5.3.2 Forensic Preservation and Investigation Workflow

The implemented forensic workflow demonstrates how Digital Forensic Readiness processes can be operationalised continuously within IoT-enabled organisational environments. The workflow integrates intrusion detection, real-time evidence collection, secure preservation, forensic analysis, and investigation reporting into a unified readiness architecture aligned with the principles of ISO/IEC 27043.

The operational forensic process begins with continuous monitoring and event detection using Wazuh. Once suspicious activities are identified, relevant logs and system artefacts are automatically preserved within secure forensic repositories. Preserved evidence is then transferred to the Splunk analysis environment, where investigators conduct correlation analysis, event reconstruction, and forensic examination using visual dashboards and search queries.

Throughout the investigation lifecycle, evidence integrity is maintained through secure storage procedures, timestamp preservation, audit trail generation, and integrity verification mechanisms. Chain-of-custody documentation is maintained continuously to record all evidence-handling activities, including acquisition, transfer, storage, access, and analysis.

This operational workflow demonstrates the practical implementation of forensic readiness principles within organisational IoT infrastructures by ensuring that evidence acquisition and preservation occur proactively rather than reactively after

incidents have escalated. Consequently, the model strengthens investigation efficiency, reduces evidence loss, and improves organisational preparedness for cybersecurity incidents and digital forensic investigations.

5.4 Chapter Summary

This chapter has presented a comprehensive overview of the preparation and setup required to detect and investigate cyber incidents using Wazuh and Splunk within a structured experimental environment, through the implementation of four distinct scenarios: brute-force attack detection, file integrity monitoring, unauthorised process detection, and denial-of-service (DoS) attack analysis. This study has demonstrated the practical capabilities of combining Wazuh's detection features with Splunk's forensic analysis tools.

Each scenario was meticulously designed to reflect real-world attack vectors, enabling the simulation and monitoring of malicious activities in a controlled environment. The integration of Wazuh enabled real-time threat detection, while Splunk facilitated deep forensic investigation and event correlation to trace attack origins, behaviour patterns, and impact. The configuration processes, alert generation, and log correlation techniques used across the scenarios provide a repeatable, scalable model for enhancing digital forensic readiness. Overall, the experimental setup highlights the effectiveness of these open-source and enterprise-grade tools in supporting proactive cybersecurity practices and incident response in modern IT environments.

6.0 Data Analysis for Cyber Attack Detection

6.1 Introduction

In this study, the analysis was conducted on network traffic data collected from the live network in May 2024. The main aim was to identify network traffic features that distinguish benign from malicious attacks, using a Random Forest Classifier to select and rank the most important features. The dataset, which includes features related to packet size, transmission speeds, and interarrival times, was examined to understand what differentiates each attack type. This study provides a comprehensive data-loading and preprocessing process, feature selection, model training, and visualisation of the most significant features for overall detection and for each attack type. We also present the most important features for each attack type and utilise them to enhance detection mechanisms for these attacks.

6.2 Dataset Overview

In this work, the dataset included several types of cyberattacks, such as DNS amplification (DDoS), brute-force attacks, and SQL injection. We captured network traffic over seven days (May 14th to May 23rd, 2024), including both benign and attack scenarios. The datasets used in this study are well-suited to IoT-enabled organisational environments because they capture network traffic characteristics, behavioural patterns, and attack types commonly observed in distributed, resource-constrained systems. IoT environments generate high-volume, heterogeneous, and time-sensitive data, often characterised by imbalanced class distributions and overlapping attack signatures. The selected datasets reflect these properties, enabling a realistic evaluation of forensic evidence patterns associated with IoT-based cyber incidents. This makes the datasets suitable not only for attack detection, but also for analysing the availability, relevance, and prioritisation of potential digital evidence within forensic readiness contexts. The breakdown of samples collected by attack type is outlined below.

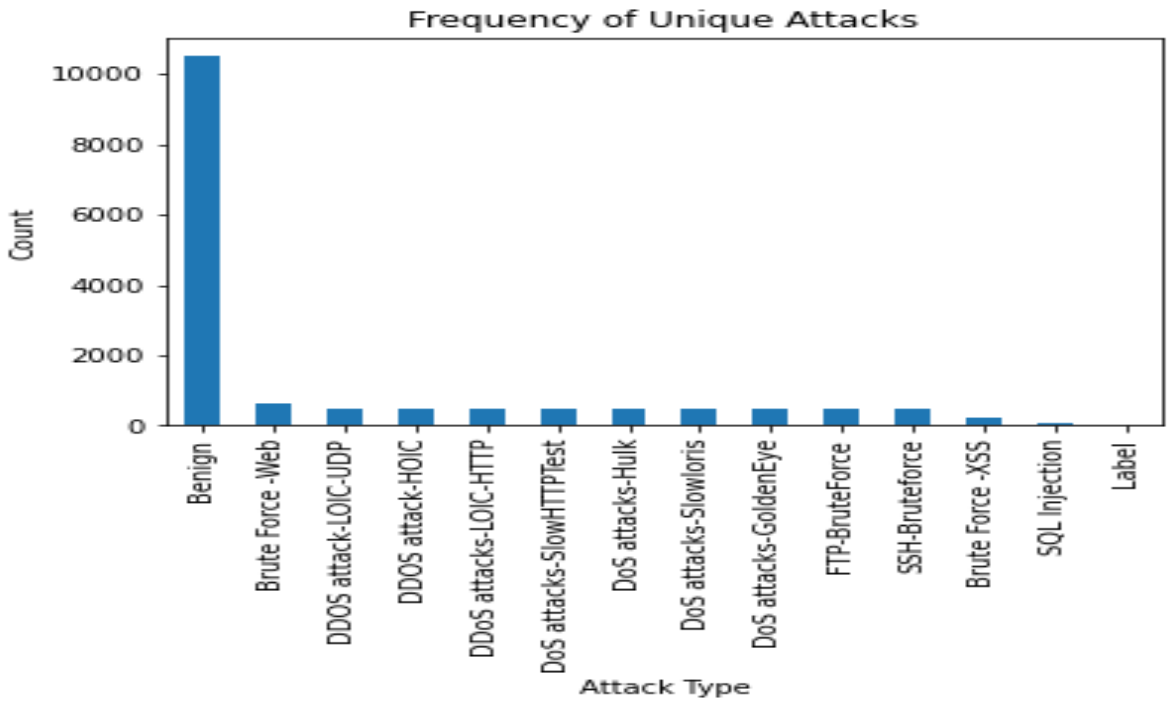

Figure 38: Frequency of Attacks

- Benign: 10,500 samples
- Brute Force - Web: 611 samples
- DDoS Attack - LOIC UDP: 500 samples
- DDoS Attack - HOIC: 500 samples
- DDoS Attack - LOIC HTTP: 500 samples
- DoS Attack - SlowHTTPTest: 500 samples
- DoS Attack - Hulk: 500 samples
- DoS Attack - Slowloris: 500 samples
- DoS Attack - GoldenEye: 500 samples
- FTP-BruteForce: 500 samples
- SSH-Bruteforce: 500 samples
- Brute Force - XSS: 230 samples
- SQL Injection: 87 samples

The dataset contains 79 features, including source and destination IP addresses, port numbers, flow duration, counts of forward and backwards packets, packet size statistics, and inter-arrival times.

The Wazuh Server primarily captures network traffic, security events, and anomalies, including source and destination IP addresses, port numbers, packet sizes, time intervals between packet arrivals, flow durations, and packet statistics, such as forward and backwards packet counts. The Wazuh Client, also installed on the victim machine, monitors Apache logs and looks for attacks such as SQL injection, brute-force, and DDoS. Additionally, IoT Logs from the subnet 192.168.0.x, where IoT devices are connected, record events such as normal traffic, DDoS attacks, and other incidents, including attacker and victim IP addresses, attack types, timestamps, and flow information, in the SECME IoT Database. Firewalls, of course, log allowed or denied traffic and can include notices of suspicious activities. Cloudflare secures external connections by logging malicious activity, such as DDoS traffic, and implementing security measures. All the logs mentioned above, totalling 79 features, were processed using appropriate techniques and saved in CSV format for analysis in the next stage. The following features are explained below.

- Flow Duration: Time in microseconds representing the total duration of any network flow.
- Total Forward and Backwards Packets: The number of packets sent and received in the flow.
- Forward and Backwards Packet Length: The packet size in the forward and backwards directions.
- Inter-Arrival Times (IAT): The time interval between consecutive packets.
- Flag Counts: The number of times certain flags, such as SYN, ACK, and RST, were set in the TCP header.
- Flow Bytes per Second: The rate of bytes transferred in a flow.

6.2.1 Dataset Description and Preprocessing

The dataset utilised in this research comprised cybersecurity network traffic and attack-related records to evaluate machine-learning-based cyberattack detection and forensic evidence analysis in IoT-enabled organisational environments. The dataset contained both benign and malicious traffic instances representing multiple attack categories, including brute-force attacks, Distributed Denial of Service (DDoS) attacks, SQL injection attacks, and denial-of-service activities.

The dataset was selected because it provides realistic network traffic behaviour and diverse attack scenarios suitable for evaluating forensic readiness, attack detection accuracy, and evidence prioritisation processes. The dataset included several traffic features associated with network communications, protocol behaviour, packet statistics, authentication activities, flow characteristics, and attack indicators.

- ✓ **Dataset Preprocessing:** Before machine learning analysis, the dataset underwent several preprocessing stages to improve data quality, analytical consistency, and model performance.

- ✓ **Data Cleaning:** Incomplete records, duplicate entries, and corrupted values were identified and removed to ensure dataset reliability and consistency. Null values and invalid records that could negatively affect classification performance were also eliminated during preprocessing.

- ✓ **Feature Selection:** Feature selection techniques were applied to identify the most significant variables associated with cyberattack detection and forensic evidence classification. Feature importance analysis was subsequently conducted using multiple machine learning classifiers to determine high-ranking attack indicators relevant to forensic investigations.

- ✓ **Data Transformation:** Categorical variables and non-numeric fields were transformed into machine-readable numerical representations suitable for machine learning analysis. Additionally, data normalisation and scaling techniques were considered to improve classification performance and reduce feature imbalance.

- ✓ **Dataset Balancing:** Class imbalance was analysed to minimise bias toward the majority traffic classes. Since cybersecurity datasets often contain significantly more benign traffic than attack traffic, evaluation metrics beyond simple accuracy were required to ensure reliable performance assessment.

6.2.2 Evaluation Metrics and Justification

The performance of the machine learning models and forensic readiness model was evaluated using multiple quantitative metrics: Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR), and True Positive Rate (TPR).

Accuracy was used to measure overall classification correctness; however, cybersecurity datasets frequently contain imbalanced attack distributions, making accuracy alone insufficient for reliable evaluation. Therefore, greater emphasis was placed on precision, recall, and F1-score metrics.

Precision measured the proportion of correctly identified attacks among all predicted attacks and helped evaluate the generation of false alerts. Recall measured the ability of the system to detect actual attacks and minimise missed incidents. The F1-score was particularly important because it provides a balanced assessment of precision and recall, making it more reliable for evaluating intrusion detection performance within imbalanced cybersecurity datasets.

False Positive Rate analysis was also included because excessive false alerts may undermine the efficiency of forensic investigations and operational incident response. These combined metrics provided a comprehensive evaluation of attack-detection effectiveness, evidence-prioritisation capability, and overall forensic-readiness performance within the proposed model.

6.2.3 Objectives of Analysing the Dataset

The main objectives of analysing the dataset are detailed below.

- Overall Feature Selection for All Attack Types: We first identified the 20 most significant features for detecting malicious network traffic across all possible attack types to address this task.

  Analysing these features yields insights into the features that differentiate regular traffic from potentially malicious activity. Focusing on these key features enables the model to effectively distinguish between benign and malicious traffic across all attack types.

- Attack-Specific Feature Selection: First, decide on the overall most essential

features, then perform an attack-specific one to determine which features are most important for each type of attack.

This also enabled us to identify the specific characteristics of each attack (packet-size variations, flow durations, interarrival times) that are essential for determining whether an attack has occurred. By understanding which features are crucial for each type of attack, we can improve our detection methods and increase the accuracy of identifying specific cyber threats.

- Manual Labelling for System Evaluation: The reduction to the selected 20 features was a crucial part of the process, enabling us to manually label our network traffic flows. This manual classification of flows into true positives, false positives, true negatives, and false negatives was used to assess the system's accuracy and performance.

6.3 Machine Learning Models for Cyberattack Detection: A Tree-Based Approach

Cybersecurity is a vital concern in today's digital landscape, especially in IoT-enabled organisational environments, where cyber threats are constantly evolving and becoming increasingly sophisticated. Timely and precise detection of cyberattacks is crucial not only for safeguarding sensitive systems and data but also for facilitating prompt forensic readiness actions, such as evidence preservation and event reconstruction. In this study, Python is utilised to implement and assess four tree-based ensemble machine learning models—XGBoost (XGB), BaggingClassifier, Extra Trees, and Random Forest—for automatic cyberattack detection and forensic evidence analysis.

These models were chosen for their robustness, scalability, and suitability for heterogeneous, high-dimensional data, which are typical of IoT network environments. Tree-based ensemble methods excel in situations involving noisy data, class imbalance, and complex feature interactions, all of which are common in real-world IoT traffic. Additionally, these models offer inherent interpretability through feature importance measures, enabling forensic analysts to understand which

attributes most significantly influence classification results. This transparency is especially crucial in forensic settings, where explainability and evidential reasoning are necessary to support investigations and potential legal scrutiny.

As the Internet becomes increasingly embedded within organisational infrastructures, corporate cyber environments have become attractive targets for malicious actors (Cochrane et al., 2021). These environments comprise multiple interconnected layers, including email systems, databases, and intranets, which collectively store highly sensitive and valuable information. The complexity and interdependence of these systems increase both the attack surface and the difficulty of forensic analysis following an incident. Consequently, automated and interpretable detection mechanisms are necessary to support continuous monitoring and readiness in such environments.

The purpose of this work is to examine how automated cyberattack detection and analysis can be performed using both previously collected datasets and live network data streams. Attacks are modelled as discrete sequences of events, enabling the identification of both known and previously unseen attack patterns. Rather than focusing solely on detection accuracy, the selected models are used to support forensic readiness objectives, including prioritising potential digital evidence, reducing investigative effort, and enabling timely forensic decision-making in dynamic IoT-enabled organisational networks.

6.3.1 XGBoost (XGB)

XGBoost (eXtreme Gradient Boosting) is an ML technique for classification and regression tasks. It builds trees sequentially, improving performance iteratively. The operations of adding a new tree and adjusting previous weights are learned from previous trees, leading to better learning at fog trees. As the name suggests, XGBoost is an enhanced version of gradient-boosted trees. Its design focuses on boosting parallel trees. Hence, XGBoost runs on multiple cores and excels with data partitioning techniques (Alqahtani et al., 2019).

XGBoost has a gradual growth strategy, constructing trees in multiple layers. Reducing the number of feature-splitting locations across different tree structures speeds up computations (Alqahtani et al., 2019). XGBoost is an efficient, scalable implementation of gradient-boosting trees, widely used in data mining and machine learning competitions. It employs an ensemble of trees in a forward, stage-wise manner, where each new tree helps to mitigate the loss of its predecessor. The key innovation in XGBoost is a novel tree boosting algorithm that can be solved effectively using approximations and resources, including data compression, quantile sketches, and optimisation of cache performance, which enable parallel and distributed computing (Chen and Guestrin, 2016).

XGBoost is an adaptation of the Gradient-Boosting method for classification tasks. Trees that can selectively accept features that help solve the classification problem are repeatedly added via a weighted combination. Gradient boosting can be viewed as a stochastic forest in which multiple trees are trained independently. Trees grow on randomly selected sub-datasets, and subsequent trees are formed that reject features that have already had splits in previous trees (Chen and Guestrin, 2016).

6.3.2 BaggingClassifier

Bagging, also known as bootstrap aggregating, was among the earliest ensemble learning techniques introduced. It merges multiple versions of the same algorithm by using random training sets drawn from the original dataset. Each model is trained separately and then combined, often via majority voting.

An ensemble learning algorithm combines multiple simple classifiers to produce a more accurate classifier. Rather than searching for a single optimal classifier, ensemble learning combines several weak or inaccurate classifiers to produce a more accurate classifier, thereby improving performance. Ensemble learning approaches are often classified as homogeneous or heterogeneous. Homogeneous ensemble approaches construct multiple identical classification models (Iwendi et al., 2020). Heterogeneous ensemble approaches combine numerous different models. Random forests are well-known heterogeneous ensemble methods that construct multiple decision trees.

Bagging-based ensemble classifiers are widely used as standard models across several domains.

In classification problems, bagging and classifier combinations are widely used. Bagging evaluates the performance of several models constructed via data resampling. Random subsets are drawn from the original training set, and predictions from each model are combined via majority voting. Bagging has shown superior performance compared to single models in terms of prediction accuracy and robustness (Iwendi et al., 2020). Given these merits, bagging has been widely applied in various domains, including medical diagnosis and medical imaging. Data poisoning is a significant threat and often leads to a decline in prediction performance. Reverse engineering generated by such data poisoning attacks is usually costly and considered beyond reach.

The bagging ensemble method, known as Bootstrap Aggregating, enhances classification performance by combining weak classifiers into a stronger model. By training multiple weak classifiers on bootstrapped samples and aggregating their predictions, bagging addresses several classifier-related problems, including overfitting, data noise, and imbalanced datasets. Additionally, bagging increases robustness and accuracy by generating diverse classifiers from a single training dataset. The outcome depends on the aggregation function, which combines the predictions of all individual base classifiers. Bagging involves generating random subsamples with replacement from a dataset or user pool. Base estimators, each trained on the same input, yield predictions with lower variance than those of strong classifiers.

The aggregation component of the identification and labelling system comprises three modules designed to address potential difficulties and biases within classifier predictions. The preprocessing step processes classifier predictions. In the next stage, a classifier-similarity computation and a layered graph construction are employed to build the layered graph. Then, a local refinement step maps the prediction counts from the initial classifiers to the predictions of a smaller set of final classifiers. The final adjusted prediction count is computed through a weighted bidirectional search and

applied to the final labelling. BaggingClassifier is implemented using the Scikit-learn package and is considered a simple ensemble model. BaggingClassifier aggregates multiple base estimators and can use redundant estimators to reduce variance; it uses an adjacency graph-based local refinement that maps estimates from trained classifiers to classes supported by an adapted local model and enables exploratory compatibility scoring with any pairwise matching criterion to inform candidate oracle selection (Iwendi et al., 2020).

6.3.3 Extra Trees

Extra Trees, or extremely randomised trees, consist of a collection of trees, each trained on a different bootstrap sample of the training data. A tree predictor is constructed by recursively partitioning the data into two daughter nodes. When splitting criteria are based on a random feature and a random threshold, as in trees, the predictor tree has considerably fewer leaf nodes than standard trees. Each tree has its own voting weight, determined as the tree is built. Ensemble methods can integrate detection algorithms with other algorithms. Generalisation errors decrease, and accuracy improves further, particularly when techniques are diversified.

Extra Trees are robust to noise and overfitting. The average-case time complexity of classification with Extra Trees is O(k), where k denotes the number of trees in the forest. Computational time is determined by the O(1) time complexity per tree and the number of trees. The classification of input features will be done on two collections of trained forests. The classifier's votes are tallied afterwards, and the class with the highest tally is returned as the predicted class. Voting time is, therefore, O(k) (Cochrane et al., 2021).

Detection algorithms can be applied to various ML prediction outputs (Devos, Meert and Davis, 2022). The idea is to incorporate them into ML libraries, but this would require effort from library maintainers. Since they use externally defined classes, detection occurs at runtime. Nevertheless, they can be passed as additional parameters when using the library's API or wrapper classes. The classification process would become substantially more complex than that implemented in scripts. Each prediction class is responsible for detection, and the metrics presented vary by model.

6.3.4 Random Forest

A Random Forest model is an ensemble of decision tree classifiers that makes collective predictions. For each new case where a prediction needs to be made, each decision tree casts a "vote", and the output class is the one with the most votes. This approach overcomes the tendency of decision trees to overfit if used in isolation. Trees learn rules based on feature thresholds, mapping different ranges of input data to different outputs. Oftentimes, a single rule suffices to fit a significant fraction of the data perfectly. In areas where the data have different distributions, additional trees are built, which are more likely to produce different thresholds and thus yield different predictions. Here, random forests improve upon decision trees by reducing the variance and bias of their predictions without compromising interpretability (Santana, Suthaharan and Mohanty, 2018). The strength of the Random Forest lies primarily in the aggregation method employed and the randomness introduced into the procedure. For each tree in the ensemble, a smaller set of randomly selected features is used to fit the tree. Therefore, the node split is randomised, and splits can happen on smaller sets of features compared to those used in the whole pool of attributes (Vitorino et al., 2024).

The Random Forest is a supervised machine learning algorithm used for both classification and regression problems. It employs ensemble learning to train multiple decision trees and outputs the class with the highest frequency (classification) or the mean prediction (regression) across the individual trees. It is widely used for its high accuracy and low overfitting (Biau and Scornet, 2015). Obtaining a clear understanding of the Random Forest classifier is critical to utilising and, if necessary, improving it for detection. A Random Forest is composed of several decision trees. During training, Random Forest selects a random sample from the training dataset, which in turn uses a random subset of features to build the tree. The trees are constructed recursively, and each node has a candidate split that maximises information gain. A reduction in uncertainty about the labels yields information gain. After building the forest, the Random Forest outputs the class label via majority voting.

Random Forests can be applied to both categorical and continuous classes; however, the default implementation is for categorical cases. The design of Random Forest primarily consists of two steps: (S1) initialising and training trees (decision trees), and (S2) building a classifier to output the label.

6.3.5 Machine Learning Hyperparameter Settings and Optimisation

This research employed multiple machine learning classification models to evaluate the effectiveness of cyberattack detection and the prioritisation of forensic evidence within IoT-enabled organisational environments. Hyperparameter tuning and optimisation procedures were conducted to improve classification accuracy, reduce overfitting, and enhance model generalisation performance.

1. **XGBoost (XGBClassifier)**

The XGBoost model was selected for its strong performance in cybersecurity classification tasks, gradient-boosting optimisation capability, and support for feature importance analysis. The following hyperparameters were configured:

- Number of estimators: 100
- Maximum tree depth: 6
- Learning rate: 0.1
- Subsample ratio: 0.8
- Evaluation metric: log loss

These parameters were selected after experimental evaluation to balance detection accuracy and computational efficiency. Increasing the number of estimators improved classification capability but also increased training complexity; therefore, moderate parameter values were selected to optimise performance while preventing overfitting.

2. **Random Forest Classifier**

The Random Forest model was implemented because of its robustness, ensemble learning capability, and resistance to overfitting. Configured parameters included:

- Number of decision trees: 100
- Maximum depth: unrestricted
- Random state initialisation enabled

- Feature sampling enabled.

The model provided strong classification stability and supported feature-importance analysis, which is useful for forensic evidence prioritisation.

3. **Extra Trees Classifier**

The Extra Trees classifier was selected because it introduces additional randomness during tree construction, improving generalisation and reducing variance. Parameters included:

- Number of trees: 100
- Random splitting enabled
- Gini impurity criterion

The model demonstrated efficient attack classification performance and produced highly informative feature importance rankings.

4. **BaggingClassifier**

The BaggingClassifier was implemented to improve classification stability using bootstrap aggregation. Configured parameters included:

- Number of base estimators: 50
- Bootstrap sampling enabled
- Random state initialisation enabled

Bagging improved robustness against noisy traffic data and reduced model instability during classification.

6.3.5.1 Hyperparameter Optimisation Rationale

Hyperparameter settings were selected through iterative experimental testing and comparative performance evaluation. The optimisation process focused on:

- Maximising detection accuracy.
- Reducing false positive rates.
- Improving recall performance.
- Enhancing F1-score reliability.
- Preventing overfitting.
- Maintaining computational efficiency.

Particular emphasis was placed on F1-score optimisation because cybersecurity datasets often exhibit class imbalance between normal and malicious traffic classes.

6.3.5.2 Alternative Machine Learning Models Considered

During the implementation and evaluation phase of this research, several alternative machine learning algorithms were considered for cyberattack detection and digital forensic readiness within IoT-enabled environments. These included:

- Support Vector Machine (SVM)
- Logistic Regression
- K-Nearest Neighbour (KNN)
- Deep Neural Networks (DNN)
- Long Short-Term Memory (LSTM)

Each of these models has been widely applied in cybersecurity and intrusion detection research and offers distinct advantages. Support Vector Machines are effective for high-dimensional datasets and can provide strong classification performance when clear decision boundaries exist between classes. Logistic Regression offers simplicity, computational efficiency, and ease of implementation, making it suitable for baseline classification tasks. K-Nearest Neighbour is a non-parametric method capable of identifying similarities between observations; however, its performance can deteriorate when processing large datasets due to increased computational requirements.

Deep learning approaches, including Deep Neural Networks and Long Short-Term Memory networks, were also considered for their ability to learn complex patterns and relationships from large volumes of security data. DNN models can capture nonlinear relationships among multiple variables, while LSTM networks are particularly effective for analysing sequential and time-dependent data, making them suitable for modelling attack behaviours that evolve over time. Despite these advantages, deep learning models typically require substantial computational resources, longer training times, and larger datasets to achieve optimal performance. Furthermore, their internal decision-making processes are often difficult to interpret,

posing challenges when explaining forensic findings to investigators, management, or legal stakeholders.

Following comparative evaluation, tree-based ensemble models were selected as the most appropriate approach for this research. Models such as Random Forest, Extra Trees, Bagging, and XGBoost demonstrated superior classification performance while maintaining a balance between predictive accuracy and interpretability. These models were capable of handling high-dimensional security data, reducing the risk of overfitting, and providing robust performance across different attack categories.

A key advantage of tree-based ensemble methods is their ability to generate feature-importance rankings, enabling investigators to identify which network attributes, system events, or behavioural indicators contributed most to attack detection. This capability is particularly valuable in digital forensic investigations, where understanding the reasoning behind a classification decision is often as important as the detection itself. The transparency provided by feature importance analysis supports evidence interpretation, incident reconstruction, and decision-making during forensic investigations.

Additionally, tree-based models exhibited lower computational complexity than deep learning approaches, enabling efficient deployment in resource-constrained IoT environments. Their ability to deliver high detection accuracy while maintaining explainability and operational efficiency made them particularly suitable for supporting Digital Forensic Readiness (DFR) objectives. Consequently, tree-based ensemble models were adopted as the primary classification approach within the proposed Digital Forensic Readiness Model developed in this study.

6.4 Feature Selection Using Four Different Classifiers

The four models were trained on the dataset, and feature importances were computed to identify which features most strongly contribute to classifying benign versus malicious traffic. The dataset was split into training and testing sets with a 70:30 ratio. The training set was used to train the models, and important features were extracted. Four tree-based models, XGBoost (XGB), BaggingClassifier, Extra Trees, and Random

Forest, were trained to detect cyberattacks, and all of them produced a feature importance ranking.

```
# Split the data into training and test sets
X_train, X_test, y_train, y_test = train_test_split(
    X, y, test_size=0.3, random_state=42
)

# Define models
models = {
    "Random Forest": RandomForestClassifier(n_estimators=100, random_state=42),
    "AdaBoost Classifier": AdaBoostClassifier(n_estimators=100, random_state=42),
    "LightGBM": LGBMClassifier(n_estimators=100, random_state=42),
    "Extra Trees (Light)": ExtraTreesClassifier(n_estimators=50, max_depth=5, random_state=42)
}
```

Figure 39: Code Snippet for Model Training

6.4.1 Overall Feature Importance

The following are the descriptions of the most important features, each of which is ranked most important (the higher the value, the more critical the feature was in the model's decision):

- **XGBoost (XGBClassifier):** The top features were Destination Port, Forward Packets per Second (Fwd Pkts/s), Forward Packet Length Std (std), Flow Packets/s (packets per second), Forward Act Data Pkts (number of data packets going in the forward direction), Flow IAT Std (inter-arrival time std), Total Forward/Bwd Packets, Packet Length Std (general), Bwd Packet Length Max (maximum in the backward direction), Forward Segment Size Min, Initial Fwd Win Bytes (initial size of forward window), Fwd Packet Length Mean, Total Length of Bwd Packets, RST Flag Count, Packet Length Max, Idle Mean, Initial Bwd Win Bytes, and Timestamp. (Most are network flow features such as packet lengths, counts, and flags.)

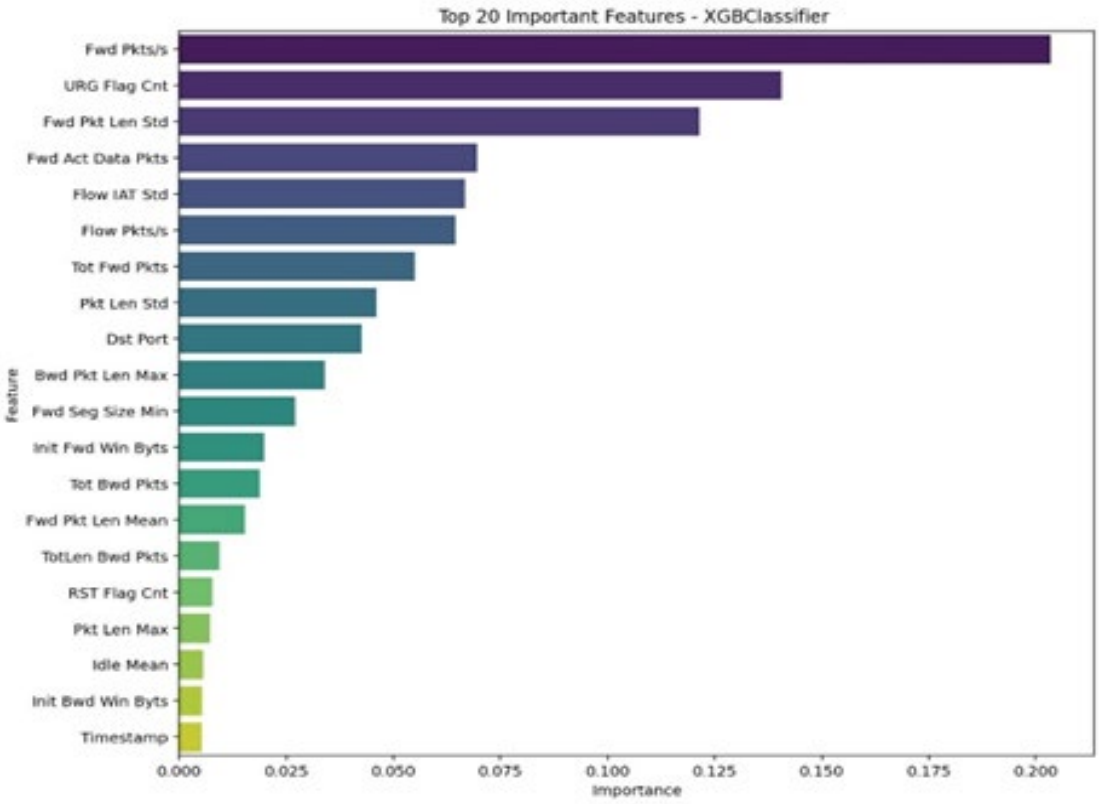

Figure 40: XGBClassifier - Top 20 Important Features

- **BaggingClassifier (bagged decision trees):** Discovered similar features like Fwd Pkts/s, Dst Port, Fwd Packet Len Std, Init Fwd Win Bytes, Flow Pkts/s, Timestamp, Flow IAT Std, Idle Mean (and Idle Std), Fwd Seg Size Min, URG Flag Count, Packet Len Std, Fwd Seg Size Avg (average forward segment size), Fwd Packet Len Mean, Fwd Header Length, Subflow Bwd Bytes (total bytes in backward subflow), Fwd IAT Mean, Bwd Pkts/s (backward packets per sec), ECE Flag Count, and TotLen Bwd Pkts. (Bagging's list is almost the same as Random Forest's, as both are ensembles of trees with bootstrapping.)

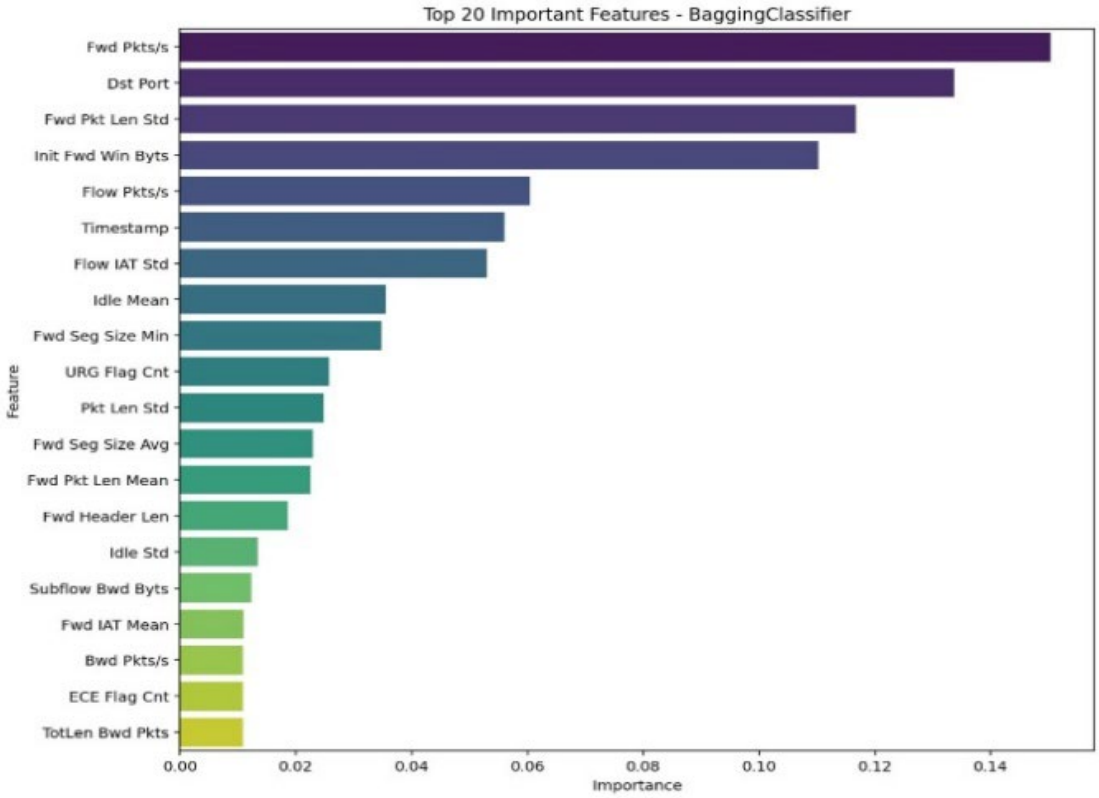

Figure 41: BaggingClassifier - Top 20 Important Features

- **Extra Trees (ExtraTreesClassifier):** The leading features were Init Fwd Win Bytes, Fwd Seg Size Min, PSH Flag Count, Dst Port, RST Flag Count, Fwd Packet Len Std, ACK Flag Count, ECE Flag Count, Fwd Header Len, Fwd Seg Size Avg, Packet Len Std, Fwd IAT Mean, Flow IAT Mean, Bwd Packet Len Std, Flow IAT Std, Fwd Packet Len Mean, Fwd IAT Min, Bwd Pkts/s, Bwd Packet Len Max, and Idle Min. (Extra Trees, being a collection of randomised trees, introduced some TCP flag counts such as PSH/ACK/ECE flags in its leading features.)

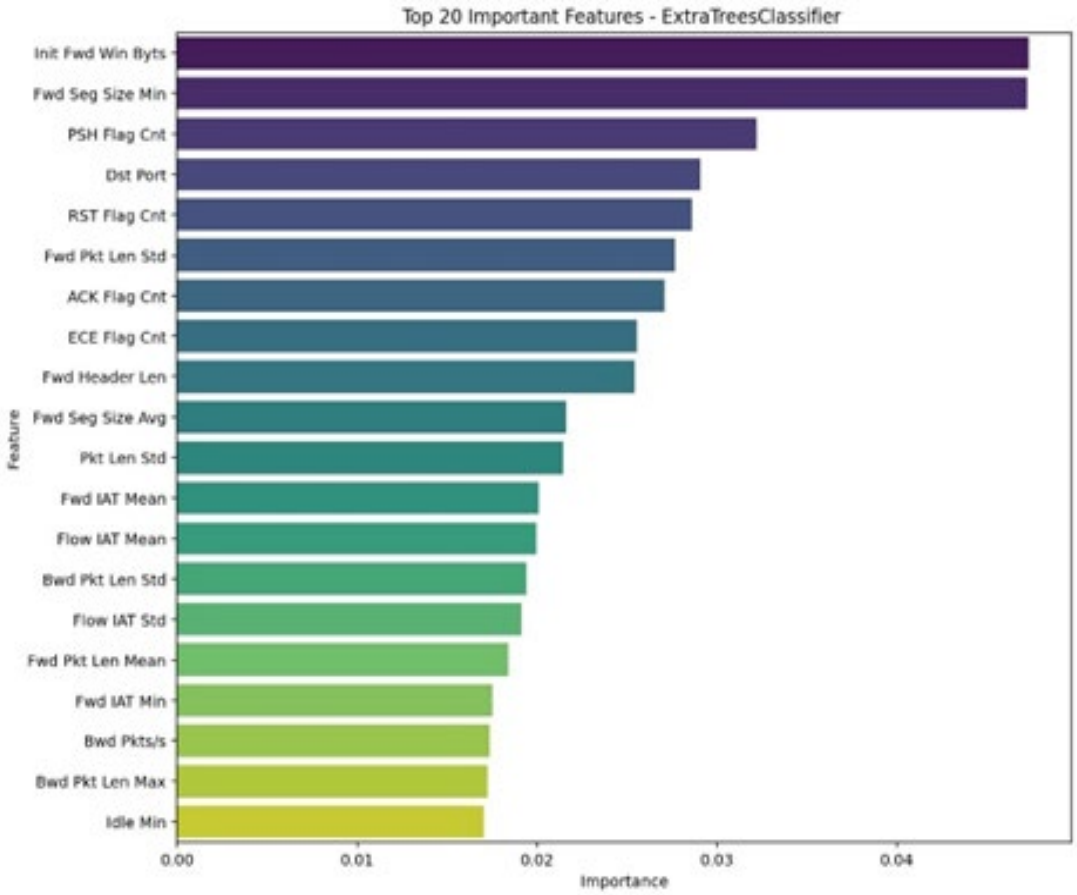

Figure 42: ExtraTreesClassifier - Top 20 Important Features

- **Random Forest:** Determined Dst Port, Init Fwd Win Bytes, Fwd IAT Min, Fwd Seg Size Min, Fwd Packet Len Mean, Fwd IAT Mean, Timestamp, Flow Pkts/s, Fwd Seg Size Avg, Fwd Pkts/s, Fwd IAT Max, Bwd Packet Len Max, Flow IAT Min, Packet Len Std, Bwd Packet Len Std, Fwd Header Len, PSH Flag Count, Fwd Packet Len Std, Flow IAT Mean, and Idle Max as its top 20. (Random Forest's most important features overlap significantly with Bagging's, but also include a set of Fwd IAT timing features.)

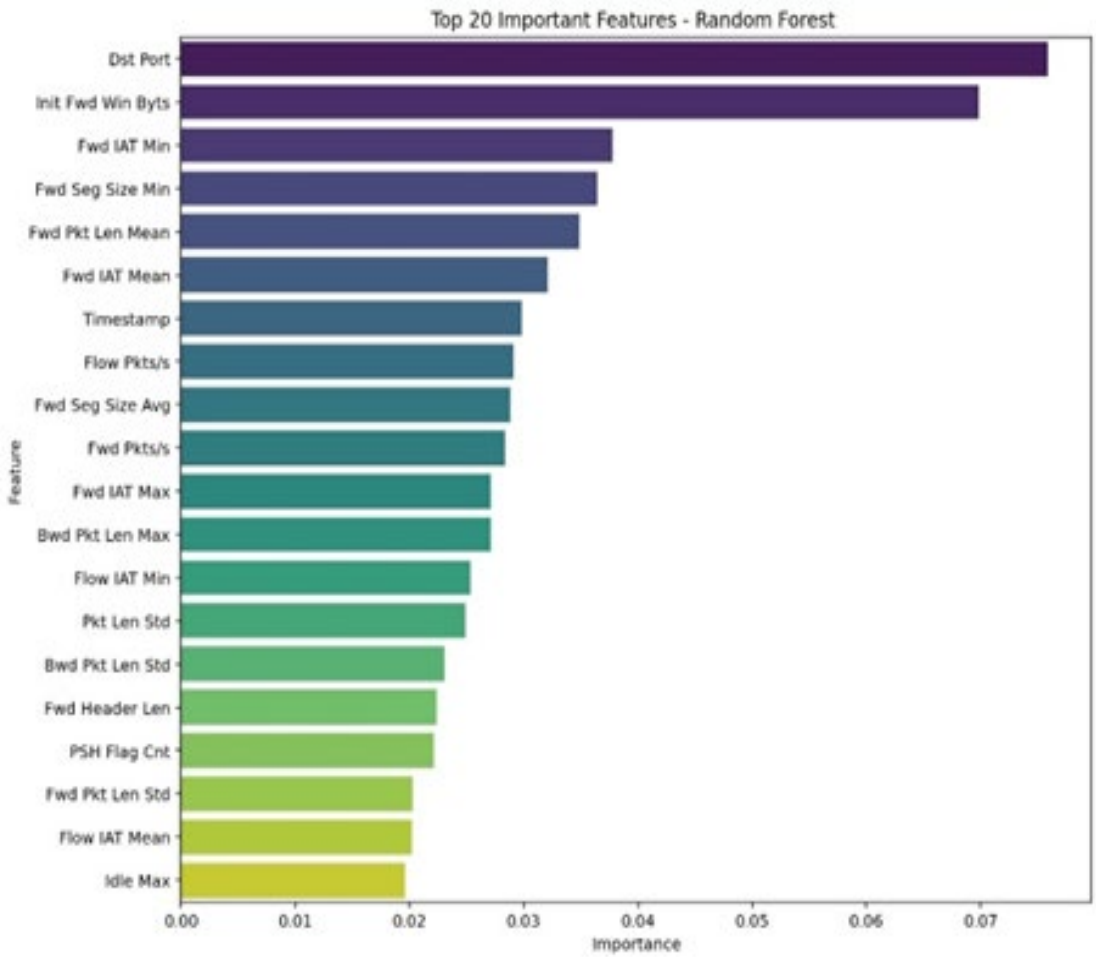

Figure 43: Random Forest - Top 20 Important Features

6.4.2 Common High-Ranking Features Across Models

Several features were ranked as very important by all four models, suggesting these are good indicators of cyberattacks by the algorithm:

- **Destination Port**: Displayed in the top features of XGBoost, Bagging, ExtraTrees, and Random Forest. This reveals that the network port through which a flow travels is a significant feature (most attacks use specific or uncommon destination ports).

- **First Forward Window Bytes**: Highest-ranked among all models. TCP's initial forward window size may indicate malicious behaviour (e.g., some attacks employ uncommon window sizes).

- **Forward Segment Size (Min)**: Detected by all models. The existence of a minimum forward segment size as a significant factor suggests that packet

segmentation behaviour is important, and that attacks can always utilise small or fixed packet segments.

- **Forward Packet Length Mean & Std**: Both the mean and standard deviation of forward packet lengths are among the highest attributes across models. This indicates that the packet-size distribution in the forward direction is a reliable indicator of attack traffic (attack traffic typically exhibits distinct packet-size patterns).

- **Packet Length Std (Total)**: Total packet size variation in a flow was highly ranked by all models. Variations in packet size, large or small, can differentiate normal from malicious traffic.

Also, a group of other characteristics, not all four possessing them, however, appeared at the top of the majority of models (appearing in three of four):

- **Fwd Pkts/s and Flow Pkts/s**: Packet rate features were an important characteristic in XGBoost, Bagging, and Random Forest. Large packet rates (either the forward-only packet rate or the aggregate flow rate) are likely indicative of scans or DoS attacks.

- **Timestamp**: The temporal component (if there was one) was accounted for by XGBoost, Bagging, and RF – perhaps capturing day-of-week patterns or order effects in the data.

- **Flow IAT Std/Mean**: Packet inter-arrival time statistics of the flow were presented in three models. This shows that burstiness or periodicity can indicate an attack.

- **Bwd Packet Len Max**: The maximum reverse packet length mattered for XGBoost, ExtraTrees, and RF. Large response packets, or the lack thereof, might differentiate certain attack types.

- **Forward Header Length & Fwd Seg Size Avg**: These were present in Bagging, ExtraTrees, and RF, suggesting that average forward segment length and header length are useful features overall.

Because these features consistently emerge as important across multiple modelling techniques, they can be considered reliable indicators of cyberattacks – they capture traffic traits that persistently distinguish malicious flows from benign ones.

6.4.3 Top Indicators for Pinpointing Cyberattacks

Observing the shared trends in each of the four models, some features emerge as the most persistent markers of cyberattack traffic:

- **Network Port (Dst Port):** Always a leading feature in all the models. This indicates that malicious flows tend to target specific ports or use non-standard port numbers (e.g., for port scanning or to exploit particular services). Observing destination port usage is crucial in intrusion detection.

- **Packet Length Measurements:** Attributes such as forward packet length mean & standard deviation (and total packet length variance) were ranked the highest by all models. These indicate the typical packet size in the traffic – most attacks (e.g., DoS floods or port scans) employ non-standard packet sizes or repeated packet lengths. These high measures across all models indicate that packet size patterns used by attackers are a strong indicator.

- **Traffic Rate/Volume Features:** Packet counts (e.g., total forward/backwards packets, etc.), Flow Pkts/s, and Fwd Pkts/s were ranked highly. Unusually low-volume traffic or high-rate bursts both signal malicious traffic. A DoS attack may have an extremely high packet rate, while a silent scan may have a normal rate but an abnormal port pair and packet size. Models collectively identified packet rate and count features as effective predictors.

- **TCP Header Window Sizes and Flag Counts:** These models found counts of TCP flags (URG, PSH, RST, ACK, ECE) and initial window sizes to be important, as these flags and window sizes are uncommon in regular traffic but can be present in attacks or scans, and a high number of certain flags can signal

anomalies. Similarly, an unusual initial window size can also indicate crafted traffic. While all models did not agree on which flag is most important, the overall observation is that anomalies in TCP/IP headers (flags, window size, and header length) are all critical for identifying attacks.

- **Timing and Idle Time Features:** Inter-arrival times (IAT) and Idle Time (gaps between the flows) were also captured by some models. Very low IAT (packets arriving one right after another, like a flood) or high idle times (significant gaps, such as during some scans or Slowloris attacks) are good indicators here. Having at least one "IAT" or "Idle" feature in each model's top list suggests that the temporal behaviour of traffic is an essential dimension in distinguishing attacks.

By focusing on the features that were universally or most frequently mentioned by the models, we can be certain of their significance. For example, suppose all models, regardless of variation, had identified Destination Port and Packet Length Std as significant. In that case, those are likely to be substantial for attack detection (not due to the bias of an individual algorithm). On the other hand, features that were significant only in a single model (e.g., Subflow Bwd Bytes in Bagging alone) may be less robust in isolation and could be replaced by other similar features.

6.5 Important Features for Each Attack

We trained each model for the different attack types, treating each attack as a binary classification problem, i.e., distinguishing it from all other attacks. We obtained feature importance scores from each classifier and identified the top 5 most essential features for each attack. Then we visualised these features to assess their value in identifying specific attacks. Below is a detailed interpretation of each attack.

6.5.1 Brute Force – Web

In all models, "Timestamp" is consistently the most prominent feature, strongly supporting the notion that timing patterns are a robust discriminator between brute-force attacks and regular web access. Moreover, the "Dst Port" is overwhelmingly dominant in the XGBoost and Bagging models, indicating that specific targeted ports play a crucial role in detecting such attacks.

"Init Fwd Win Byts" is essential, particularly in the ExtraTrees and Random Forest models, indicating that the initial forward window byte size also contributes to detecting brute-force activity. Overall, tracking timestamps, destination ports, and initial forward window bytes is crucial for effectively detecting and preventing brute-force web cyberattacks.

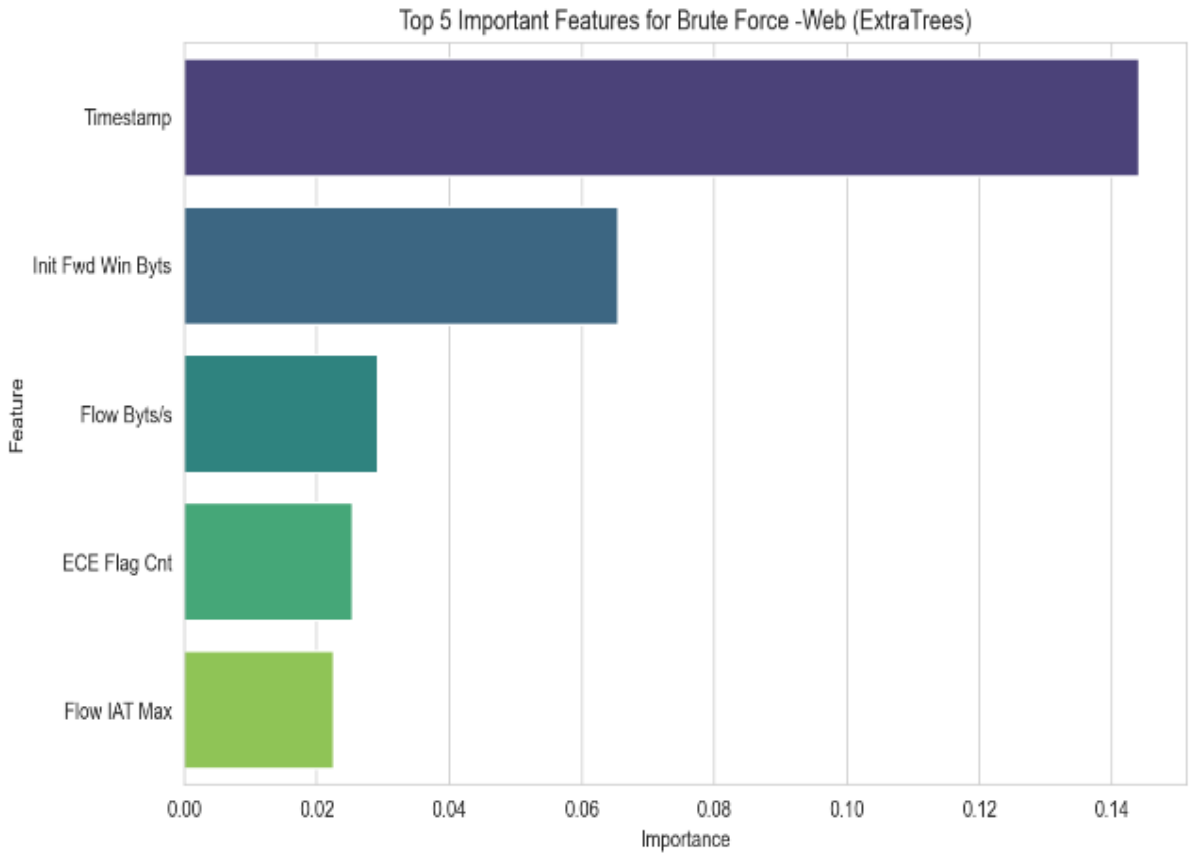

Figure 44: Important Features for Brute-Force – Web (Extra Trees)

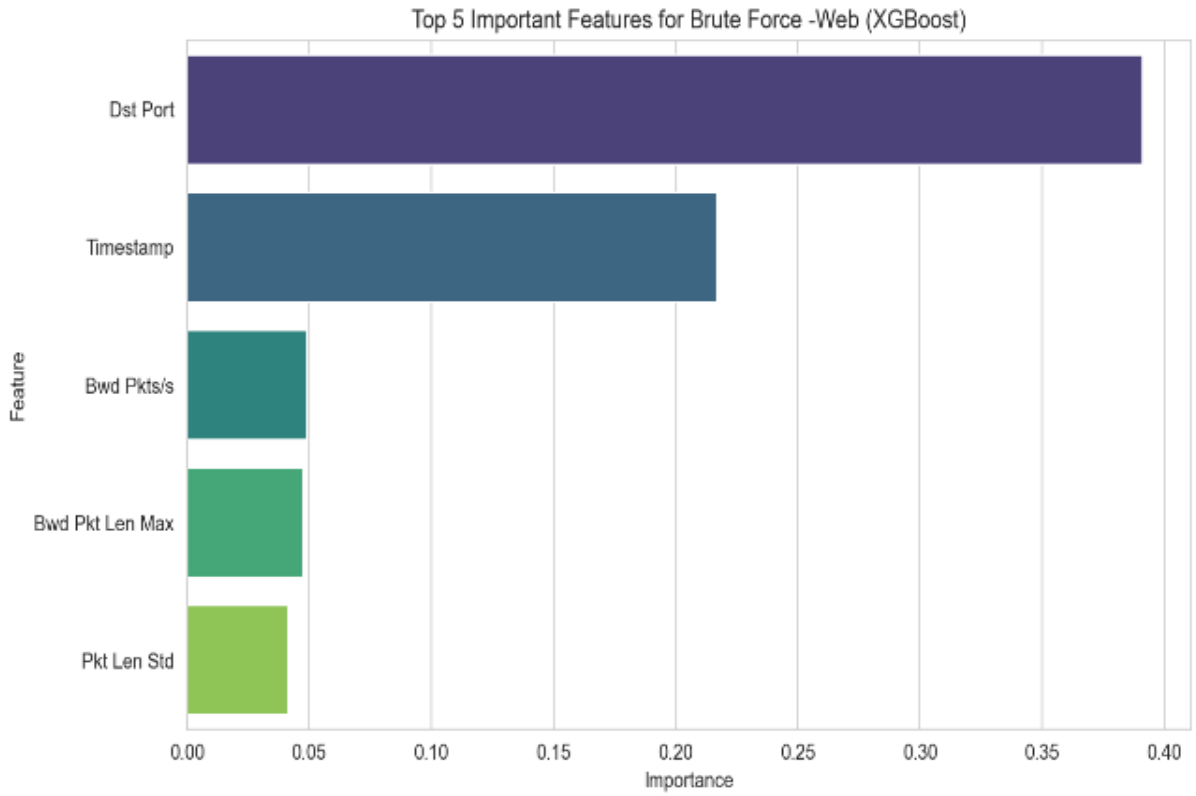

Figure 45: Important Features for Brute-Force - Web (XGBoost)

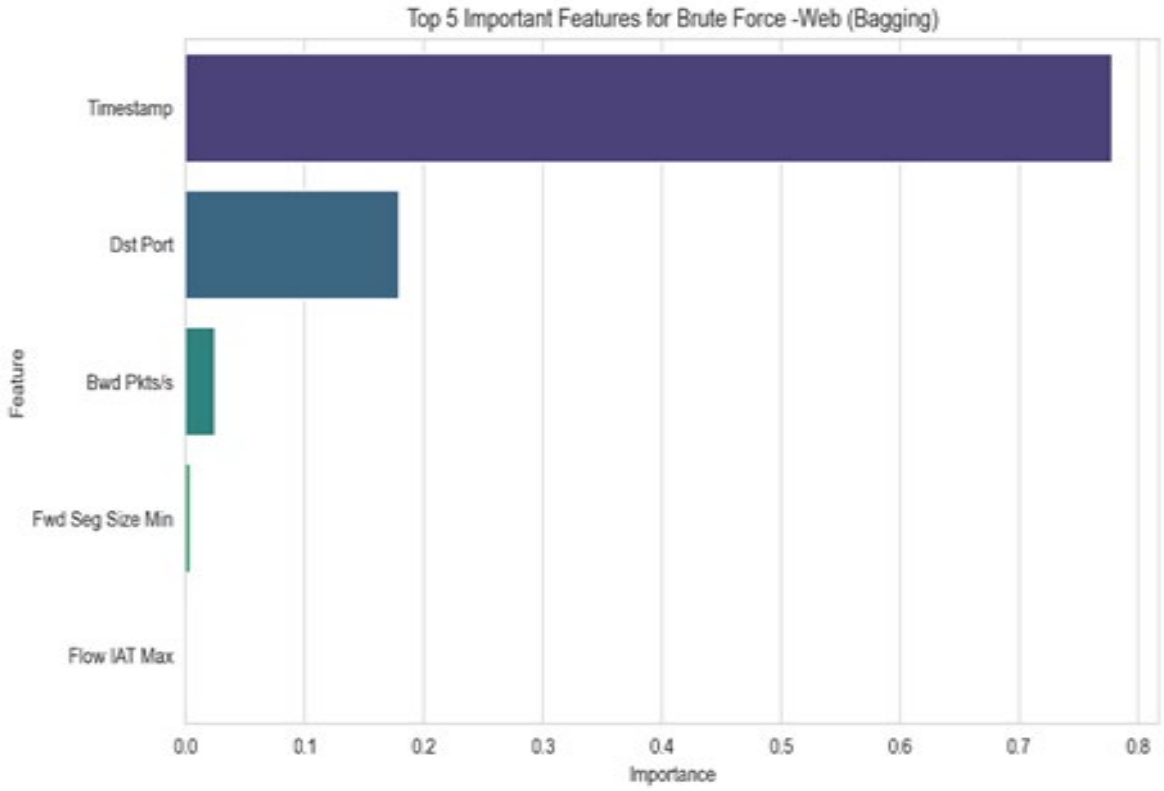

Figure 46: Important Features for Brute-Force - Web (Bagging)

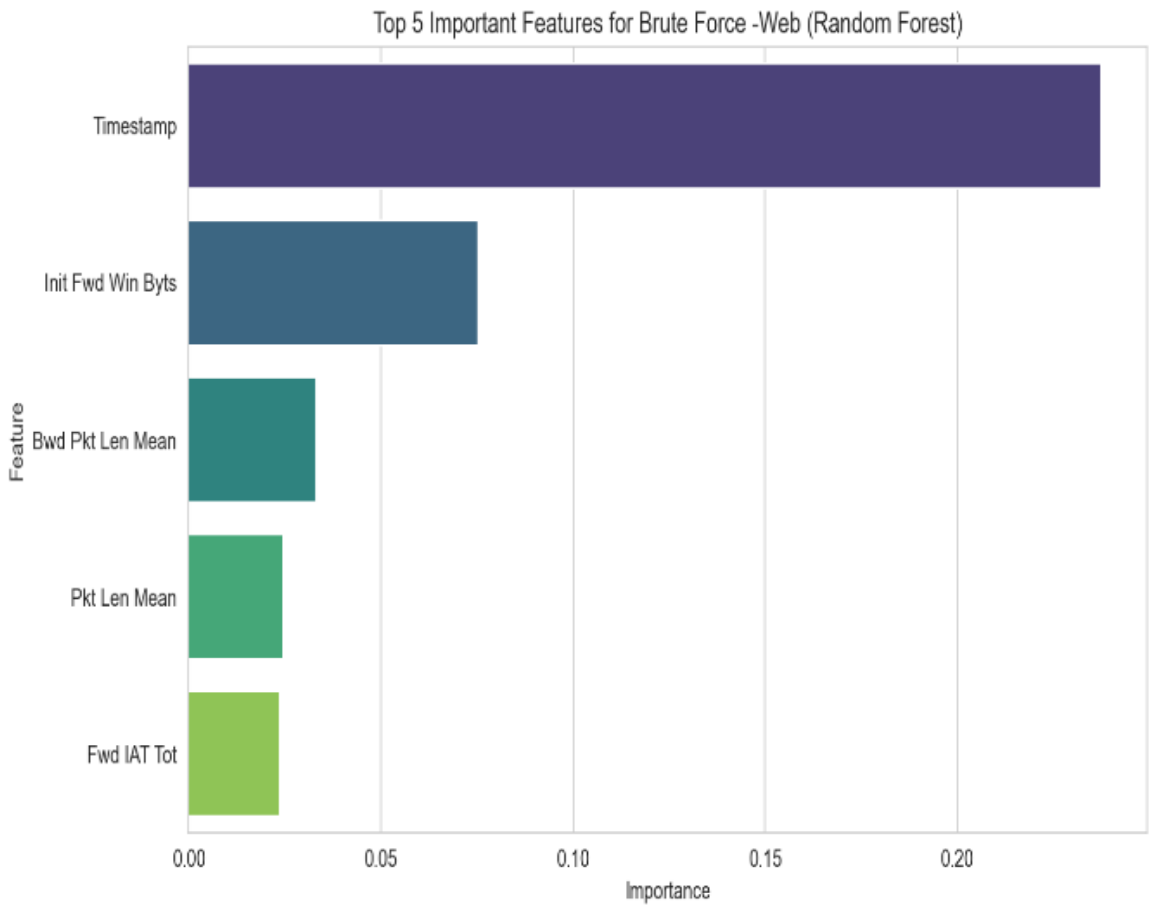

Figure 47: Important Features for Brute-Force – Web (Random Forest)

6.5.2 DDoS (Distributed Denial of Service) Attack - HOIC (High Orbit Ion Cannon)

In all models, "Init Fwd Win Byts" (Initial Forward Window Bytes) always remains the most significant feature. Its high significance as a feature indicates that attackers using HOIC most likely manipulate initial TCP window sizes, and therefore, this feature is a good choice for identifying such attacks. Similarly, the "Timestamp" feature remains highly significant across all models, indicating that packet timing patterns and intervals are key features distinguishing HOIC DDoS traffic from regular traffic.

Secondary features such as "Dst Port" (Destination Port), "Bwd Header Len" (Backward Header Length), "Fwd IAT Mean" (Forward Inter-Arrival Time Mean), and others also remain significant, though to varying degrees across models, reflecting their supporting but lesser role in detection. For optimal detection effectiveness,

network monitoring and defence systems should primarily focus on "Init Fwd Win Byts" and "Timestamp," while also considering secondary features for a comprehensive threat analysis.

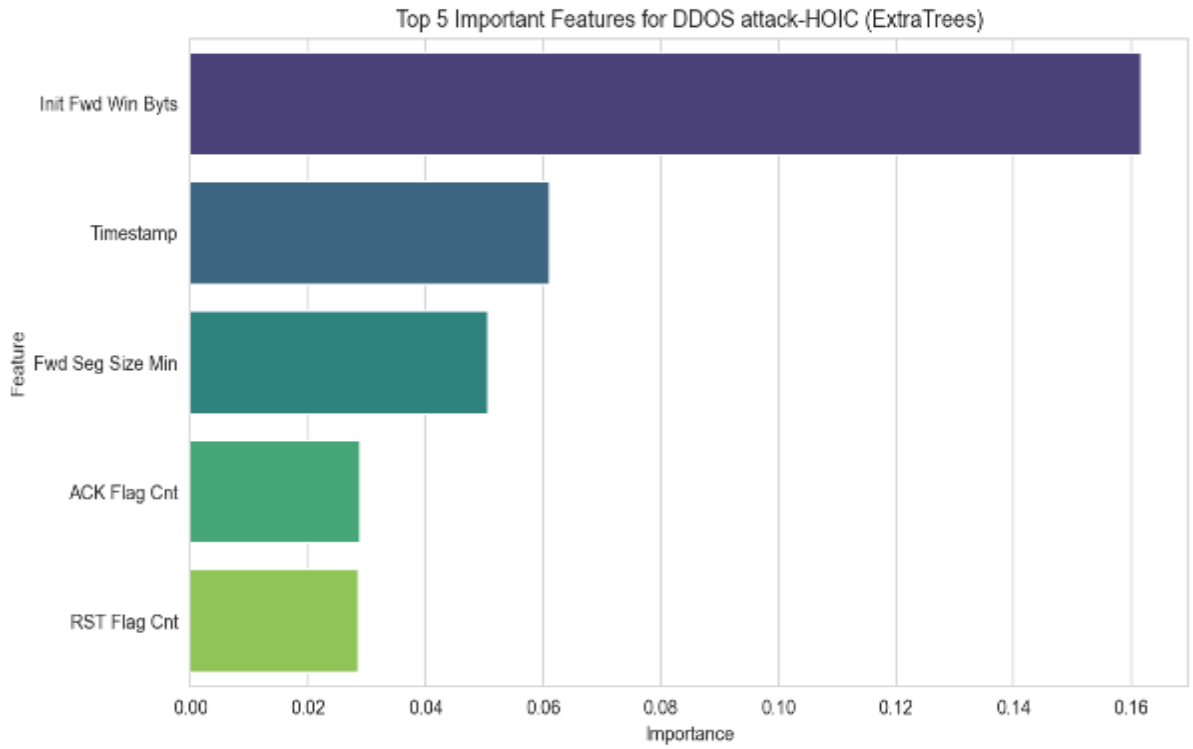

Figure 48: Important Features for DDOS attack – HOIC (Extra Trees)

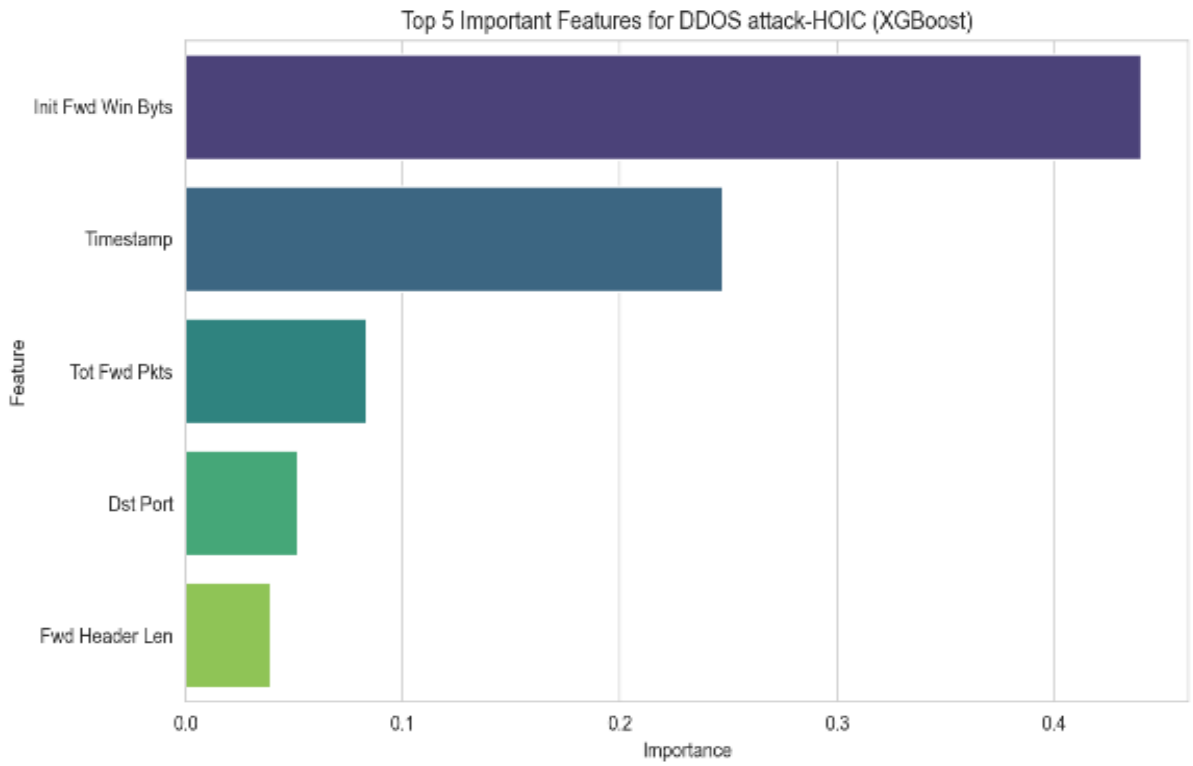

Figure 49: Important Features for DDOS attack – HOIC (XGBoost)

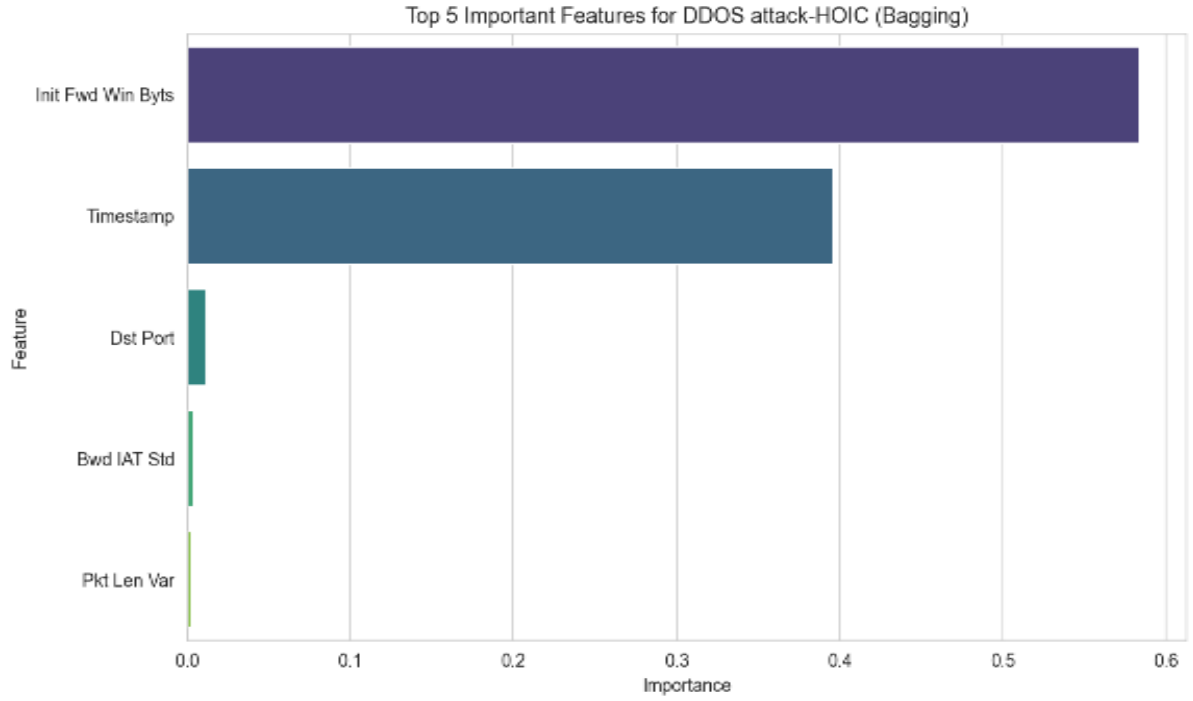

Figure 50: Important Features for DDOS attack – HOIC (Bagging)

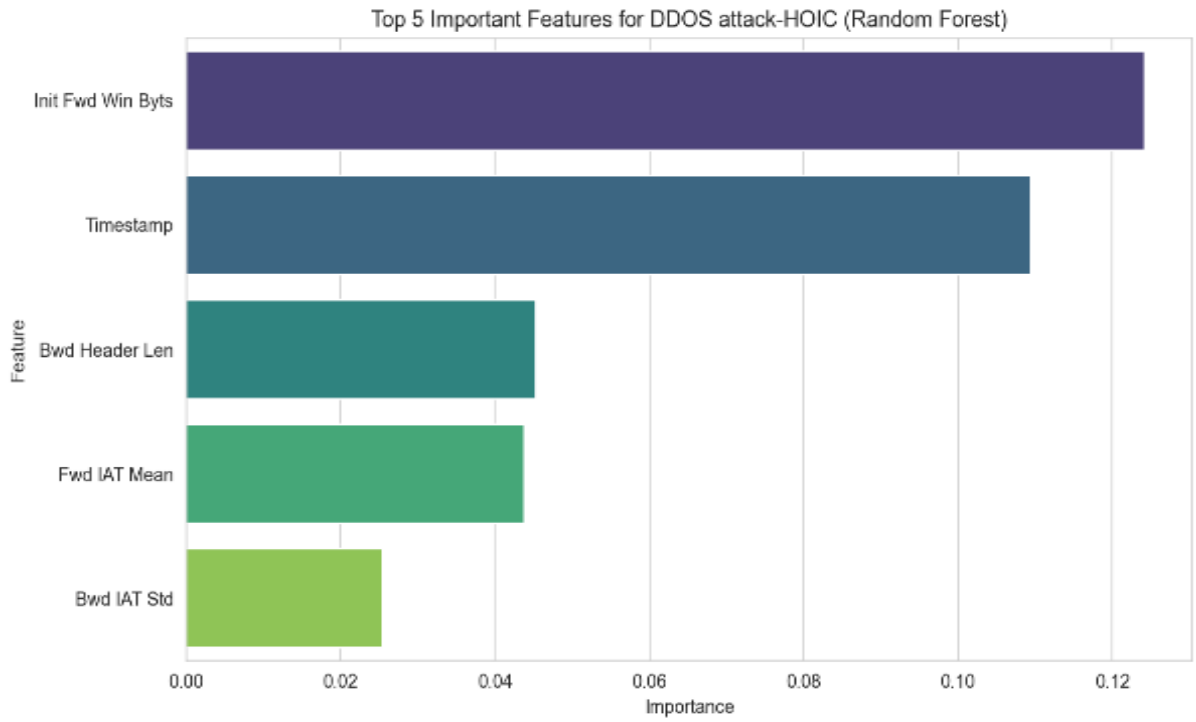

Figure 51: Important Features for DDoS attack – HOIC (Random Forest)

6.5.3 DDoS Attack - LOIC-HTTP

These feature-importance visualisations for LOIC-HTTP DDoS attack detection using Bagging, Random Forest, XGBoost, and ExtraTrees highlight different essential features across the models. "Bwd Header Len" (Backward Header Length) stands out in Bagging and XGBoost models, showing extensive manipulation of reverse packet headers in LOIC-HTTP attacks.

Another common and important feature is "TotLen Bwd Pkts" (Total Length of Backward Packets), which indicates that attackers can send abnormally large or large numbers of backward packets, thereby making malicious activity easier to detect. Furthermore, "Dst IP" (Destination IP address) and "RST Flag Cnt" (Reset Flag Count) are significant in Random Forest and ExtraTrees, indicating probable patterns in the attackers' destination IP addresses and the rate of TCP reset flags, respectively. Features such as "Subflow Bwd Byts," "Src Port," and "TotLen Fwd Pkts" are secondary but still useful complementary indicators. For effective LOIC-HTTP DDoS detection, special monitoring focus should be placed on "Bwd Header Len," "TotLen Bwd Pkts," "Dst IP," and "RST Flag Cnt," as they exhibit the best discriminative ability.

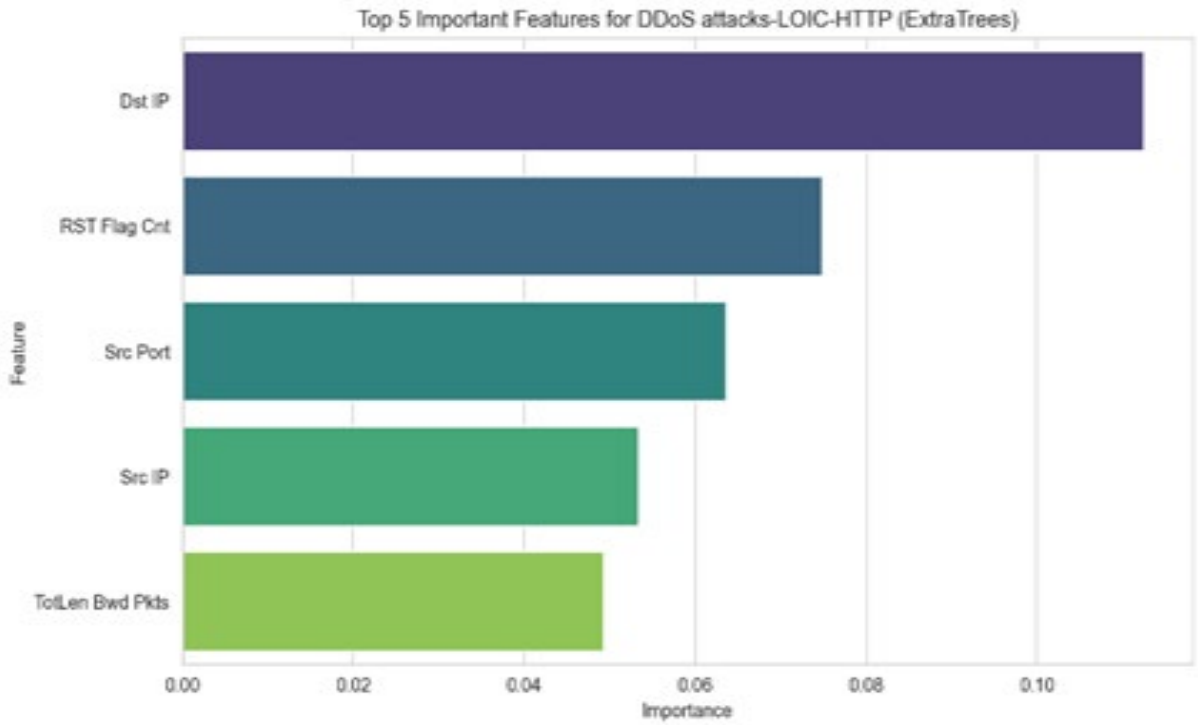

Figure 52: Important Features for DDoS -LOIC-HTTP (Extra Trees)

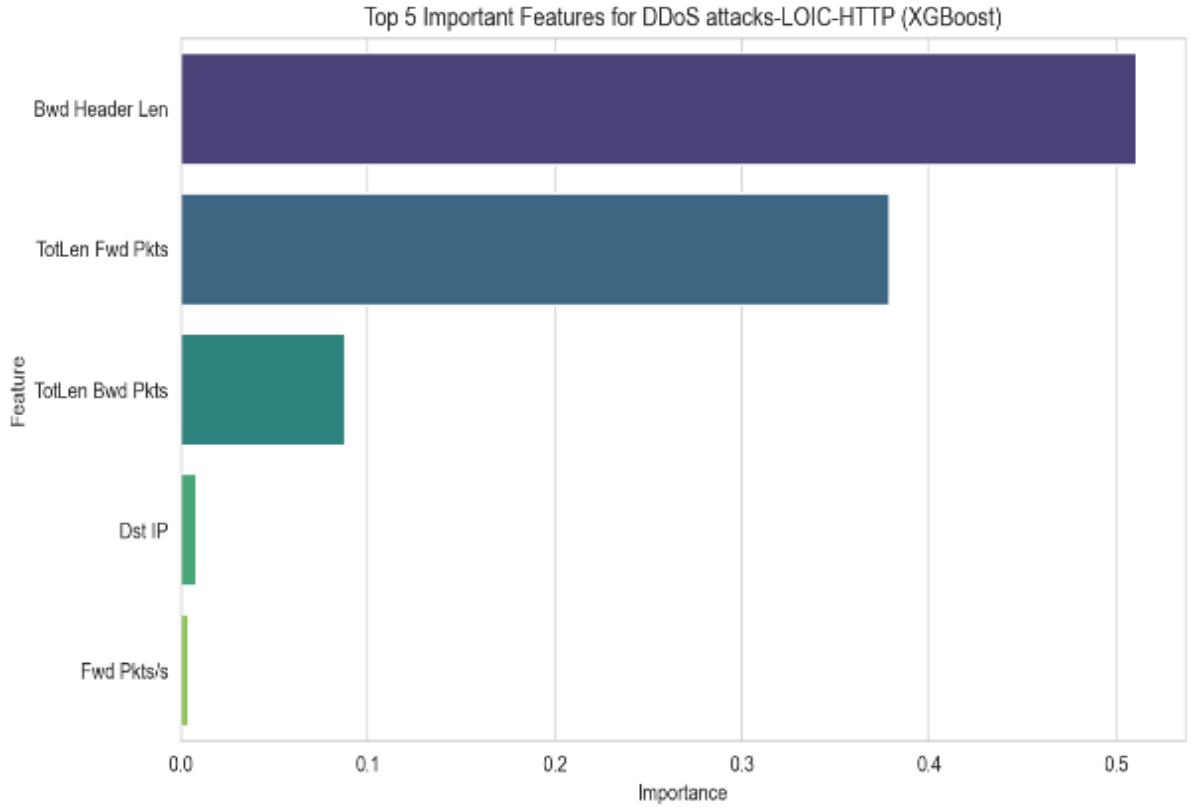

Figure 53: Important Features for DDoS -LOIC-HTTP (XGBoost)

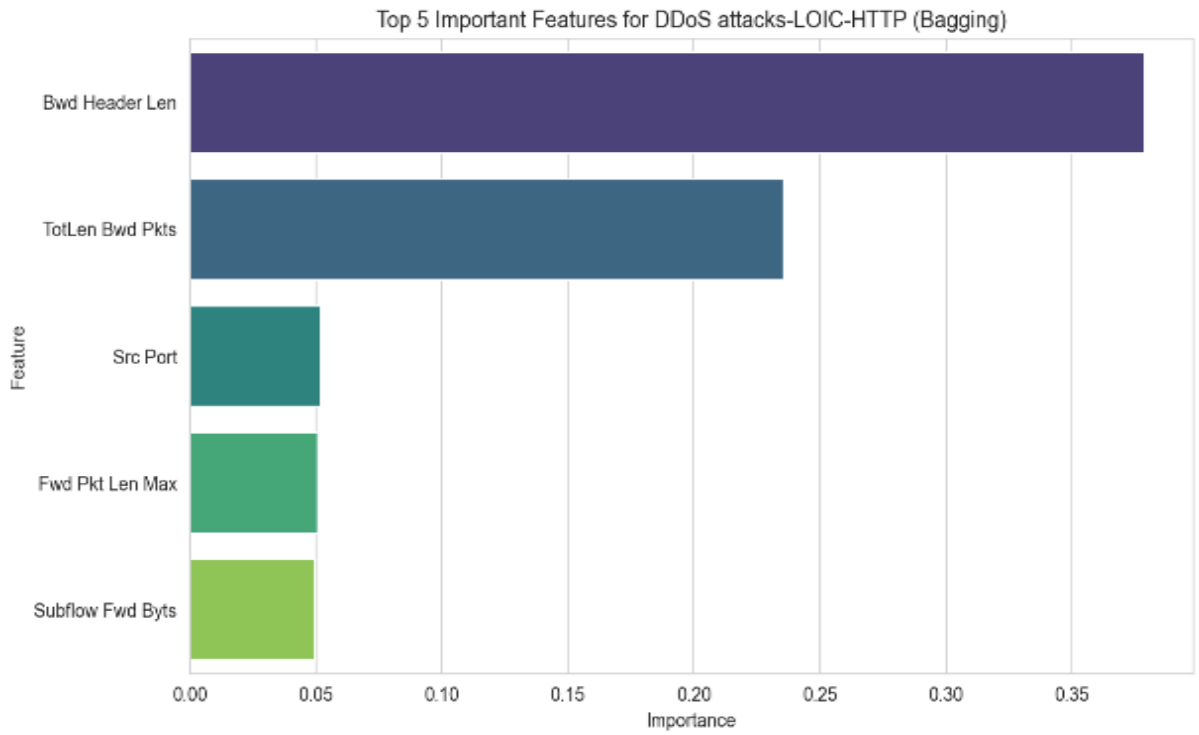

Figure 54: Important Features for DDoS -LOIC-HTTP (Bagging)

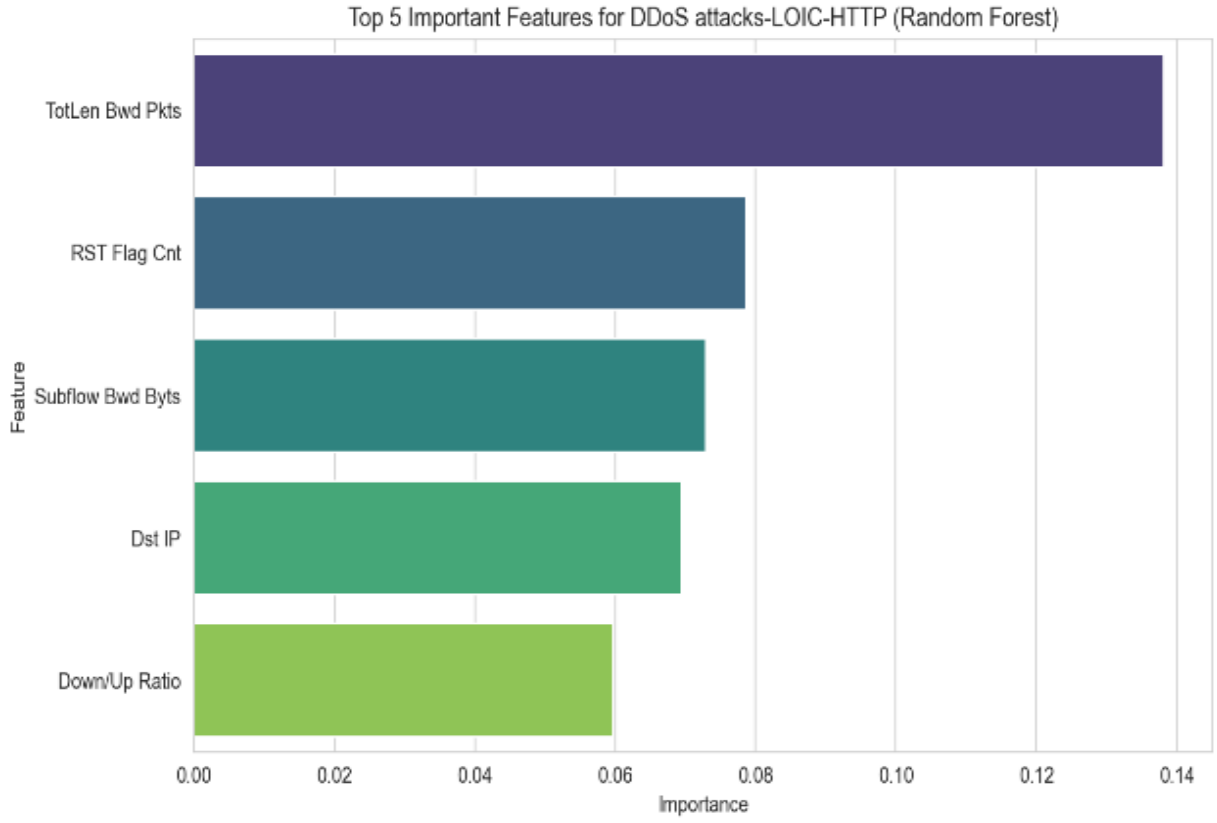

Figure 55: Important Features for DDoS -LOIC-HTTP (Random Forest)

6.5.4 DoS Attack - GoldenEye

The ExtraTrees, XGBoost, Random Forest, and Bagging models indicate that several features are repeatedly identified as most important for classifying GoldenEye DoS attacks. "TotLen Bwd Pkts" (Total Length of Backward Packets) is strongly represented across models, showing that anomalous backward packet lengths or quantities define GoldenEye attacks. Is "Subflow Bwd Byts" strongly represented, indicating that the amount of backward bytes in subflows is key to identifying this style of DoS attack?

Similarly prominent are packet length measures, such as "Bwd Pkt Len Std" (Backward Packet Length Standard Deviation) and "Pkt Len Std" (Packet Length Standard Deviation), which indicate that packet size variability is key to identifying GoldenEye attacks. Features such as "Timestamp" and "Fwd Pkts/s" (Forward Packets per Second) are presented as supplementary indicators, further underscoring the importance of time and packet transmission rates for the precise detection of GoldenEye attack signatures. Effective detection of GoldenEye DoS attacks should thus revolve around tracking backward packet lengths ("TotLen Bwd Pkts," "Subflow Bwd Byts") and packet-size variability ("Pkt Len Std," "Bwd Pkt Len Std").

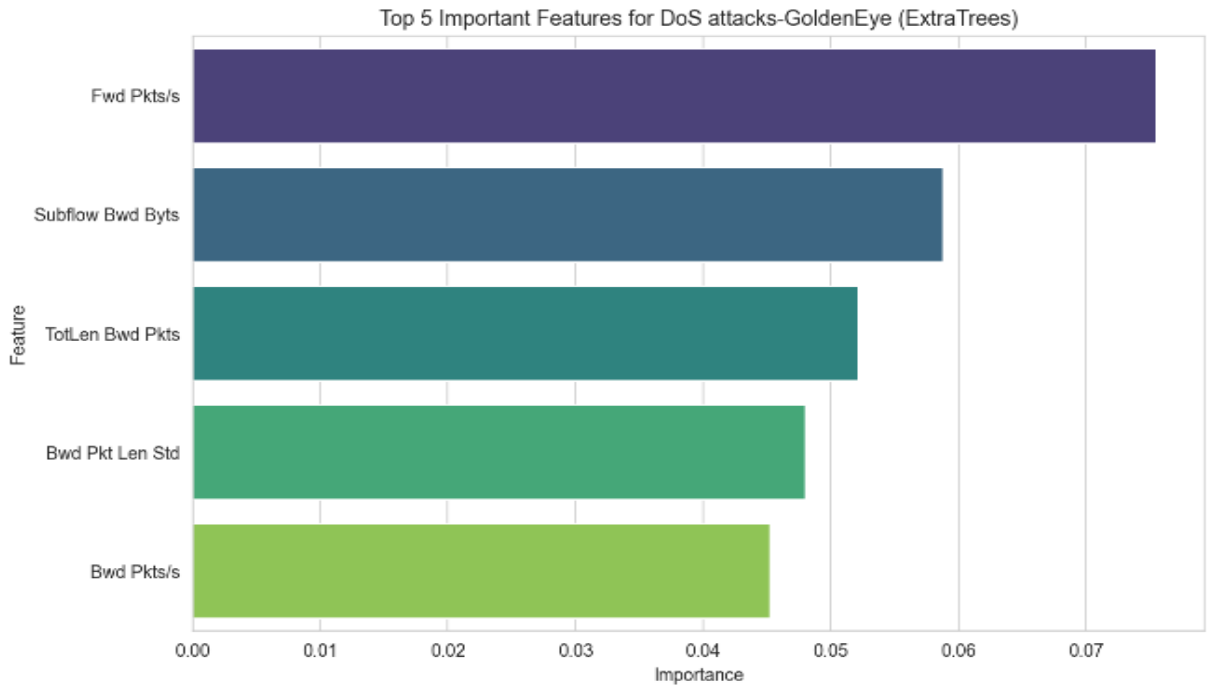

Figure 56: Important Features for DoS Attack-GoldenEye (Extra Trees)

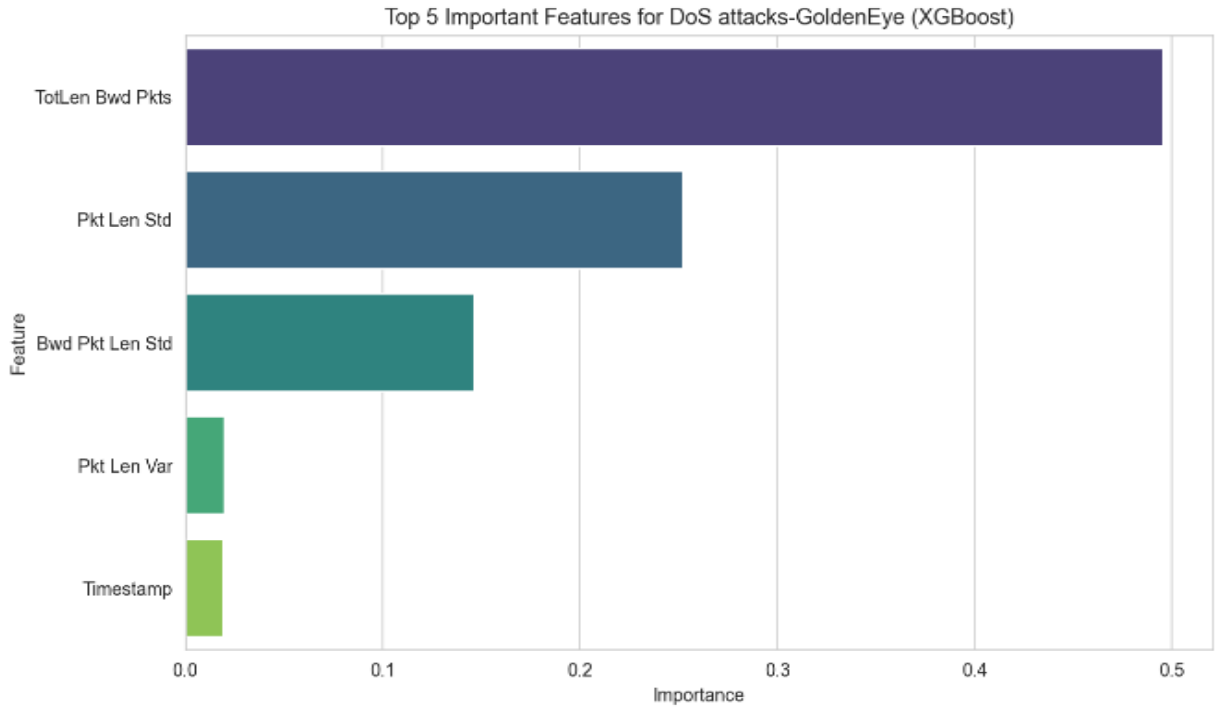

Figure 57: Important Features for DoS Attack-GoldenEye (XGBoost)

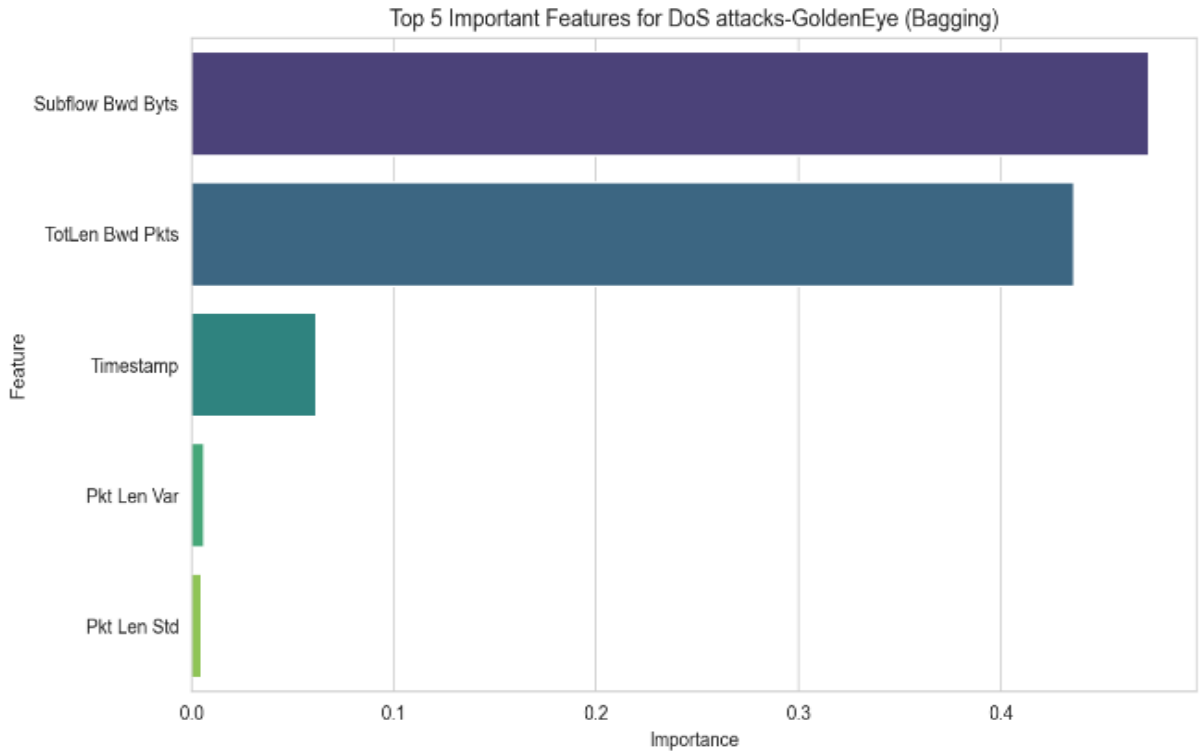

Figure 58: Important Features for DoS Attack-GoldenEye (Bagging)

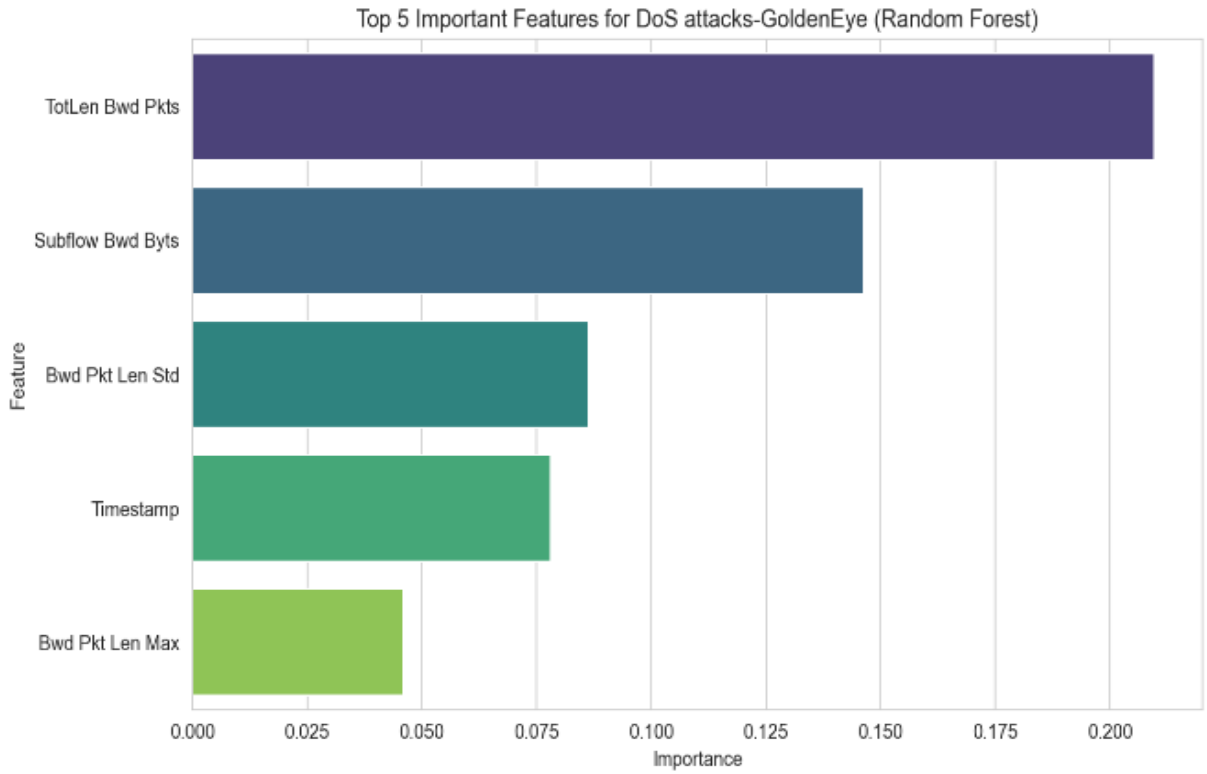

Figure 59: Important Features for DoS Attack-GoldenEye (Random Forest)

6.5.5 SQL Injection

Key features critical to the detection of SQL Injection attacks. The "Timestamp" feature is given high prominence, particularly in Bagging, Random Forest, and ExtraTrees models, because timing patterns in request arrivals strongly distinguish SQL injection activity from everyday database interactions. "Bwd Pkt Len Std" (Backward Packet Length Standard Deviation) also shows high prominence, particularly in XGBoost and Bagging models, as SQL injection attempts are often characterised by abnormality in backward packet lengths. "Dst Port" (Destination Port) also appears prominently, indicating that attackers frequently target specific database query ports.

Additionally, features such as "Flow Pkts/s" (Flow Packets per Second) and "Init Fwd Win Byts" (Initial Forward Window Bytes) are valuable secondary indicators, as they help monitor packet-rate variations and initial TCP handshake behaviour during such attacks. Overall, effective monitoring techniques for SQL Injection detection should primarily concentrate on inspecting request timing ("Timestamp"), packet size variation ("Bwd Pkt Len Std"), and target ports ("Dst Port"), complemented by supporting evidence from packet flow rates and TCP window behaviours.

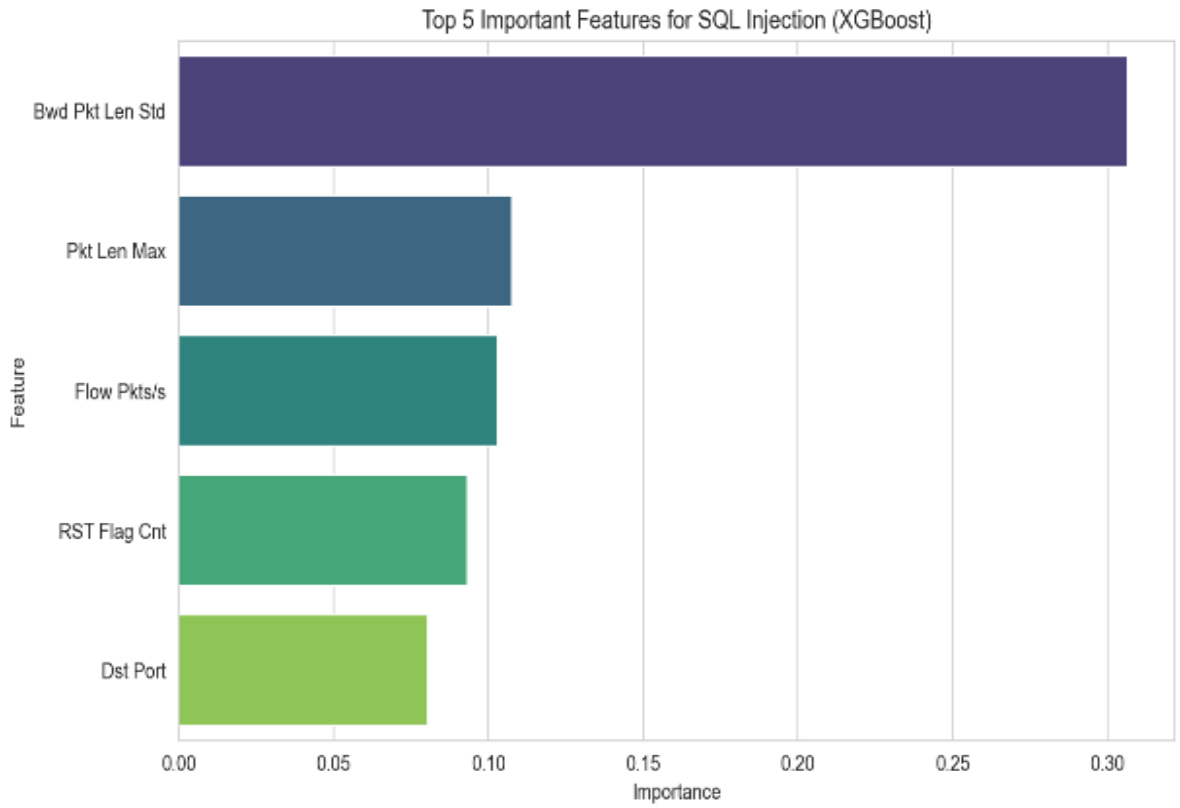

Figure 60: Important Features for SQL Injection (XGBoost)

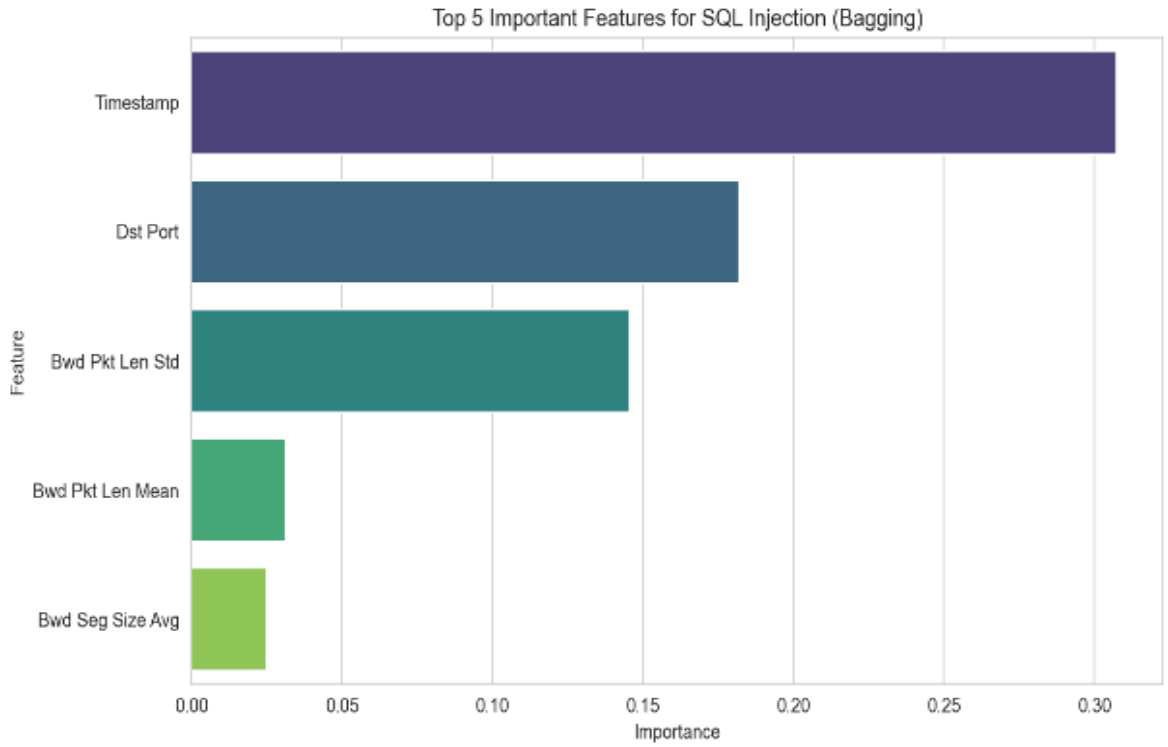

Figure 61: Important Features for SQL Injection (Bagging)

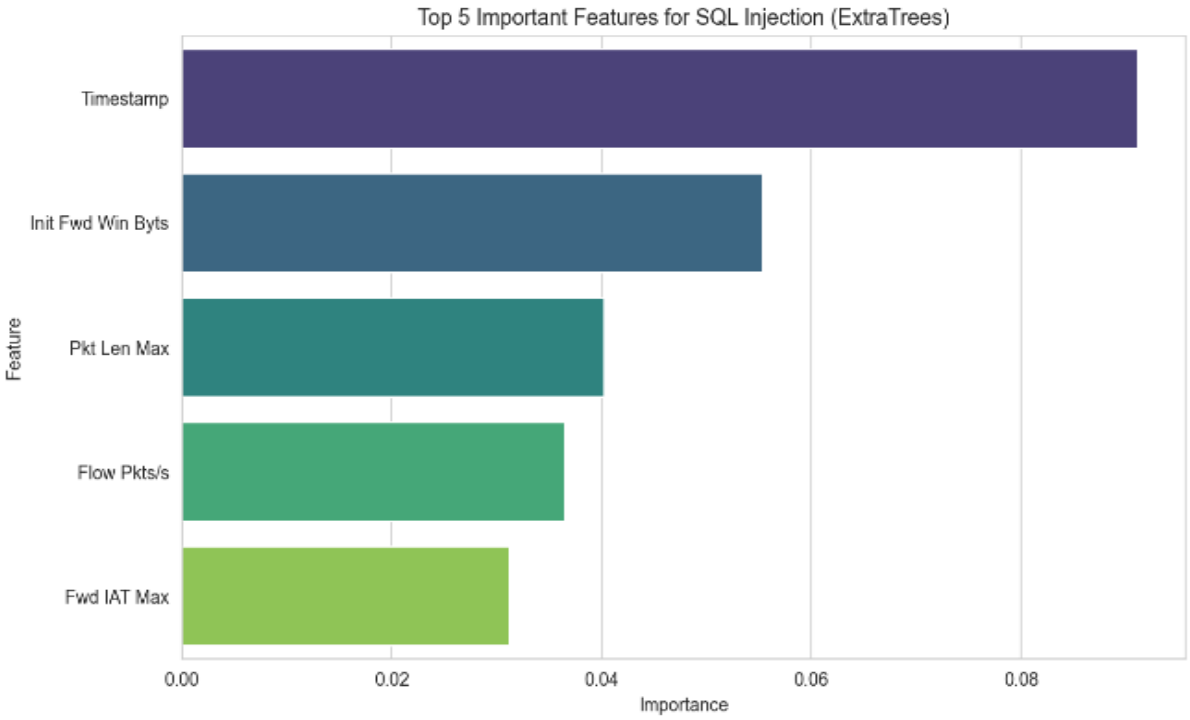

Figure 63: Important Features for SQL Injection (ExtraTrees)

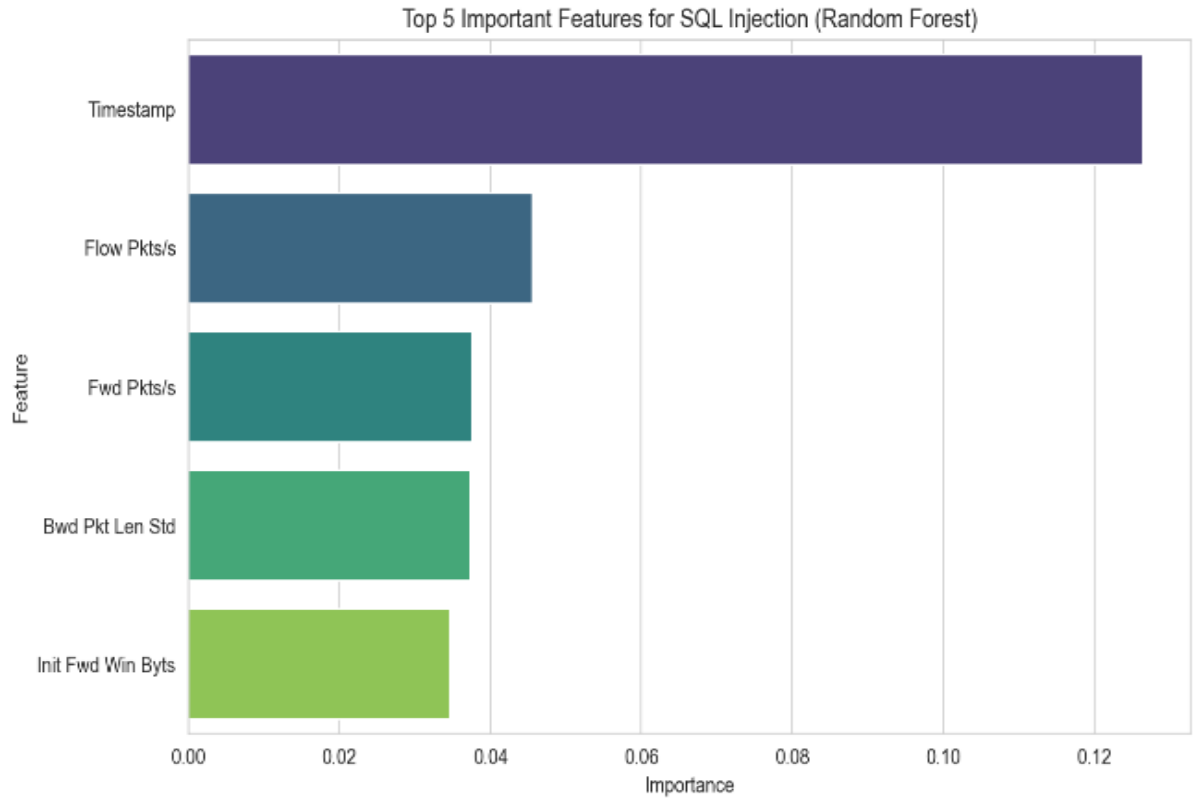

Figure 62: Important Features for SQL Injection (Random Forest)

6.5.6 DoS Attack - Hulk

Visualisations from ExtraTrees, XGBoost, Bagging, and Random Forest algorithms reveal significant features that effectively discriminate Hulk DoS attacks. "Idle Mean" (mean idle time between packets) is a strong discriminator that appears prominently in XGBoost, Bagging, and Random Forest models, suggesting that idle-time irregularities between packet streams generally distinguish Hulk attacks. The "Dst Port" (Destination Port) is also highly important, particularly in XGBoost and Bagging models, suggesting that Hulk attacks prefer to concentrate traffic on particular target ports. Features like "Active Std" (standard deviation of active periods), "Idle Std" (idle time standard deviation), and "Fwd Header Len" (Forward Header Length) also reflect high importance, especially in the ExtraTrees and Random Forest models, which reflect the variability of activity periods and abnormal forward packet headers as predictive indicators. "Timestamp" also contributes to these features, underscoring the significance of temporal patterns in traffic analysis. To further improve the detection accuracy of Hulk DoS attacks, monitoring should be prioritised to analyse idle periods ("Idle Mean," "Idle Std"), target destination ports ("Dst Port"), and packet header anomalies ("Fwd Header Len").

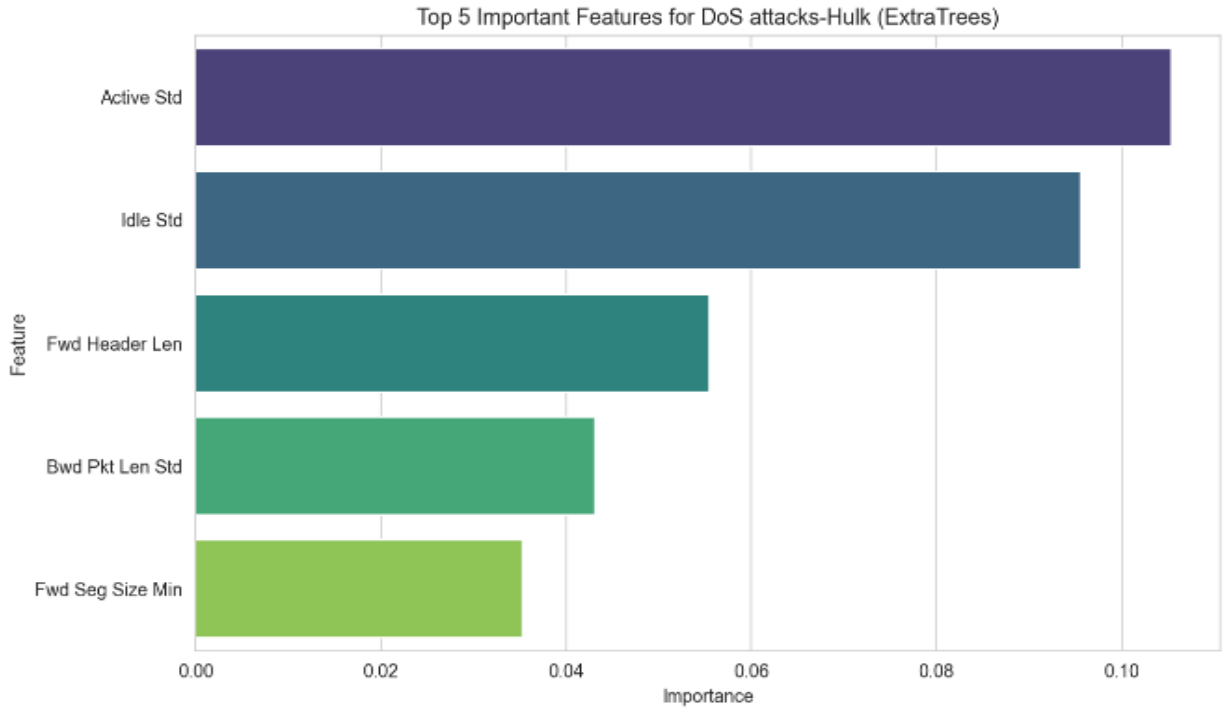

Figure 64: Important Features for DoS-Hulk (ExtraTree)

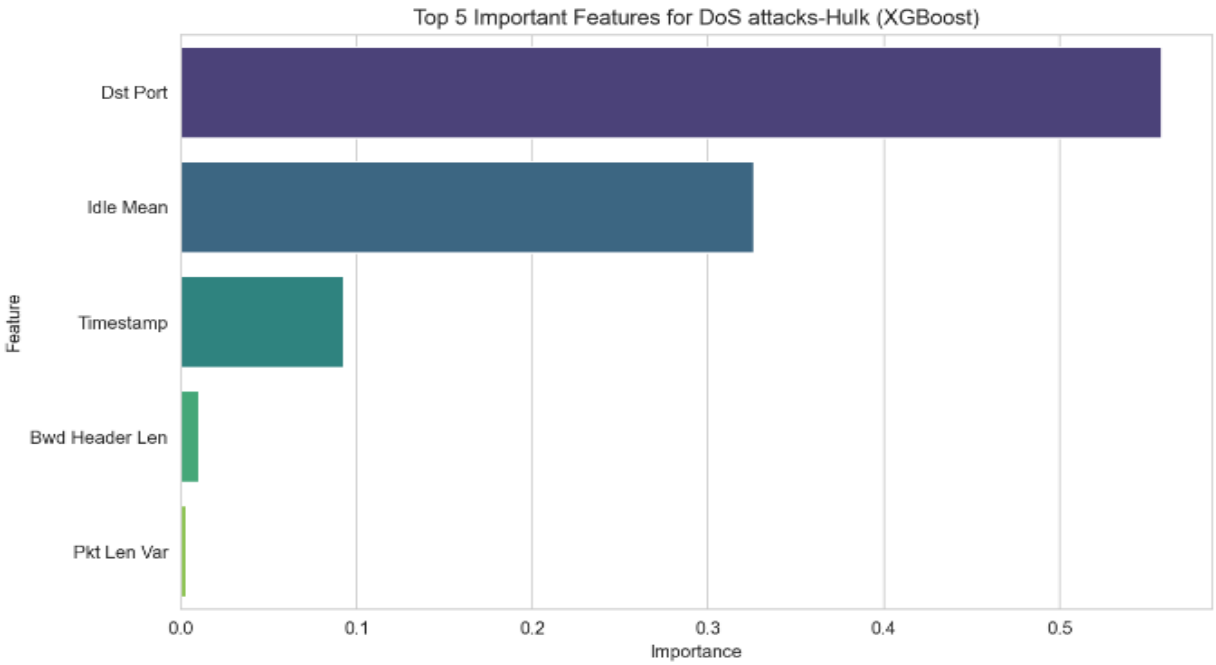

Figure 65: Important Features for DoS-Hulk (XGBoost)

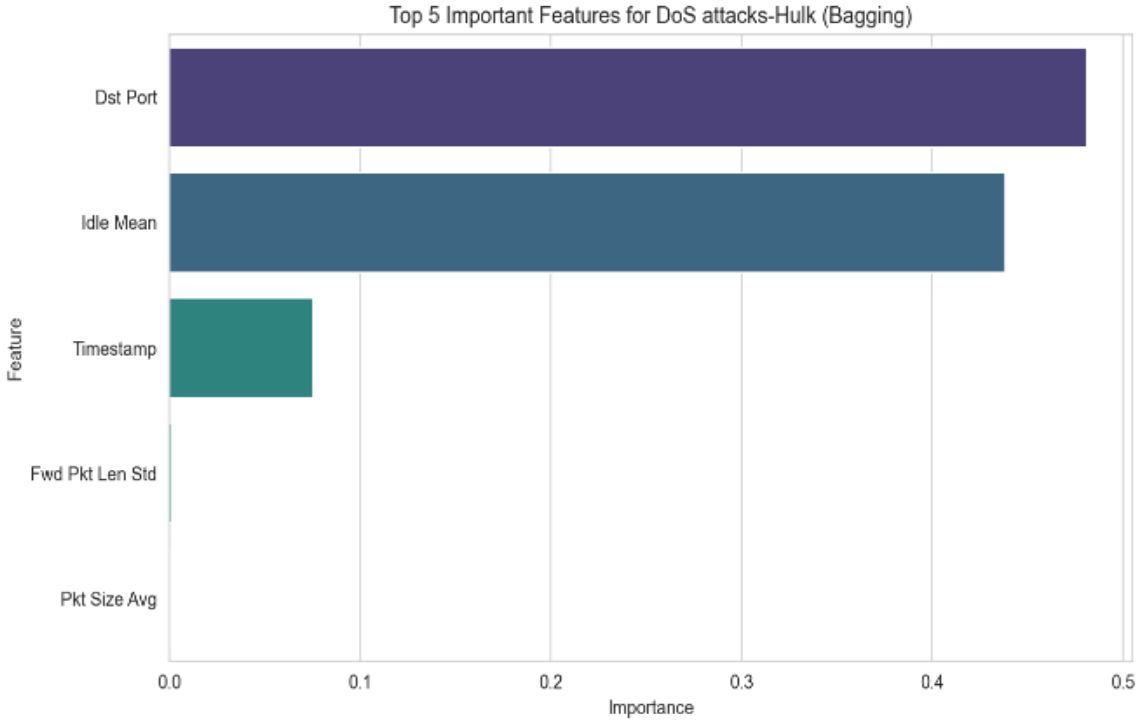

Figure 66: Important Features for DoS-Hulk (Bagging)

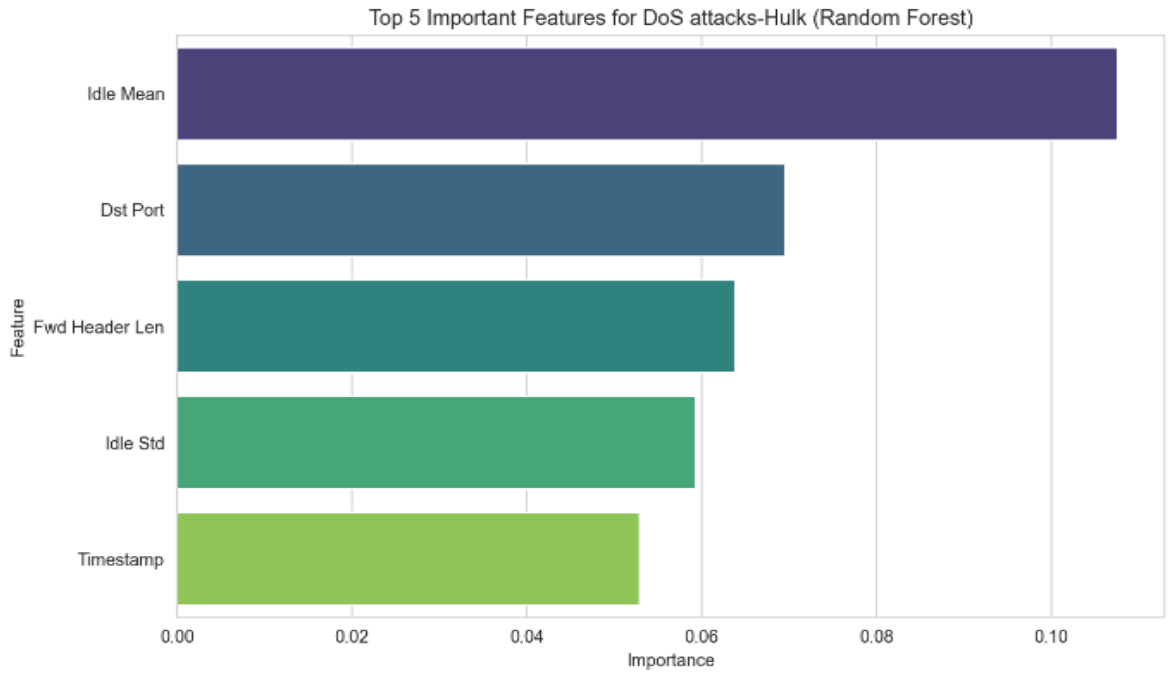

Figure 67: Important Features for DoS-Hulk (Random Forest)

6.5.7 File Transfer Protocol - Brute force

The visualisations are provided by the Random Forest, Bagging, XGBoost, and ExtraTrees models, all of which indicate the significance of specific features in detecting FTP-BruteForce attacks. The "Timestamp" feature is prominent across the Random Forest, XGBoost, and ExtraTrees models, indicating that timing patterns and packet arrival intervals play a key role in distinguishing brute-force attacks against FTP servers. Furthermore, "Dst Port" (Destination Port) is prominent across all models, as it denotes purpose-specific attacks targeting FTP ports. "Fwd Seg Size Min" (Minimum Forward Segment Size) and "Fwd Pkts/s" (Forward Packets per Second) also emerge as prominent factors in this context, highlighting that attackers' efforts are characterised by smaller packet sizes and higher packet transmission rates.

The other secondary indicative relevant metrics are "Flow IAT Max" (Maximum Flow Inter-Arrival Time), "Init Fwd Win Byts" (Initial Forward Window Bytes), and "Fwd Header Len" (Forward Header Length), which all indicate anomalous packet transmission behaviour of the session and characteristics of TCP handshakes. To efficiently identify FTP-BruteForce attacks, monitoring must prioritise detecting timing patterns ("Timestamp"), port-specific traffic ("Dst Port"), packet transmission rates ("Fwd Pkts/s"), and fluctuations in forward segment sizes ("Fwd Seg Size Min").

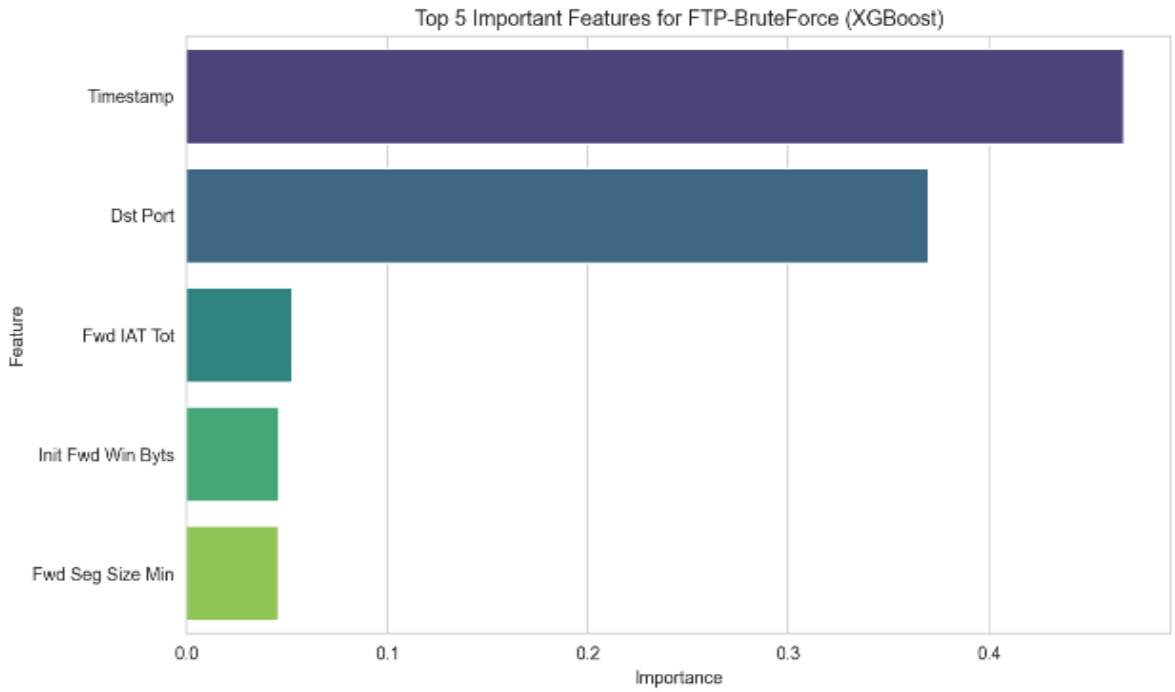

Figure 68: Important Features for FTP-Brute Force (XGBoost)

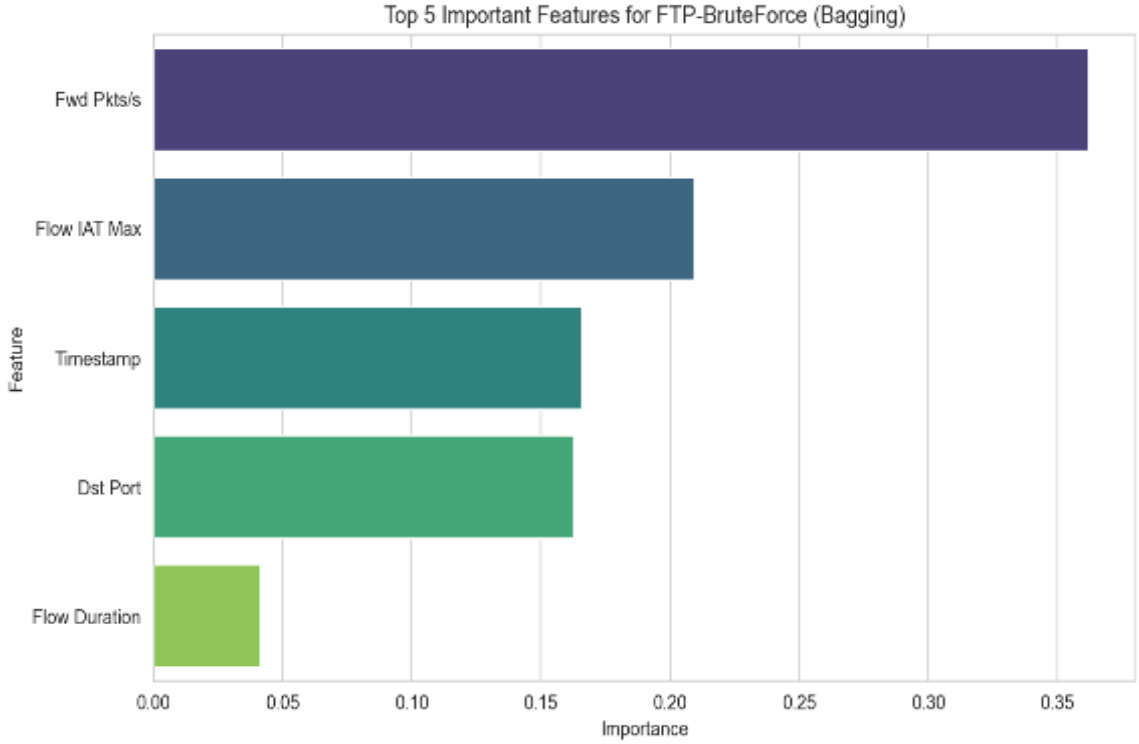

Figure 69: Important Features for FTP-Brute Force (Bagging)

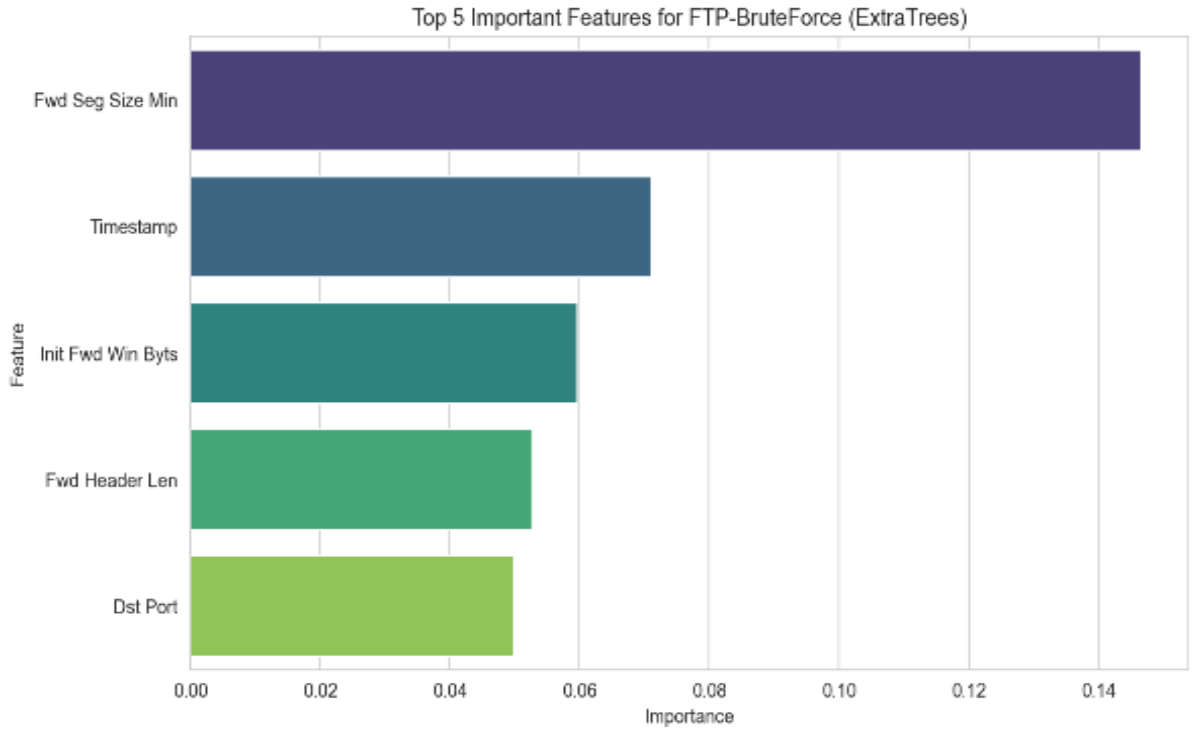

Figure 70: Important Features for FTP-Brute Force (ExtraTrees)

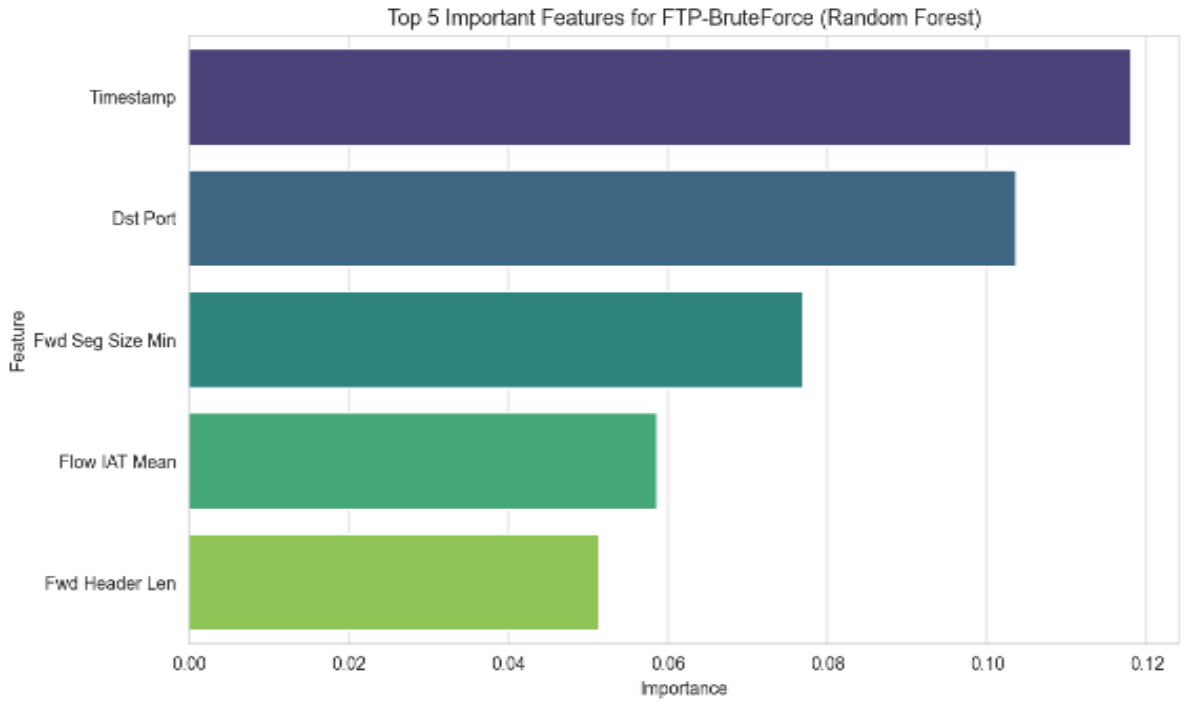

Figure 71: Important Features for FTP-Brute Force (Random Forest)

6.6 Ontology Diagram

Ontology diagrams are used to represent concepts, relationships, and hierarchical structures within a specific domain. In cybersecurity and digital forensics, ontologies

provide a formal mechanism for organising knowledge, defining relationships between entities, and enabling consistent interpretation of information across systems and stakeholders. By establishing a shared conceptual model, ontologies improve communication, reduce ambiguity, and support more effective decision-making during forensic investigations (Liepiņš et al., 2016). Ontology diagrams provide a basis for focusing on terms and their meanings, aiding in the specification of corresponding entities within a shared vocabulary (Sato et al., 2023).

Within the proposed Digital Forensic Readiness Model, the ontology serves a broader purpose than simply visualising domain concepts. It provides a structured knowledge representation model that links network traffic data, attack categories, machine learning models, classification outcomes, and forensic features into a unified model. This enables the representation of relationships among evidence sources, attack behaviours, and detection mechanisms in a consistent and machine-interpretable manner.

The ontology begins with network traffic data, which is categorised into benign and malicious traffic classes. Malicious traffic is subsequently associated with different attack categories, including brute-force attacks, denial-of-service (DoS), distributed denial-of-service (DDoS), web attacks, and injection attacks. These attack types are linked to machine learning classification models, including Random Forest, Extra Trees, XGBoost, and LightGBM, which are used to identify and classify malicious activities. The resulting classifications are then linked to key forensic features that contribute most to attack detection and forensic analysis.

A significant contribution of the ontology is its support for automation within the Digital Forensic Readiness process. By formally defining relationships between attack indicators, evidence sources, and classification outputs, the ontology enables automated reasoning and knowledge sharing across security monitoring and forensic systems. Security events detected by monitoring platforms can be automatically mapped to known attack categories and their associated forensic artefacts, reducing the need for manual interpretation and accelerating investigations.

The ontology also strengthens evidence correlation capabilities. One of the major challenges in IoT-enabled environments is the fragmentation of evidence across multiple devices, platforms, and network locations. The ontology provides a mechanism to link related events, features, and attack classifications, enabling investigators to establish relationships among seemingly independent artefacts. This improves incident reconstruction by enabling forensic analysts to correlate network traffic characteristics, machine learning predictions, and attack behaviours within a unified knowledge structure.

Furthermore, the ontology enhances knowledge representation by capturing both explicit and implicit relationships within the forensic domain. Explicit relationships describe direct associations, such as a machine learning model classifying a particular attack type. Implicit relationships can be inferred through reasoning mechanisms, enabling investigators to identify previously unknown connections between events, devices, and attack patterns. This capability is particularly valuable in complex IoT ecosystems where evidence is distributed and continuously evolving.

From a Digital Forensic Readiness perspective, the ontology contributes to proactive investigative preparedness by standardising the representation, sharing, and analysis of forensic knowledge. It provides a common vocabulary for describing attacks, evidence sources, machine-learning outputs, and forensic features, thereby reducing inconsistencies among investigators, security analysts, and organisational stakeholders. The ontology also supports future integration with automated reasoning engines, Security Information and Event Management (SIEM) platforms, and forensic decision-support systems.

Overall, the ontology extends the capabilities of the proposed Digital Forensic Readiness Model beyond traditional monitoring and evidence collection. By enabling structured knowledge representation, automated evidence interpretation, and enhanced evidence correlation, it improves the organisation's ability to detect, understand, and investigate cybersecurity incidents within complex IoT-enabled environments.

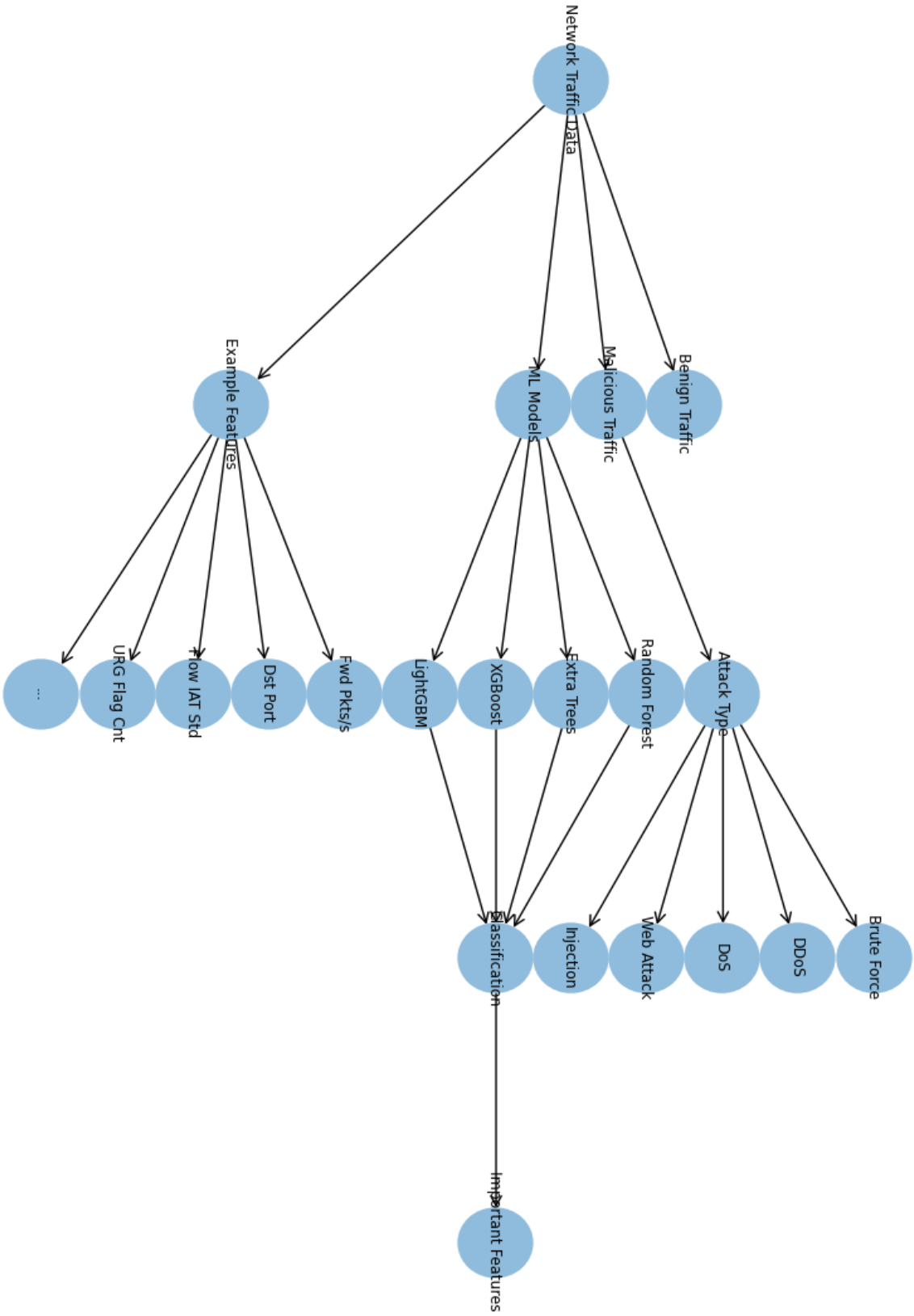

Figure 72: Ontology Diagram

6.7 Chapter Summary

This chapter analysed network traffic data to identify and characterise cyber threats within IoT-enabled environments, with a particular focus on feature selection and the use of tree-based machine learning models to distinguish attack-related patterns. Four ensemble models—XGBoost (XGB), BaggingClassifier, Extra Trees, and Random Forest—were trained and evaluated to identify significant network characteristics associated with multiple attack types, including Distributed Denial of Service (DDoS) and SQL injection. The analysis demonstrates that feature importance can improve threat-identification accuracy while reducing response time, thereby enabling more efficient security monitoring in IoT-based networks.

Despite the demonstrated effectiveness of the machine learning models in analysing attack-related data, several limitations must be acknowledged, particularly within forensic and legal contexts. Machine learning outputs are inherently dependent on the quality, completeness, and representativeness of training data and may be affected by dataset bias, concept drift, or adversarial manipulation. Moreover, classification results alone do not constitute legally admissible evidence and must be interpreted as decision-support outputs rather than definitive forensic conclusions. Legal requirements related to transparency, reproducibility, and expert validation further constrain the direct use of automated models in judicial proceedings. Consequently, machine learning in this study is positioned as an assistive mechanism that complements, rather than replaces, established digital forensic processes.

Significantly, the results of this chapter extend beyond attack detection and contribute directly to the broader objective of Digital Forensic Readiness. Feature importance analysis provides forensic insight into which network and system attributes are most relevant for reconstructing events and preserving evidential context during investigations. By supporting the identification and prioritisation of high-value forensic artefacts, the machine-learning analysis enhances readiness by informing evidence-collection strategies, reducing investigative effort, and enabling timely forensic decision-making. In this way, the data analysis component strengthens the integration between automated analytics and the standards-aligned forensic readiness

processes proposed in this research, reinforcing the role of machine learning as an enabler of proactive forensic preparedness in IoT-enabled organisational environments.

7.0 Discussion of Findings

7.1 Introduction

This chapter discusses the study's findings by critically interpreting the experimental results presented in Chapters 4, 5, and 6, and by evaluating and situating them within the broader context of the research objectives, the proposed Digital Forensic Readiness (DFR) model, and existing literature. Rather than restating empirical outcomes, the discussion examines how the findings collectively demonstrate that effective forensic readiness in IoT-enabled organisational environments requires a proactive, integrated approach that extends beyond traditional post-incident investigation. The results indicate that aligning organisational governance, technical infrastructure, and real-time security monitoring within a standard-compliant framework enhances the timely generation, preservation, and traceability of digital evidence.

Furthermore, the findings indicate that the layered DFR model improves investigative efficiency, reduces reliance on manual forensic intervention, and strengthens chain-of-custody integrity in dynamic IoT environments. Compared with prior research, which often treats security, forensics, and organisational readiness as separate concerns, this study provides empirical support for a unified, ISO/IEC 27043–aligned approach to forensic readiness. Overall, the discussion highlights how the proposed model advances both the theoretical understanding and the practical implementation of DFR by demonstrating its feasibility, effectiveness, and relevance in real-world IoT-enabled organisational contexts.

7.2 Digital Forensic Readiness (DFR) Model for IoT-Enabled Organisations

The rapid growth of IoT devices has revolutionised the digital world, enabling interconnected systems and opening new paths for industries. Nonetheless, this has enabled rapid connectivity, which has brought serious cybersecurity risks, as smart devices are vulnerable to cyber threats due to weak security measures. They explain why sound digital forensics models must be implemented to enable investigators to assess and tackle these threats. A significant difference from traditional computer systems, which are more uniform, is that IoT systems are heterogeneous, have limited storage and computational capacity, and generate large amounts of data from many

diverse sources. This work addresses these challenges by presenting a research model of readiness and resilience in IoT-enabled organisations, with a focus on applying it to cyber threats. By applying real-time data analysis and modern forensic methodologies, the research aims to provide organisations with solutions to transform and enhance their overall cybersecurity posture, thereby achieving business continuity amid constantly evolving threats.

Digital technology has advanced rapidly, alongside the widespread adoption of IoT devices in organisations, bringing significant benefits. This relates to enhancing operational efficiencies, innovating business models, and facilitating better data-driven decision-making. However, building these huge IoT ecosystems has not come without significant challenges, especially in cybersecurity. Most of the IoT devices are minimally secured, ultimately broadening the attack surface and exposing an organisation to breaches, data theft, and other cybercrimes. Added to this is the nature of diverse, often interconnected IoT devices, which complicate the task of securing a digital environment.

In the current landscape, Digital Forensic Readiness (DFR) has emerged as a vital strategy for organisations seeking to proactively prepare for and respond to cyber incidents. For example, DFR can be described as the identification, preservation, and analysis of digital evidence within a systematic framework to provide a fast and effective response to security breaches, minimise damage during the event, and ensure compliance with legal and regulatory requirements. This chapter presents an end-to-end IoT-based DFR model for an environment. The model thus addresses concerns IoT ecosystems face, including the heterogeneity of devices, the high volume and velocity of data, and the need for real-time evidence collection. Secondly, the model focuses on commitment to ISOs, thereby forming a more transparent, globally accepted approach to forensic preparedness. The chapter adopts an overarching architecture to develop an IoT forensic-readiness model and to incorporate innovative forensic methods for future investigations.

7.2.1 ISO/IEC 27043: A Framework for Forensic Readiness

ISO/IEC 27043 is one of them, which addresses forensic readiness by requiring the organisation to implement a structured digital forensics plan. To this end, it ensures that an organisation can collect, preserve, and analyse evidence in accordance with its legal and operational frameworks. It also focuses on the 'chain of custody' principle, which is the approach that guides the handling of the evidence in an unaltered state, whether physically or electronically, throughout the entire cycle. This strengthens its credibility and admissibility in litigation; it is a cornerstone of successful investigations. Another central principle is traceability and verifiability: that each operation on digital evidence must be easily explained, reported, and verified by others. This fosters confidence in the forensic process and provides investigators with a viable technique to corroborate their evidence. The standard also contains a jurisdictional consistency provision to provide some reassurance over the challenges that come when undertaking investigations across jurisdictions.

The scope of ISO/IEC 27043 is to establish a forensic standard and unify forensic practices worldwide, thereby improving cooperation among organisations, police departments, and regulatory authorities. Consequently, all data are treated equally and processed using the same procedure, regardless of their location. The adoption of ISO/IEC 27043 will significantly benefit organisations by enhancing their operational feasibility and resilience, among other advantages. In this regard, this standard compliance relates to legal and regulatory conformity, specifically ensuring adherence to global frameworks for managing evidence. It also reduces the likelihood that evidence will be excluded in a legal process, thereby enhancing its legal protection and the organisation's standing. Apart from this, the standard also ensures reduced costs and time in conducting investigations by adopting measures such as forensic readiness investigations.

Adopting a credible pre- and post-incident business continuity management plan and process reduces the time and resources required to gather, analyse, and document evidence. This, in the long run, shortens the time needed to resolve such incidents and reduces operational costs. Also, there is ongoing improvement as organisations align their forensic strategies with ISO/IEC 27043. It urges them to revisit earlier incidents

and to improve forensic analysis logically, anticipating new threats that are continually evolving within an organisation.

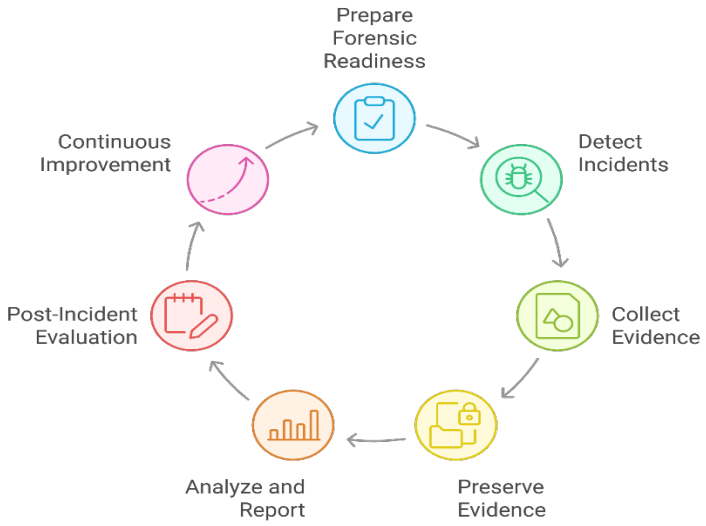

Figure 73: Forensic Readiness and Incident Management Cycle

7.2.2 Practical Application of ISO/IEC 27043 in DFR

One significant contribution of ISO/IEC 27043 to an organisation's incident response and cybersecurity frameworks is its improvement of digital forensic readiness. Organisations set up automated tools to monitor and log in accordance with the standard's guidelines. Proper maintenance and security of these logs during any investigation could make them relevant evidence. It is also helpful to have a standard that clarifies roles and responsibilities in forensic teams, reducing confusion or delays during incident response. Hence, regular training and auditing are recommended to ensure the staff are conversant with all requirements and best practices outlined in the standard.

For multinationals, ISO/IEC 27043 provides a common framework and means for handling evidence across different countries. This is particularly important in incidents involving IoT devices, as data from such incidents may be scattered across multiple jurisdictions. Under the principles of the standard, organisations may become better empowered to respond to cyber incidents while maintaining robust, defensible, and globally benchmarked forensic processes.

The findings of this research demonstrate that effective Digital Forensic Readiness within IoT-enabled organisational environments requires support for the complete

ISO/IEC 27043 forensic investigation lifecycle rather than focusing solely on intrusion detection or post-incident forensic analysis. While traditional cybersecurity monitoring primarily emphasises attack detection and operational response, ISO/IEC 27043 extends this perspective by incorporating proactive readiness, evidence acquisition, preservation, examination, analysis, reporting, and continuous assessment processes into a unified investigative model.

The proposed Digital Forensic Readiness Model operationalised these lifecycle processes by integrating real-time monitoring infrastructure, forensic evidence preservation mechanisms, machine-learning-based analytical models, and structured chain-of-custody management procedures. This comprehensive lifecycle approach enabled the model to support continuous forensic preparedness and improve evidence reliability, investigative efficiency, and organisational cyber resilience.

Furthermore, the inclusion of concurrent and assessment process groups strengthened the model's operational robustness by ensuring continuous monitoring of evidence integrity, documentation consistency, forensic accountability, and ongoing evaluation of readiness effectiveness throughout the investigation lifecycle.

7.3 Evaluation of the DFR Model: Automated Proactive Readiness Model (APRM)

The evaluation results presented in this chapter directly address the research objectives defined in Chapter 1. The organisational and conceptual assessment confirms the validity of the proposed DFR model design (Objective 2), the practical implementation and experimental scenarios demonstrate feasibility and operational effectiveness (Objective 3), and the quantitative performance metrics and forensic analysis validate the model's ability to enhance forensic readiness in IoT-enabled organisations (Objective 4). By mapping evaluation outcomes explicitly to the research objectives, this chapter provides strong empirical support for the research claims and reinforces the contribution of the proposed model.

The Automated Proactive Readiness Model (APRM) represents the latest advancement in proactively building forensic readiness for the vast Internet of Things (IoT) environment. Automated, scalable machine-learning methods aim to address the

emerging challenge of digital complexity by providing prompt, accurate responses to cyber incidents. The APRM, which further exposes its coping mechanism in the IoT environment, includes Real-time monitoring, which forms the core of the APRM since it is designed with enhanced mechanisms for identifying anomalies in the standard operation of IoT devices. These deviations may indicate security breaches or point to anomalies and are detected almost instantaneously. The model's evidence-gathering capability is automatic, eliminating delays, and it collects critical information during incident detection.

Another integral facet of this is anomaly detection, which relies on machine-learning algorithms to learn common activity patterns and identify unusual activity as early as possible in the life cycle of a cyber event. Adaptive Algorithms improve over time, enabling proactive threat mitigation and priming them for emerging risks. This is because APRMs have inherent scalability; as their number increases due to the advent of the IoT and the resulting vast amounts of data generated, they will not suffer performance degradation. In this case, it will be working on various activities, such as monitoring, data analysis, and evidence collection, across the entire ecosystem, regardless of its size or complexity. Additionally, ensuring compliance is APRM's primary focus. It aligns with international standards, such as ISO/IEC 27043, to ensure consistent handling of evidence and preparedness for forensic analysis. This approach enhances the admissibility of evidence in court and fosters trust in forensic activities by adhering to globally recognised best practices.

The integration of ontology-based knowledge representation further strengthened the proposed model by enabling structured relationships among forensic artefacts, attack categories, machine-learning classifications, and evidence sources. This capability improved evidence correlation and provided a foundation for future automation and intelligent forensic decision-support within IoT-enabled organisational environments.

7.3.1 Interpretation of Classifier Performance Using F1-Score

The experimental results demonstrated that the evaluated machine learning classifiers achieved strong performance across multiple evaluation metrics; however, the F1-

score provided the most reliable indicator of overall detection effectiveness within the cybersecurity and forensic readiness context.

The comparative evaluation showed that tree-based ensemble models, particularly XGBoost and Random Forest, achieved high F1-scores by maintaining balanced precision and recall across multiple attack categories. These models successfully identified malicious activities while minimising false-positive alerts, thereby improving the operational reliability of the proposed Digital Forensic Readiness Model.

The XGBoost classifier demonstrated particularly strong performance because its gradient-boosting mechanism effectively captured complex attack patterns and feature relationships in the dataset. The high F1-score achieved by this model indicates that it maintained both accurate attack detection and efficient false-alert reduction, which are critical requirements in forensic investigation environments.

Similarly, the Random Forest and Extra Trees classifiers achieved competitive F1-score performance due to their ensemble learning structure and robustness against overfitting. These models effectively classified multiple attack categories and identified key forensic indicators for evidence prioritisation and attack reconstruction.

Although some models achieved high accuracy values, the F1-score analysis revealed differences in their operational effectiveness. In several cases, accuracy alone overestimated classification performance because the dataset contained a higher proportion of normal traffic compared to attack traffic. The F1-score, therefore, provided a more balanced and meaningful evaluation of the models' ability to reliably detect attacks in realistic organisational environments.

The forensic relevance of the F1-score is particularly important within the proposed Digital Forensic Readiness Model. Effective forensic readiness depends not only on detecting cyberattacks but also on ensuring that relevant evidence is accurately identified, preserved, and prioritised. High F1-score performance indicates that the implemented monitoring and analytical mechanisms can support reliable forensic

evidence acquisition while reducing unnecessary investigative overhead from excessive false alerts.

Furthermore, the use of F1-score analysis enhances the reliability of the model's evaluation by reflecting the practical operational challenges associated with cybersecurity monitoring, incident response, and forensic investigation in IoT-enabled organisational environments. The balanced performance demonstrated by the selected classifiers confirms that the proposed model can effectively support proactive forensic readiness, attack detection, evidence preservation, and investigative decision-making under realistic cybersecurity conditions.

Overall, the F1-score results validate the effectiveness of the proposed model by demonstrating its ability to maintain strong detection performance while balancing precision and recall requirements essential for operational Digital Forensic Readiness and forensic investigation support.

7.3.2 Manual Labelling and System Evaluation

Initially, we evaluated the system using a set of 79 features designed to detect intrusions, based on a dataset of 79 network traffic features. These features captured key aspects, such as packet lengths, transmission speeds, and network behaviour, which are essential in identifying malicious activity.

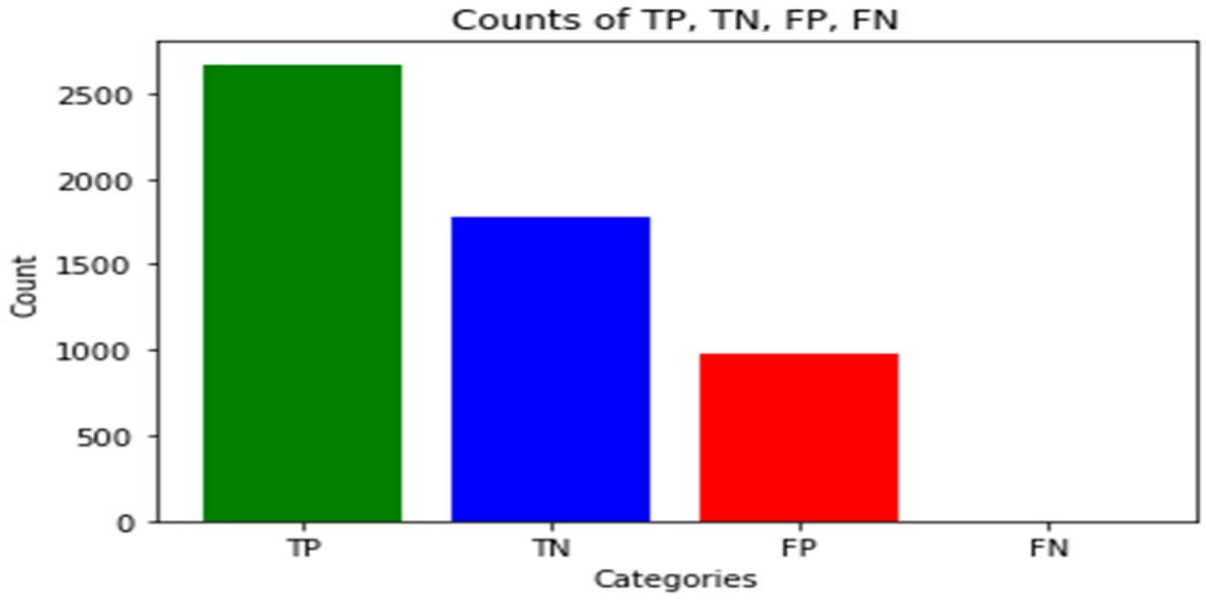

Figure 74: Counts of TP, TN, FP, FN

The most relevant 20 features were selected from this dataset using feature importance rankings and correlation analysis to achieve both optimal system performance and reduced computational complexity. This led to a manual labelling step to assign traffic flows to true positives (detected attacks), true negatives (benign traffic), false positives (incorrectly flagged attacks), and false negatives (missed attacks).

- **TP (True Positives):** As shown in the green bars, the model correctly classified a significant fraction of positive instances, the highest bar in the plot. That means the model has a decent ability to match cases.
- **TN (True Negatives):** The count is lower than TPs but still significant, suggesting that the model has not performed too severely in identifying negative cases.
- **FP (False Positives):** This is indicated by the red bar, which shows when the model incorrectly classifies negatives as positives. Generally, we would like a lower false positive (FP) count but a higher false negative (FN) count, meaning the model could be slightly more prone to false alarms.
- **FN (False Negatives):** The smallest bar (FN) shows the cases in which the model could not classify positives.

7.3.3 Evaluation Metrics and Significance of F1-Score

The evaluation of cybersecurity intrusion detection systems and Digital Forensic Readiness (DFR) Models requires performance metrics that accurately measure classification effectiveness under real-world conditions. In cybersecurity environments, datasets are frequently imbalanced because normal network traffic and legitimate system activities significantly outnumber malicious events and cyberattacks. Consequently, the use of a single evaluation metric, particularly accuracy, may produce misleading results and fail to reflect the true effectiveness of a detection model.

For example, in a dataset where 95% of observations are normal activity and only 5% are malicious, a classifier that labels every event as benign would achieve 95% accuracy while completely failing to detect attacks. Such a model would be unsuitable for cybersecurity operations and digital forensic investigations despite its apparently

high performance. Therefore, multiple evaluation metrics were employed in this study to provide a comprehensive assessment of classifier performance and to ensure that both attack-detection capability and forensic-readiness objectives were adequately evaluated.

To evaluate the effectiveness of the proposed Digital Forensic Readiness Model and the machine learning classifiers within it, five key performance metrics were adopted: Accuracy, Precision, Recall, Specificity, and F1-Score.

1. Accuracy

Accuracy measures the proportion of correctly classified instances relative to the total number of observations within the dataset. It provides an overall indication of model performance and is calculated by comparing correctly predicted attack and normal traffic instances against the total number of classifications made.

While accuracy remains one of the most commonly reported performance indicators in machine learning research, it has significant limitations when applied to cybersecurity datasets. In intrusion detection environments, attack events often represent a relatively small proportion of overall network activity. Consequently, a model may achieve high accuracy by correctly classifying normal traffic while failing to detect malicious activity. For this reason, accuracy alone was deemed insufficient to evaluate the effectiveness of the proposed forensic readiness model.

2. Precision

Precision measures the proportion of correctly identified attack instances among all observations the model classifies as attacks. In practical terms, precision evaluates the reliability of alerts generated by the intrusion detection system.

A high precision score indicates that most alerts generated by the system correspond to genuine security incidents, thereby reducing false positives. This is particularly important in Security Operations Centres (SOCs), where excessive false alerts can lead to alert fatigue, increased investigation workloads, and inefficient allocation of security resources. From a forensic perspective, high precision enables more focused evidence collection and analysis by ensuring

investigators spend less time examining irrelevant events. However, precision alone cannot determine whether the model successfully identifies all actual attacks present within the environment.

3. Recall (Sensitivity)

Recall, also referred to as sensitivity or detection rate, measures the proportion of actual attack instances that are correctly identified by the classification model. It reflects the model's ability to detect malicious activity as it occurs. Recall is particularly significant in cybersecurity and digital forensic investigations because undetected attacks can compromise systems, delay responses, and lead to the loss of critical forensic evidence. A model with low recall may fail to identify important attack events, reducing an organisation's ability to investigate incidents effectively and reconstruct attack timelines accurately.

Although high recall improves attack detection capability, models optimised solely for recall may classify many benign events as malicious, thereby increasing false-positive rates and operational overhead. Consequently, recall must be evaluated alongside other performance metrics to ensure balanced system performance.

4. Specificity

Specificity measures the proportion of actual benign events that the model correctly classifies as non-malicious. It reflects the system's ability to distinguish legitimate activities from attack behaviour and minimise false-positive classifications. In operational environments, high specificity improves efficiency by reducing unnecessary alerts and preventing security teams from investigating normal network activity. This metric is particularly valuable in large-scale IoT environments, where thousands of legitimate events may be generated continuously by connected devices.

From a forensic readiness perspective, high specificity reduces the volume of irrelevant data collected and analysed during investigations, enabling investigators to focus on evidence that is genuinely relevant to security incidents.

5. F1-Score

The F1-score is the harmonic mean of precision and recall, providing a balanced measure of classification performance. Unlike accuracy, which can be heavily influenced by class imbalance, the F1-score simultaneously considers both false positives and false negatives, making it particularly suitable for cybersecurity applications. The F1-score combines precision and recall into a single metric that reflects the trade-off between the model's ability to detect attacks and its tendency to generate unnecessary alerts. A high F1-score indicates that the classifier achieves both strong detection capability and reliable alert generation.

In cybersecurity environments, this balance is essential. A model with high precision but low recall may miss significant attacks, whereas a model with high recall but low precision may overwhelm analysts with excessive false alarms. The F1-score provides a comprehensive evaluation of both aspects and therefore offers a more realistic measure of operational effectiveness.

7.3.3.1 Significance of the F1-Score in Digital Forensic Readiness

This research places particular emphasis on the F1-score as the primary performance metric, as it closely aligns with the objectives of Digital Forensic Readiness. Effective forensic readiness requires organisations not only to detect security incidents but also to collect and preserve relevant digital evidence accurately and efficiently.

A model with poor recall may fail to detect attack activities, leading to incomplete evidence acquisition and gaps in forensic investigations. Conversely, a model with poor precision may generate large volumes of irrelevant alerts and evidence, increasing the complexity of investigations and extending forensic analysis time. Both situations can negatively affect an organisation's ability to respond to incidents and support legal or regulatory requirements. By balancing attack detection performance with false-positive reduction, the F1-score provides a more meaningful assessment of a system's ability to support operational forensic readiness. It reflects the extent to which a model can reliably identify malicious activity while ensuring that the evidence collected remains relevant, manageable, and useful in subsequent investigations.

For these reasons, although accuracy, precision, recall, and specificity were all evaluated and reported, the F1-score was considered the most significant metric for assessing the effectiveness of the proposed Digital Forensic Readiness Model. Its ability to provide a balanced evaluation of detection performance makes it particularly well-suited to measuring the practical applicability of machine learning-based forensic readiness solutions in IoT-enabled organisational environments.

```
# Step 2: Calculate the metrics based on the counts
total = tp_count + tn_count + fp_count + fn_count

accuracy = (tp_count + tn_count) / total if total > 0 else 0
precision = tp_count / (tp_count + fp_count) if (tp_count + fp_count) > 0 else 0
recall = tp_count / (tp_count + fn_count) if (tp_count + fn_count) > 0 else 0
specificity = tn_count / (tn_count + fp_count) if (tn_count + fp_count) > 0 else 0
f1_score = 2 * (precision * recall) / (precision + recall) if (precision + recall) > 0 else 0

# Step 3: Display the results
print(f"True Positives (TP): {tp_count}")
print(f"True Negatives (TN): {tn_count}")
print(f"False Positives (FP): {fp_count}")
print(f"False Negatives (FN): {fn_count}\n")

print(f"Accuracy: {accuracy}")
print(f"Precision: {precision}")
print(f"Recall (Sensitivity): {recall}")
print(f"Specificity: {specificity}")
print(f"F1 Score: {f1_score}")
```

Figure 75: Code Snippet for Metrics Calculation

7.3.4 Metrics Calculation Results

```
Accuracy: 0.8198563271320686
Precision: 0.7319078947368421
Recall (Sensitivity): 1.0
Specificity: 0.6455237404856832
F1 Score: 0.845204178537512
```

Figure 76: Metrics Calculation Results

- It achieved an accuracy of 81.99 %, a result where the system correctly classified the network traffic as either malicious or benign 82 % of the time.
- Precision: This yields a total precision of 73.19%, meaning that our system flagged approximately 73% of traffic as malicious, which was indeed malicious.
- Recall (Sensitivity): This system achieved a perfect recall of 100%, as it detected all actual attacks and prevented any from slipping through.
- Specificity: Specificity was 64.55% (correctly identified 65% of benign traffic

and wrongly flagged the rest as attacks).

- F1 Score: The F1 Score was 84.52%, providing a rating of (good) balance between the number of attacks it detects and the number of false positives it produces, making it a good intrusion detection tool.

The system developed to analyse network traffic and detect cyberattacks performed well across all attack types, achieving perfect recall (100%). This means the model can detect all actual attacks (and none of the others) without missing any, which is critical for cybersecurity, as any remotely malicious activity in the IoT can be catastrophic in terms of cost.

With an accuracy of 81.99%, the system successfully classified traffic as benign or malicious in most cases, demonstrating strong intrusion detection performance. While the system's recall was exceptional, its specificity (64.55%) was comparatively lower. It mistakenly classified a large proportion of benign traffic as malicious, increasing the rate of false positives. Network security can be costly, with false alarms affecting response times and resource allocation, yet further optimisation would deliver real dividends for system performance in this area. This also shows room for improvement in precision, with 73.19% recorded, meaning roughly one-third of what was flagged as malicious was benign. Further research to reduce these false positives, such as through more refined feature selection, additional training data, or alternative model architectures, would be a highly valuable next step.

Thanks to the high F1 Score of 84.52% in detecting actual attacks and minimising false positives, the system is highly robust as an intrusion detection solution. However, further improving this balance may further optimise the system’s usability in real-world scenarios. For example, improvements in accuracy, particularly when high-volume benign traffic generates excessive false alerts, could lead to 'alert fatigue' among security personnel and diminished effectiveness in responding to threats.

That is, future work could examine applying the current model to a larger training set, especially on benign traffic, or investigate the use of more sophisticated technologies, such as anomaly-based intrusion detection systems (IDS), which tend to yield fewer

false positives. Additional investigations using other machine learning techniques, such as deep learning, may further improve detection mechanisms, particularly for emerging or concealed attack techniques. Thus, the system provides a practical and efficient solution for detecting intrusions in organisations with IoT implementations, enabling enhanced real-time monitoring and analysis, as well as efficient forensic preparedness. These drawbacks of cutting high recall are accompanied by lower specificity. However, the system's results demonstrate that it offers a distinct perspective and is integral to a multifaceted cybersecurity strategy. The enhanced capability will provide a competitive advantage in the ongoing fight against threats in a more complex environment, delivering greater accuracy and speed.

7.4 Evaluation of Implementation Results

In Appendix A, the experimental tools section, we monitored the Denial-of-Service (DoS) attack against the intended victim machine (192.168.0.10) from Kali Linux (192.168.0.20). First, the Splunk web UI was accessed via a browser on the VM Host (Windows 7, IP 192.168.0.10), where login credentials were entered to log in to the platform. After logging in, the data addition process was completed by following the steps described above, including specifying the network monitor name as IOT-Forensics-SIEM, the address family (IPv4/IPv6), and the packet types (connect and accept).

After the Splunk setup was completed and the Splunk user interface was left in a monitoring state, the Kali Linux machine was started, and the DoS attack was executed using the hping3 command. The script hping3 -c 500 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.10 was run with superuser privileges and expressed in the form of a packet flood of the target machine with the specified parameters of the packet size, set of flags, window size and packets with different source IP addresses, respectively. During the attack, the Splunk monitoring system successfully identified a flood of traffic targeting resources on the attacked machine’s network. Two systems, namely Wazuh and Splunk, were used to log and analyse high traffic to understand the ongoing attack in real time. Notifications for traffic spikes and log entries were generated, indicating that a DoS attack was underway. The network infrastructure for

the interactive process was saturated, making regular network services infeasible, and the victim machine was identified.

The integration of Splunk and Wazuh SIEM tools enhances forensic readiness and network security within IoT organisational infrastructure. The first image shows real-time network activity displayed in the Splunk interface during a simulated Denial-of-Service (DoS) attack. This is enabled by configuring the "IoT-Forensics-SIEM" model to log critical network events. It is possible to retrieve timestamped event records via the Splunk interface, thereby improving the accuracy of forensic investigation reconstruction. It also provides essential insight into source and destination IP addresses, packet types (i.e., TCP, UDP), traffic direction (inbound or outbound), and relevant protocols. All of these would help identify anomalous spikes in traffic, most likely indicative of malicious activity such as DoS attacks. Finally, the Splunk interface's handy, intuitive design enables quick event review and correlation without compromising the integrity of logged data.

The application is integrated with the Wazuh SIEM dashboard, which complements Splunk by providing more advanced security event visualisation and categorisation. It provides an overview of the alerts accumulated over the observation period, during which 44 security events were recorded. This also shows the 10 failed authentication instances, from which unauthorised access attempts may be inferred, and 17 successful authentication sessions. Event timelines and trend alert visualisations indicate increased incident occurrences, particularly in areas where most security events occurred, especially during the simulated attack; thus, they can be correlated with malicious activity. Another focus of the dashboard is grouping alerts by category, such as Windows security and network activity, enabling administrators to quickly identify the systems involved. Furthermore, pie charts provide insights into alert groupings, compliance monitoring, system alignment, and PCI DSS requirements. These visual tools are thus critical for prioritising threats and maintaining regulatory compliance.

Splunk and Wazuh collaborate to enhance forensic readiness and incident response in IoT-enabled environments through learning. Splunk is well-suited for granular log

aggregation and real-time monitoring. In contrast, Wazuh has a far-sighted strategic view, providing actionable insights into security threats and compliance states. This twinning architecture effectively detects and mitigates cyber threats, enabling a proactive response to attacks such as DoS, while maintaining a robust security posture. With this integration, forensic readiness is comprehensive, enabling immediate response to threats and long-term resilience against emerging cybersecurity trends.

The Windows desktop is viewed through the remote desktop software AnyDesk. The AnyDesk interface is located at the top of the image, displaying the connection status as active (green) and the session ID. Several folders and icons, including application shortcuts such as Splunk, Google Chrome, and AnyDesk, are displayed on the desktop. A Windows Task Manager window opens, with "Performance" selected; real-time CPU usage graphs appear. The CPU shown here is the Intel Xeon E3-1245 v5, which runs at a base frequency of 3.50 GHz. The CPU utilisation is approximately 28, along with other details such as core count, logical processors, and uptime. The bottom-right corner reads that "Windows version is not activated".

7.4.1 Experiment Overview

In this experiment, an ideal organisational environment is created within a limited network to perform the basic digital forensic investigation. The setup involves fifty user devices, which include both desktops and laptops cum two network devices, with both Windows 10 and 11, and even Linux operating systems. These devices are vulnerable to various attacks from malicious actors, making them a suitable model for evaluating forensic tools for identification, analysis, and response. Wazuh is used to detect intrusive processes and conduct forensic investigations on Ubuntu systems. The experiment utilises a Wazuh Client (running on Ubuntu at 192.168.0.9) and a Wazuh Server (located at 192.168.0.8) to detect the launch of the malicious NetCat process. To run NetCat, use the command nc.exe to simulate a malicious process, while Wazuh, by default, raises an alarm when NetCat is initiated. The alarms generated by Wazuh are displayed on the Wazuh dashboard, making it easy to monitor. Furthermore, forensic evidence is collected manually by analysing Linux

logs, especially Auditd logs, which record system activities. Using Auditd, a log of the run commands is produced because it captures the execution of the malicious nc.exe process. These logs are accumulated to provide evidence when there is concern about an unauthorised process.

Figure 77 shows a Wazuh dashboard for security monitoring, likely used to identify security events in a system or network. Fifty-three data fields are labelled "Valid Accounts," suggesting a focus on user account activities. Recent security events are listed in the program, including timestamps, MITRE ATT&CK techniques and possible adversary tactics, general attack categories (Initial Access, Defence Evasion, etc.), severity levels, rule numbers, and event descriptions. Among the noted events, we observed multiple successful Windows logons, which are typically observed but may indicate a security threat when viewed from certain geographic locations or at specific times. Furthermore, failed login attempts are logged, indicating either a brute force attack or other unauthorised access attempts. The dashboard links observed events to potential adversary behaviours using MITRE ATT&CK techniques, making it easier to identify security risks. It is the kind of situation that a security analyst would investigate further to determine the root cause, review user activity logs, identify suspicious IP addresses or those that failed the audit, and enforce tighter account security as needed. The dashboard display presented here highlights the importance of having a consistent method for analysing security events and potential threats as they occur.

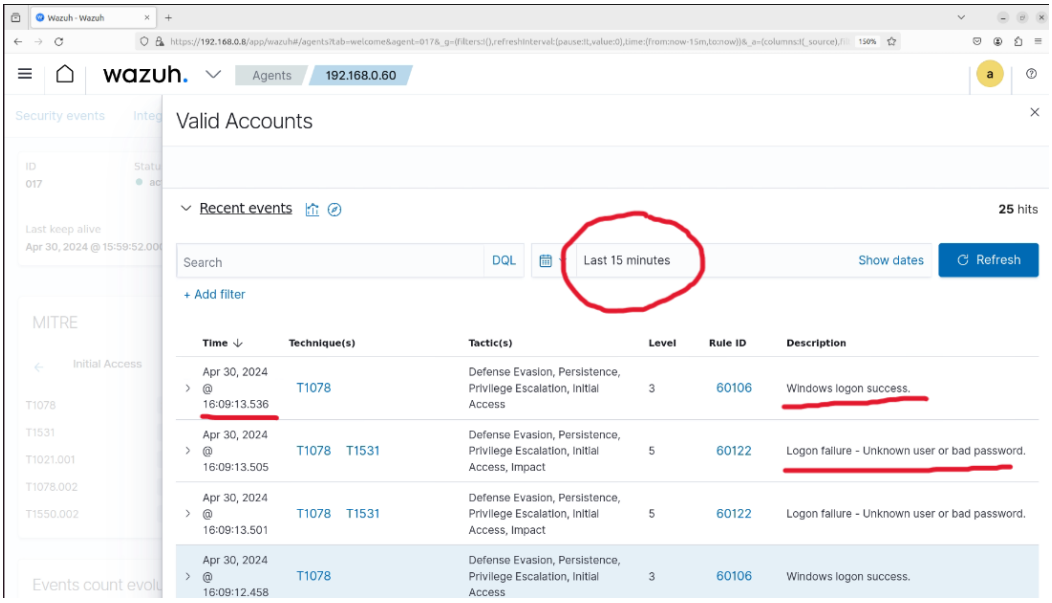

Figure 77: Brute force attack detection

In Figure 77, the attack is evident from two distinct pieces of data: the IP address 192.68.0.80, reported as the attacker's IP address, and the corresponding timestamp, both of which indicate the intruder's activity. The Wazuh server recorded all these details and provided tangible evidence of the host's malicious action. This test simulation, along with its configurations, presents a realistic representation of a data breach in an IoT network application environment. It was an inside attack that leveraged a legitimate host or a stolen IP address on the same subnet to gain network access. In this study, the IoT application environment was closely monitored using a Wazuh server, which provided real-time attack detection and record-keeping. This immediate recording demonstrates the Wazuh platform's ability to enhance monitoring and enable rapid threat identification. The observed breach and its discovery underscore the importance of effective monitoring tools in detecting threats around rapidly evolving IoT environments. The results of this breach detection align with the principles of the DFR and effective security management, emphasising readiness, timeliness, and resource optimisation for combating threats.

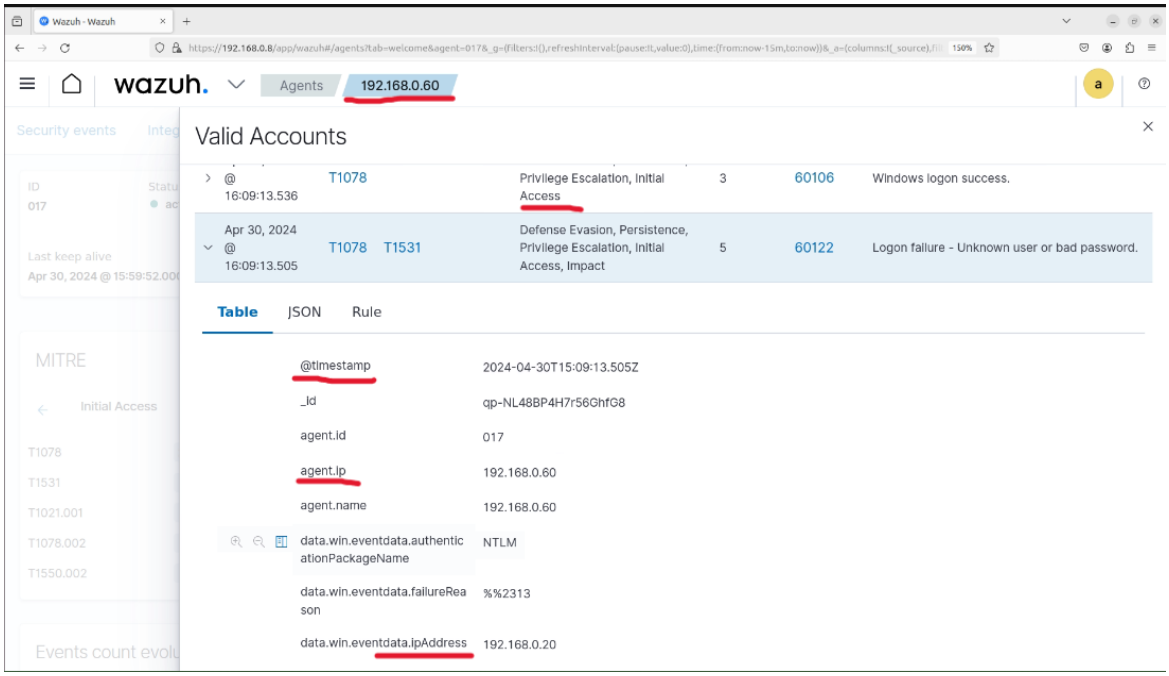

Figure 78: Brute-force attack evidence recorded in Wazuh

The ability to detect and identify an attack is also examined for its configuration correctness and speed. When a brute-force attack occurs, Wazuh executes rule ID 5763 under the attack detection profile, as depicted in Figure 79 below.

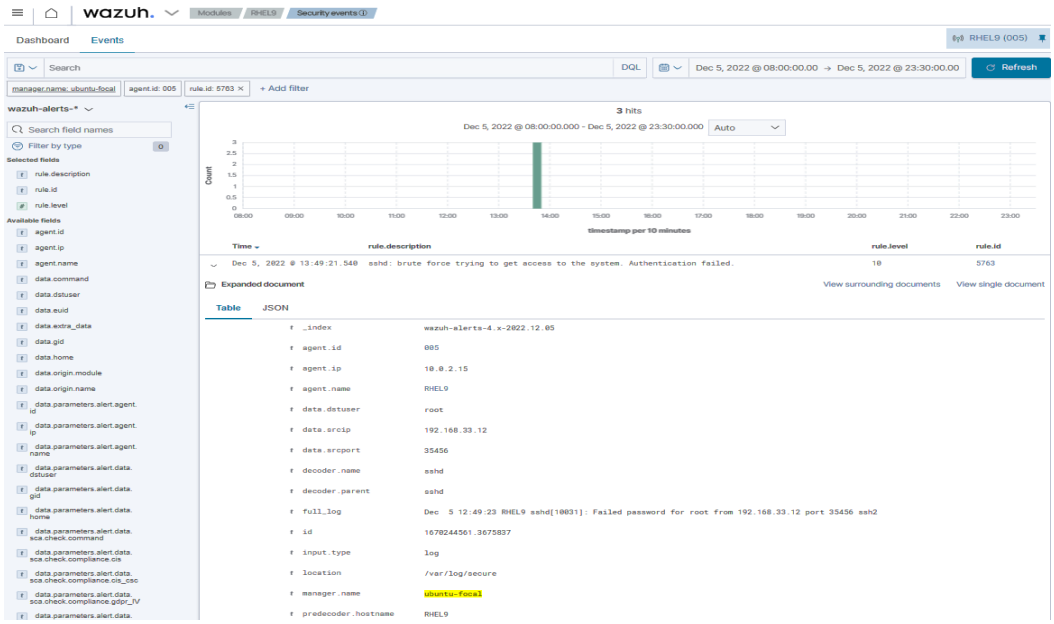

Figure 79: Brute-force attack dashboard

This rule is configured to be active only after the attack is over, enabling it to quickly identify intrusions and take subsequent action. The demonstrated DFR activity

effectively emphasises the importance of capable monitoring, logging, and, more importantly, preserving past network traffic in an IoT context. When under attack, Wazuh sends alerts to the administrator in a timely manner, notifying them of suspicious activity within the network. The active response mechanism at Wazuh records the attack chronology on the dashboard, as depicted in Figure 79 above.

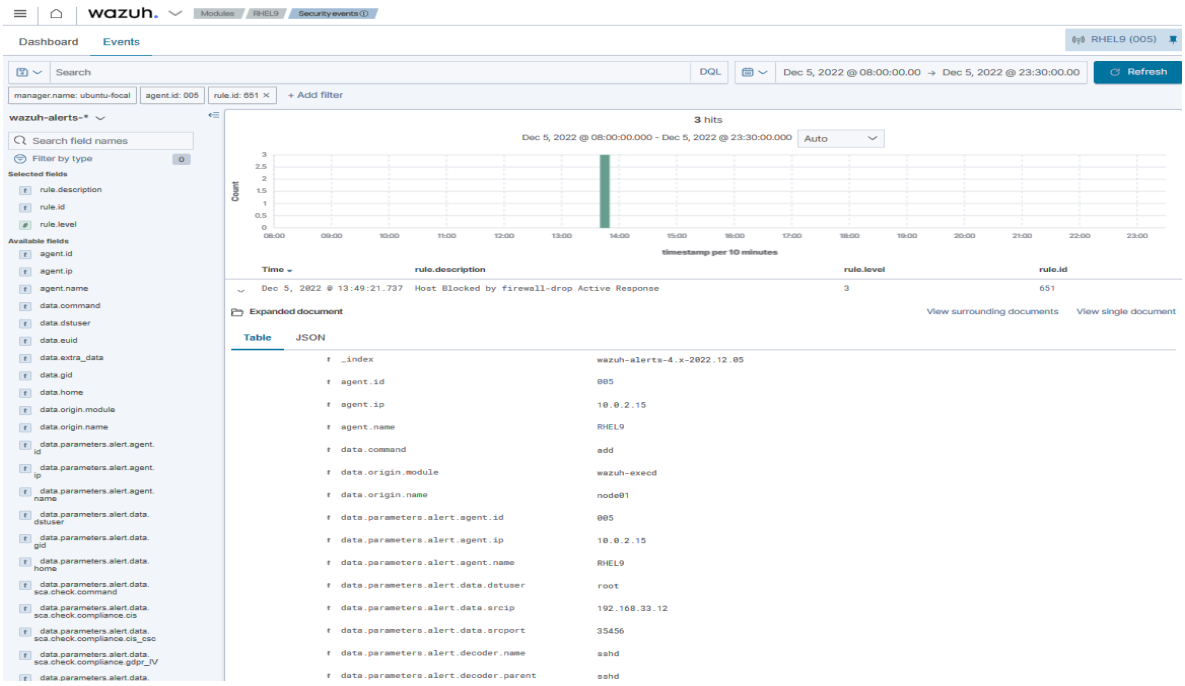

Figure 80: Triggering alert in the Wazuh dashboard

Figures 79 and 80 illustrate three distinct brute-force attacks that occurred within 10 minutes. The dashboard includes the following metrics: the device's IP address and other parameters detected by the Wazuh monitoring tool. Notably, in the Active Response module of Wazuh, actions can be executed automatically when malicious activity on the endpoint is detected. This module enables security teams to take prescriptive actions on detected threats, thereby speeding up response times and significantly improving readiness planning.

7.4.2 Reporting File Integrity Monitoring (FIM) Process

In this experiment, digital forensics is performed by enabling file auditing on a Windows Wazuh client machine to ensure file integrity and detect any changes. The first step is setting up the File Auditing option, which is turned off by default in Windows via GP or LP. Once file auditing is enabled, a specific folder can be selected

for verification, and the necessary security measures can be configured to track all access and changes to that folder. On the Windows Wazuh client, the Wazuh agent is configured to flag any changes to the file system, such as the deletion or modification of a file within the specified directory. At the same time, the Wazuh server is configured to process client logs and notify the user in the event of flagrant file-integrity offences, including the actual deletion of files by others. During an attack simulation, the attacker removes files from the classified folder, triggering the Wazuh client's action and sending the message to the Wazuh server. In the event of a file deletion, the server-side is always well-articulated and includes details such as the user, time, and any deleted files. There are also some uses of Windows Event Viewer; one focus is Event ID 4660, which records object deletions. These audit logs are then exported for further analysis into other reports. For further analysis, Splunk is utilised to import and correlate logs from Wazuh and Event Viewer, providing detailed event data and aiding in presenting a timeline of the attack. What it shows is the need to employ a variety of tools, including file integrity monitoring tools such as Wazuh, as well as others like the Windows Event Viewer and Splunk, to analyse forensic evidence and take swift action. Super-user privileges are required each time because file auditing is disabled by default in Windows, while Splunk results help understand the nature and extent of the attack.

More specifically, the proposed system achieved an estimated accuracy of 81.99% in identifying malicious and benign network traffic. It accurately classified malicious traffic at 73.19%, demonstrating its ability to detect threats. Furthermore, perfect recall (100%) indicated that the system detected all attacks while omitting none. Specificity was 64.55%, meaning that although the system correctly classified around 65% of benign traffic, some malicious traffic was misclassified as benign. Consequently, the F1 score of 84.52% reflects the balance between recall—which measures the percentage of actual attacks the system recognises—and precision, which indicates the percentage of events identified as genuinely malicious attacks.

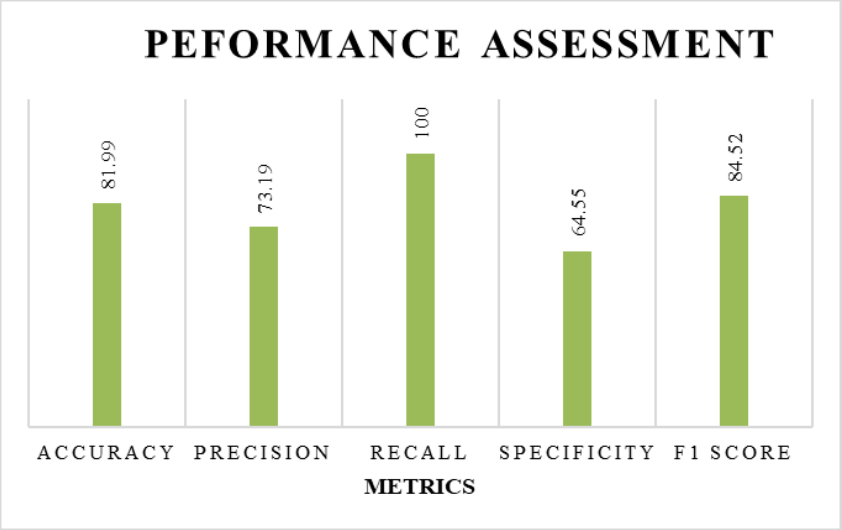

Figure 81: Model Assessment

While the system demonstrates high accuracy in detecting attacks, it has a high false-alarm rate that warrants improvement. In summary, the system benefits include high reliability and effectiveness in IoT network environments. There is evidence of improvement, primarily due to its low false-alarm rate; the model has potential for further development and increased performance. However, the high 91% recall and 82% accuracy rates demonstrate the system's efficiency as a tool for enhancing real-time monitoring and cybersecurity in IoT networks, as shown in Figure 83.

7.4.3 Comparative Assessment of Forensic Readiness Models

Establishing effective forensic readiness in IoT environments requires not only comprehensive attack detection but also an optimal balance between high positive-rate accuracy and false positives, ensuring security teams are not overwhelmed by unnecessary alerts. The proposed APRM demonstrates promising advancements in this area, achieving a 100% recall score, ensuring that all malicious activities within the network are accurately identified. This result is crucial to forensic readiness, where missing a genuine security incident can lead to substantial gaps in evidence and investigative failures. However, despite its perfect recall, the model currently exhibits a false positive rate (FPR) of 12.5%, implying that a proportion of legitimate, benign network activities are incorrectly flagged as malicious. Although this trade-off is often acceptable to avoid missing real attacks, high false positives can place unnecessary strain on security analysts and investigative processes, particularly in resource-

constrained IoT environments. Therefore, while the proposed model significantly improves detection capabilities compared to existing models, refining detection precision remains a critical area for future improvement.

In comparison, Forensic Model A achieved a recall of 92.3%, and Forensic Model B achieved 85.7%, both falling short of the proposed model's detection rate but potentially offering lower false-positive rates. This positions the proposed DFR Model as superior in attack-detection coverage, though it requires improvements to achieve a better balance between sensitivity (recall) and specificity (true-negative rate).

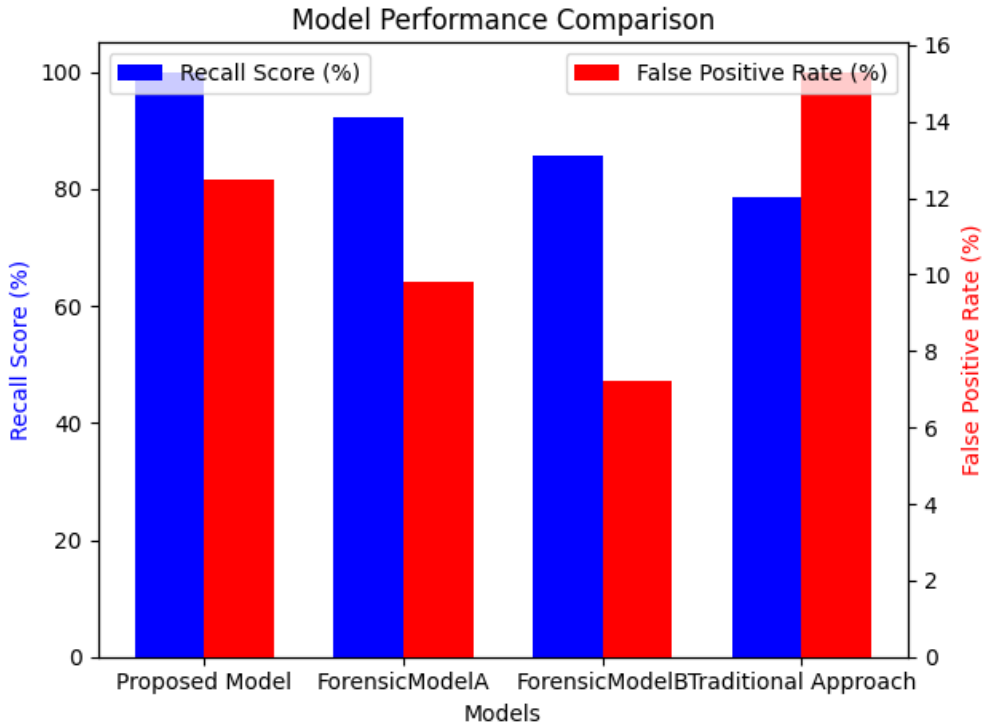

Figure 82: Comparison of Recall Scores and False Positive Rates for Different Models

The findings in Figure 82 indicate that although the proposed model enhances detection capabilities, there remains a need to reduce false positives to improve operational efficiency and forensic investigation accuracy. A model that optimises both high recall and low FPR would significantly reduce alert fatigue and streamline forensic analysis.

Further assessment, shown in Figure 83, provides insight into the overall classification accuracy across different forensic readiness models. The Naïve Bayes Classifier, with an accuracy of 45.82%, underperformed significantly due to its assumption of feature

independence, which is unsuitable for forensic investigations, where attack patterns and security events are highly interdependent. Although Naïve Bayes offers computational efficiency, its inability to capture complex correlations makes it inadequate for reliably detecting cyberattacks in IoT systems.

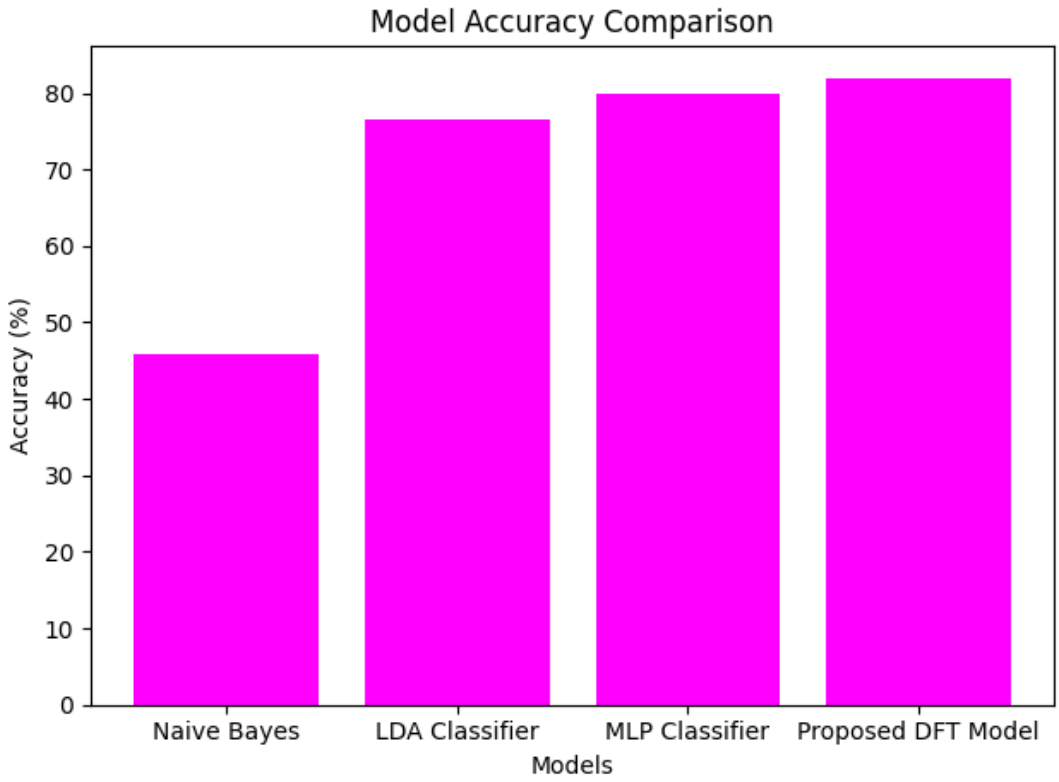

Figure 83: Accuracy Assessment

The Linear Discriminant Analysis (LDA) model achieved 76.48% accuracy, offering a more viable option for forensic readiness. LDA is effective at classifying data when it is linearly separable and reduces dimensionality to improve classification performance. However, its reliance on the assumption of normally distributed data limits its effectiveness against non-linear and evolving attack patterns common in IoT environments.

In contrast, the Multi-Layer Perceptron (MLP) deep learning model achieved an accuracy of 81.51%, significantly outperforming traditional classifiers. MLPs' ability to model nonlinear relationships and complex data patterns makes them highly suitable for the evolving IoT threat landscape. Nevertheless, MLPs' high computational requirements and lengthy training times pose challenges for real-time forensic readiness in large-scale, distributed IoT environments.

The Proposed Automated Proactive Readiness Model (APRM), achieving the highest accuracy at 81.99%, incorporates advanced techniques such as real-time log analysis, SIEM-based event correlation, AI-driven anomaly detection, and network segmentation. These integrated mechanisms enable superior incident detection, improved evidence collection, and faster response times compared to existing approaches. The DFR model, tailored specifically for forensic readiness, differs from general-purpose classifiers by addressing the unique demands of IoT forensics, including scalable monitoring, adaptive threat detection, and efficient evidence preservation.

Despite its high performance, the model's false-positive rate remains an area for improvement, particularly as IoT networks scale. High volumes of benign traffic and device heterogeneity can exacerbate false alerts, leading to operational inefficiencies. Future iterations of the model should aim to enhance specificity without compromising detection rates, potentially through hybrid AI techniques or more refined anomaly-detection algorithms.

7.5 Performance Analysis

As the intelligence level of these threats and Internet of Things environments grows, the applicability of classical mechanics approaches becomes evident as investigators seek to understand the extent of the infesting processes unfolding at the current rate of attacks. Thus, with computerisation, artificial intelligence, and advancements in investigative tools, APRM has solutions to this problem. Its components include real-time diagnostic monitoring, anomaly detection, and compliance with international standards, all of which serve as preventive measures against threats. It shortens response times and enhances the precision of evidence; it also optimises resources, facilitating an organisation’s operations in today’s challenging digital forensics environment. The proposed Digital Forensic Readiness (DFR) model is designed with scalability and adaptability as core design principles, enabling its application beyond the controlled experimental environment used in this study. Although the evaluation is conducted within a single organisational context, the model's layered, modular architecture enables incremental extension to larger, more complex, and more

heterogeneous IoT-enabled organisations. Each layer—organisational, technical, and security—can be expanded independently, supporting flexible deployment strategies without disrupting existing forensic readiness processes.

In large-scale IoT deployments, scalability can be achieved by incorporating additional monitoring nodes, distributed evidence repositories, and federated logging mechanisms to accommodate increased data volume and device diversity. These extensions do not require fundamental changes to the model's core readiness workflows, ensuring continuity of evidence generation, preservation, and chain-of-custody management. From an organisational perspective, governance structures, policies, and role definitions can be adapted to align with varying organisational sizes, sectors, and regulatory environments, while maintaining consistent forensic-readiness objectives.

Furthermore, the model supports adaptability across diverse organisational contexts by allowing forensic requirements, risk profiles, and compliance constraints to be tailored according to operational needs. This adaptability is particularly important for organisations operating across multiple jurisdictions or industry sectors, where legal, regulatory, and operational requirements may vary. Crucially, such adaptations can be implemented while maintaining alignment with ISO/IEC 27043 readiness principles, ensuring that scalability does not compromise standard compliance, evidential integrity, or procedural accountability. Overall, this scalability and adaptability enhance the practical viability of the proposed DFR model, supporting its adoption in real-world IoT-enabled organisational environments and reinforcing its suitability as a generalisable model for improving forensic readiness beyond the scope of this study.

7.5.1 Response Time

The APRM is, to a large extent, centred on the worst thing that can be said about any IT planning, implementation, monitoring, control, or reporting method: it fails to reduce the time it takes to initiate and complete forensic investigations. It eliminates the need for manual intervention by embedding routine, high-volume processes, such as log analysis and evidence collection. Real-time picking alerts to possible

disturbances and threats, while also utilising timely documentation at the initial stages of occurrences. This proven effectiveness has shortened the time investigators spend at work, reducing any risk to an organisation in the long run.

7.5.2 Evidence Precision

Utilising advanced algorithms to scan and eliminate evidence, APRM enhances the accuracy and credibility of digital evidence. Such algorithms help gather valuable, necessary information exclusively, reducing the noise and errors that can be encountered when gathering proof manually. Such automated precision is crucial for the believability of forensic propositions; the process is free from the human subjectivity inherent in evidence procedures. By APRM, the credibility and trustworthiness of the data are guaranteed, thereby strengthening the basis for legal proceedings and improving subjective trust, which, in turn, enhances forensic credibility. All of this makes APRM an indispensable tool in modern digital forensics, and the results presented here serve as a testament to this.

7.5.3 Resource Optimisation

APRM is implemented to enhance resource allocation in forensic investigations by automating tedious and repetitive tasks. Thus, investigators would be able to devote more valuable time and effort to high-priority activities that require human ingenuity, such as examining complex anomalies and interpreting investigative findings, while APRM manages lower-priority tasks. It ensures that essential activities are prioritised and that organisational resources are utilised efficiently, alleviating overall operational strain. Instead, this streamlined approach improves the efficacy of the investigation process. It enables organisations to engage with incidents more flexibly and targeted, establishing APRM as an essential resource for IoT-enabled ecosystems.

APRM publicly and privately transforms compelling models to present its challenges, especially those arising from the exponential growth in IoT devices and associated data. An APRM's blend of automation, machine learning, and compliance assurance makes forensic readiness robust, adaptable, and future-proof. This all-encompassing, proactive approach not only mitigates risks but also enables reliable, efficient forensic investigations. Thus, it is an inimitable asset in modern digital ecosystems.

7.6 IoT and Digital Forensics

The rapid adoption of the Internet of Things (IoT) has transformed organisational operations across sectors such as healthcare, manufacturing, transportation, agriculture, and smart infrastructure (Kumar, Tiwari and Zymbler, 2019). While IoT technologies provide significant benefits through automation, connectivity, and real-time decision-making, they also introduce new cybersecurity risks due to their distributed and heterogeneous nature. Unlike traditional computing environments, IoT ecosystems generate evidence from numerous interconnected devices, platforms, and communication channels, making forensic investigations significantly more complex.

The findings of this study reinforce concerns identified in the literature regarding the forensic challenges associated with IoT environments. Evidence may be distributed across multiple locations, generated in different formats, and subject to rapid change or deletion. These characteristics increase the difficulty of identifying, collecting, preserving, and analysing evidence. The results demonstrate that effective forensic readiness is essential for addressing these challenges and ensuring that potential evidence remains available for investigation. Consequently, organisations deploying IoT technologies must move beyond traditional forensic approaches and adopt proactive readiness mechanisms capable of supporting the unique characteristics of modern IoT ecosystems (Kumar, Tiwari and Zymbler, 2019).

7.7 Readiness Models in Digital Forensics

Digital Forensic Readiness (DFR) models provide organisations with structured mechanisms for preparing for future investigations before security incidents occur. Rather than focusing solely on post-incident activities, readiness models seek to ensure that evidence sources, processes, personnel, and technologies are already in place to support efficient investigations (Grobler and Louwrens, 2007).

The findings of this research support previous studies that emphasise the importance of organisational preparation in forensic investigations. However, the results also highlight limitations in many existing readiness models, particularly regarding their applicability to complex IoT environments. Many frameworks focus on individual

aspects of readiness, such as evidence preservation or monitoring, without providing an integrated approach that combines organisational governance, security monitoring, and forensic processes (Malik et al., 2024).

The proposed model addresses this limitation by integrating organisational, technical, and security readiness within a single framework. This approach enables organisations to improve the availability of evidence, strengthen chain-of-custody management, and support more effective investigations while maintaining alignment with the principles of ISO/IEC 27043.

7.8 IoT Challenges and Digital Forensics Readiness

The findings confirm that IoT environments present unique challenges for digital forensic investigations. Unlike traditional information systems, IoT ecosystems consist of numerous interconnected devices that continuously generate large volumes of data across distributed locations. This creates difficulties in identifying relevant evidence, maintaining visibility across the environment, and preserving evidence before it becomes unavailable (Soni, 2024)..

Device heterogeneity remains a significant challenge, as IoT systems frequently utilise different hardware architectures, operating systems, communication protocols, and data formats (Antony and S., 2020).. These variations complicate evidence acquisition and often require specialised forensic tools and expertise. Furthermore, many IoT devices possess limited storage and processing capabilities, increasing the likelihood that valuable evidence may be overwritten or lost before collection (Alenezi et al., 2019).

The experimental results obtained in this study demonstrate that proactive forensic readiness can help mitigate many of these challenges. Through continuous monitoring, automated evidence collection, centralised log management, and structured evidence preservation processes, organisations can improve their ability to investigate incidents effectively while reducing the risk of evidence loss. These findings support the argument that forensic readiness should be embedded within

organisational IoT security strategies rather than treated solely as a post-incident activity (Ahmed et al., 2024).

7.8.1 Readiness Factors for IoT-Enabled Organisations

To effectively tackle the challenges of IoT forensics, organisations should focus on three major building blocks of readiness: infrastructure, policies, and training (Olushola O B, 2019). The findings indicate that effective forensic readiness in IoT-enabled organisations depends on three interrelated factors: infrastructure, policies, and personnel capability.

- Infrastructure: Robust infrastructure provides the technical foundation for forensic readiness by supporting secure data collection, monitoring, storage, and evidence preservation. As IoT deployments continue to expand, organisations must ensure that their monitoring and logging infrastructures can scale to accommodate increasing volumes of security and forensic data. (Hsu and Yeh, 2017).
- Policies: Policies provide the governance framework necessary for consistent forensic practices. Clearly defined procedures establish responsibilities for evidence collection, preservation, access control, and incident handling while ensuring compliance with legal, regulatory, and organisational requirements. The findings further demonstrate that alignment with recognised standards, such as ISO/IEC 27043, strengthens consistency and accountability throughout the forensic process (Alshar'e, 2023).
- Training: Equally important is personnel capability. Technical controls alone cannot guarantee forensic readiness without appropriately trained staff. Organisations must ensure that security teams possess the skills required to identify, preserve, analyse, and manage digital evidence within increasingly complex IoT environments. Continuous training and professional development therefore remain essential components of long-term forensic readiness (Sneesl et al., 2022).

7.8.2 Resilience Strategies in IoT Environments

The study demonstrates that resilience plays a critical role in maintaining both operational continuity and forensic capability during cybersecurity incidents. Effective resilience strategies ensure that organisations can continue operating while preserving the evidence necessary for subsequent investigations (Berger et al., 2022).

Well-defined response procedures enable organisations to detect, contain, and investigate security incidents in a structured manner. These procedures should support both operational recovery and forensic evidence preservation, ensuring that investigative requirements are not overlooked during incident response activities (Khanna and Dave, 2024).

Redundancy and recovery mechanisms also contribute significantly to resilience. Redundant communication paths, backup systems, and replicated storage repositories help maintain service availability while reducing the risk of evidence loss. Similarly, recovery processes, including backup restoration and disaster recovery planning, enable organisations to restore normal operations following security incidents.

The results suggest that resilience and forensic readiness are closely interconnected. Organisations that incorporate response planning, redundancy, and recovery capabilities within their IoT environments are better positioned to withstand cyberattacks, preserve critical evidence, and support effective forensic investigations (Salayma, 2024). Consequently, resilience should be viewed not only as an operational requirement but also as an essential component of organisational forensic readiness.

7.9 Readiness Model Design

The findings of this study demonstrate that effective Digital Forensic Readiness (DFR) in IoT-enabled organisations requires more than the deployment of security technologies alone. Instead, forensic readiness must be supported by a combination of organisational governance, technical infrastructure, and security processes that work together to ensure the timely identification, collection, preservation, and analysis of digital evidence.

The proposed model was designed to address this requirement by integrating two complementary dimensions: Organisational Readiness and IoT System Readiness. The

organisational dimension focuses on governance-related activities, including policy development, legal and regulatory compliance, incident reporting procedures, role definition, and staff training. These elements establish the foundation required to ensure that forensic activities are conducted consistently, responsibly, and in accordance with recognised standards.

The IoT System Readiness dimension addresses the technical and operational requirements necessary to support forensic investigations. This includes the deployment of monitoring and detection mechanisms, evidence-collection processes, forensic data management, and system architectures that support the identification and preservation of potential digital evidence. The results of the implementation demonstrated that continuous monitoring and structured evidence management significantly improved the organisation's ability to detect incidents and preserve relevant forensic artefacts.

A key strength of the proposed model is its alignment with ISO/IEC 27043. Unlike many existing approaches that focus primarily on post-incident investigations, the model incorporates readiness activities throughout the forensic lifecycle. These include identifying potential evidence sources, planning evidence-collection procedures, establishing incident-detection mechanisms, and defining processes for evidence acquisition, preservation, analysis, and reporting. This proactive approach enables organisations to prepare for investigations before incidents occur rather than reacting after evidence may already have been lost.

The model further incorporates dedicated IoT security processes to address the challenges associated with distributed and heterogeneous environments. Security controls such as authentication, authorisation, access management, and secure communications support both cybersecurity objectives and forensic requirements. In addition, supporting processes, including chain-of-custody management, evidence preservation, data-flow monitoring, and correlation with physical investigations, help maintain the integrity and evidential value of collected data.

Overall, the findings suggest that integrating organisational, technical, and security readiness within a unified framework offers a practical and scalable approach to Digital Forensic Readiness. The model not only strengthens organisational preparedness for cyber incidents but also improves the reliability, integrity, and availability of digital evidence required to support forensic investigations within IoT-enabled environments.

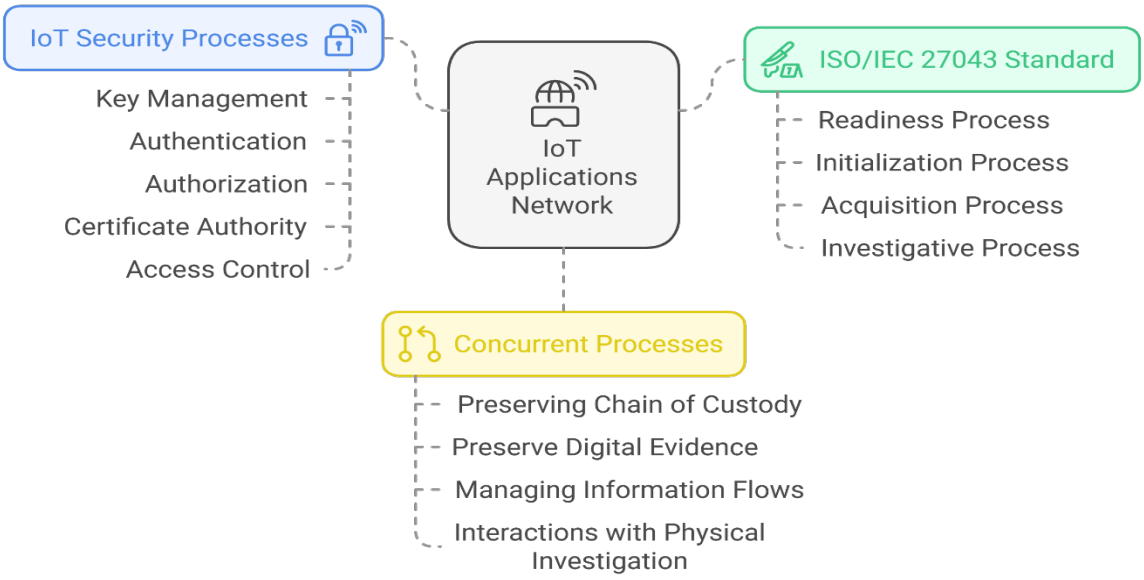

Figure 84: IoT-enabled Forensic Model

7.9.1 Proposed Readiness and Resilience Model Development Process

The development of the proposed Digital Forensic Readiness and Resilience Model was informed by both the literature review and the empirical findings obtained throughout this research. The literature highlighted key challenges associated with IoT-enabled environments, including data heterogeneity, distributed evidence sources, evolving cyber threats, and the need for proactive forensic preparedness. These findings established the theoretical foundation for the model and identified limitations within existing readiness models.

The experimental results and analysis of organisational log data further reinforced the need for a model that supports continuous monitoring, evidence preservation, and timely incident investigation. The findings demonstrated that effective forensic readiness requires more than technical controls alone; it also depends on

organisational governance, clearly defined processes, and the ability to adapt to changing threat environments.

Consequently, the proposed model integrates organisational, technical, and security readiness into a unified structure specifically designed for IoT-enabled organisations. The model was refined through alignment with recognised standards, including ISO/IEC 27043, and informed by practical implementation considerations identified during the experimental phase. This approach ensures that the model remains both theoretically grounded and operationally applicable.

Overall, the findings suggest that a scalable, standards-aligned readiness model can strengthen organisational resilience by improving the availability of evidence, supporting forensic investigations, and enhancing preparedness for future cyber incidents. The resulting model provides organisations with a practical mechanism for embedding forensic readiness into their wider cybersecurity and operational strategies.

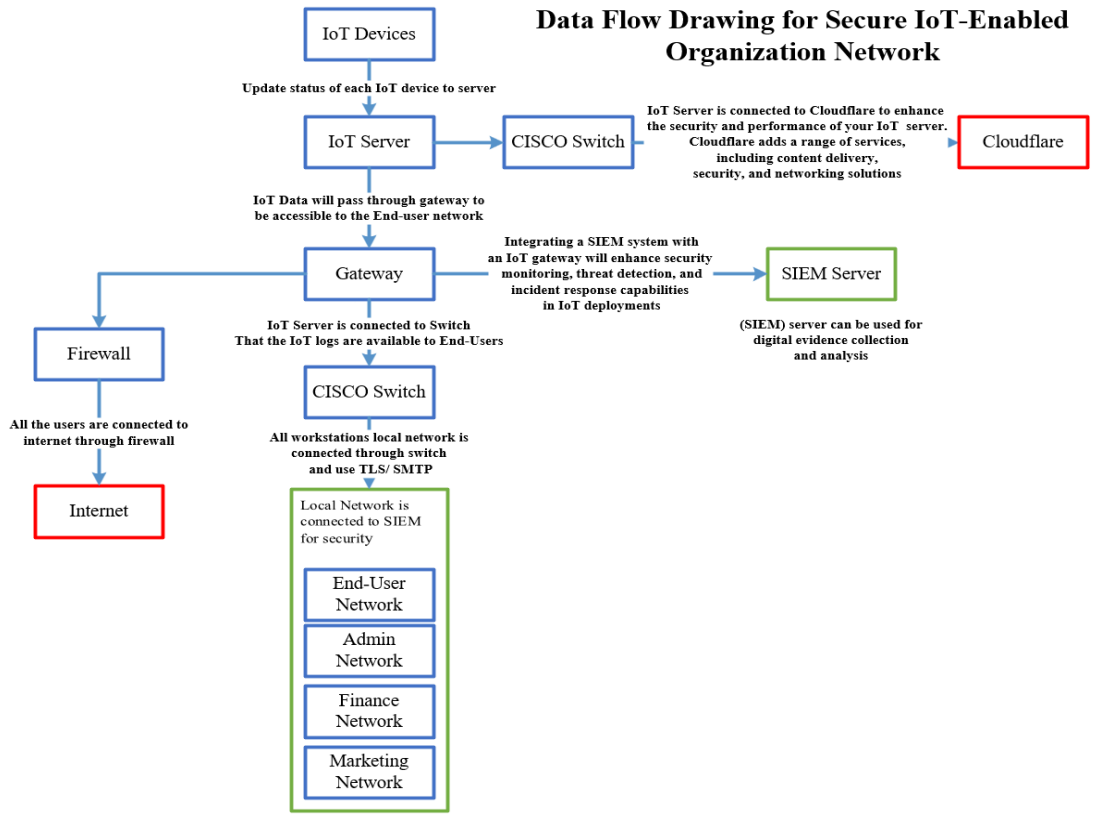

Figure 85: IoT-Enabled Organisation Network Data Flow

Figure 85 illustrates the data flow diagram specific to the secure interaction between IoT devices and their IoT-enabled organisational network, including the IoT server, critical security components such as the Cisco switching device, Cloudflare, the gateway, the SIEM server, and the firewall. It clearly shows how data flows securely from IoT devices to end-users, emphasising the multilayered measures taken to safeguard the network. This is complemented by a comprehensive visualisation that enhances understanding of the architecture and security measures critical to resilient IoT-enabled organisational environments.

The Internet of Things (IoT) has rapidly gained traction across various industries, introducing significant interconnection and automation. The open environment, however, poses significant challenges for individuals in terms of security and forensic readiness. IoT networks generate vast amounts of data, contain heterogeneous devices, and generally operate in highly dynamic environments; therefore, they are most likely to face a high risk of cyberattacks and system vulnerabilities. In such situations, IoT forensic readiness is essential, as it helps organisations establish cybersecurity hygiene to proactively prepare for security incidents, collect and preserve digital evidence, and comply with legal and regulatory requirements. (Atlam et al., 2020). This research focuses on developing an IoT Digital Forensic Readiness Model that encapsulates organisational policies, IoT-related readiness procedures, and dominant ones such as ISO/IEC 27043. The model aims to enhance organisational resilience and improve incident response capability, addressing specific challenges faced in IoT security environments, while providing robust security measures to safeguard data and systems in a connected world.

- IoT Devices

The IoT devices serve as the backbone of currently connected networks, acting as primary building blocks for the continuous interaction between the connected device and the IoT server, thereby enabling real-time updates. They comprise the connected world- industrial automation, healthcare systems, smart homes, and transportation networks. They enable monitoring of various activities and conditions, facilitating the seamless flow of data and supporting optimal operation and informed decision-

making. Each device is designed to send status updates or perform dedicated tasks while reporting anomalies, thus keeping the system alert and responsive to changes (Stoyanova et al., 2020).

Real-time information sharing is a crucial feature of IoT applications, especially in those that require quick decisions. For example, IoT-enabled devices, such as wearable sensors, monitor vital signs and alert medical practitioners to irregularities in health conditions, ultimately saving lives. They are similar to industrial settings, where sensors detect oddities in machine performance, predicting failures and reducing downtime and cost. However, IoT devices are not free from challenges. They follow many protocols, have low computational capabilities, and, most of the time, insecure communication channels. This makes the devices susceptible to cyber threats. While collecting and transferring data, IoT devices must be protected from unauthorised access and tampering to ensure the integrity and confidentiality of the network. Furthermore, since the devices are continuously connected to the IoT server, they require robust monitoring mechanisms to detect and correct anomalies. IoT devices can thus play a crucial role in enabling connectivity, driving innovation, and enhancing reactivity and responsiveness. The real-time continuous monitoring, updating, and alarming features of these devices will ensure that IoT-enabled networks function effectively within the broader context of automation, security, and resilience. However, comprehensive security strategies will also be required to address some of their vulnerabilities regarding trust in connected ecosystems (Alahi et al., 2023).

- IoT Server

An IoT server will act as a centralised core hub in an organisation's network, enhanced with IoT capabilities, and serve as the main point of data aggregation, processing, and distribution. This server will receive real-time updates from IoT devices, analyse incoming data, and make it available to different network components so they can make informed decisions and operate more effectively. Integrity and security are paramount because the IoT server handles sensitive information and supports critical network processes (Allioui and Mourdi, 2023). The IoT server has a unique attribute:

its integration with a Cisco switch, which together ensures a very high level of security and operational performance. The switch features highly efficient data flow management, minimising timing issues and maximising its ability to handle high traffic volumes. This is particularly critical in the IoT environment, where data influx is pervasive and heterogeneous. In addition to the aforementioned, Cloudflare's connectivity would increase the safety and optimisation of the IoT server.

Cloudflare can provide robust security against cyber threats, such as Distributed Denial-of-Service (DDoS) attacks, and deliver content securely to end users. Its advanced networking approaches, therefore, ensure reliability, minimise vulnerabilities, and impose overall resilience on the IoT server. The role of the IoT server is to do more than process data; It also safeguards the integrity and availability of the IoT network. By integrating advanced networking and security tools, the server enables IoT devices to operate securely and efficiently. It protects the network from potential threats in a standard manner, at the core of the IoT ecosystem. The IoT server reflects the balance of 'both performance and security' that marks a successful IoT-enabled operation (Gugueoth, Safavat, and Shetty, 2023).

- Cisco Switch

Cisco Switch enhances its application to IoT networks, with a focus on security and performance. It works between the IoT server and other key components in Cloudflare, ensuring the necessary detectability and sealing the network from potential vulnerabilities. This is useful in environments with high data traffic, as it efficiently processes large volumes of data. The primary function of this switch is to maintain the server's security in the IoT environment. It serves as a proper mediator, directing data flow packets while filtering unauthorised traffic to reach the server. This not only increases the server's operational reliability but also reduces the likelihood of cyberattacks targeting sensitive information (Bröring et al., 2020).

Security is only one half of the equation regarding the Cisco switch, which also helps further enhance network performance. This is achieved by prioritising certain data packets based on their importance and destination to minimise latency, while ensuring that critical information is transmitted without delay. The importance of

such capabilities in IoT networks cannot be overstated, as these networks require real-time data transfer to remain responsive and reliable. However, the switch also serves a more crucial purpose in the context of the connection between the IoT server and Cloudflare. This integration enables the delivery of superior, optimised, and secure networking solutions to counter threats while enhancing the server's capability to manage various data sources. In other words, the Cisco switch is one of the cornerstones of the IoT infrastructure, connecting all points to ensure safe, efficient, and reliable data communication across the network (Gooley et al., 2020).

- Cloudflare

The architecture of an IoT-enabled organisational network relies on Cloudflare's capabilities to enhance security, reliability, and performance. A holistic security networking solution that protects the IoT network from many cyber threats, while content delivery optimisation ensures seamless communication among components (Singh, Buyya and Kim, 2024). Cloudflare plays a vital role in an IoT network as a firewall. It protects against the risks of distributed denial-of-service (DDoS) attacks, unauthorised access, and data breaches. This fortifies the network's defences by authenticating and blocking all malicious actions and analysing the incoming traffic, thus protecting the integrity and availability of IoT data (Iqbal et al, 2024).

Besides security, much of what Cloudflare does is increase network performance. The content delivery network optimises data transmission by caching and delivering content from servers closest to end users, reducing latency and providing an incredibly user-friendly experience for IoT applications that require real-time responsiveness. Load balancing and traffic optimisation are among the advanced networking solutions Cloudflare provides. These would distribute data evenly across servers to do away with bottlenecks, guaranteeing efficient use of the resources involved (Wang et al., 2015). Cloudflare enables these advanced features by integrating the IoT server with the rest of the network components, thereby guaranteeing the robustness, scalability, and adaptability of IoT infrastructures against future demands. Cloudflare indeed plays a crucial role in securing and optimising IoT-enabled networks. As a cornerstone of modern IoT, organisations can

operate within an interconnected environment that requires both security and efficiency. As such, highly accessible and efficient networking helps address security threats and improve data delivery.

- Gateway

IoT gateways often serve as the interface, bridging the gap between IoT data and the end-user network. Apart from enhancing security for organisation-wide data traffic, it serves as a scanning entry point for all data from the IoT ecosystem into the more extensive organisational networks (Vig, 2023). It provides a pipeline to connect IoT devices and end-user facilities while ensuring data integrity during transfer. Security information and event management (SIEM) integration with the gateway is one of the most crucial features. This improves network security by enabling the SIEM to monitor, detect threats, and respond to incidents. The SIEM processes most of the data on the site as it traverses the gateway and thus notices signs of potential security threats, mainly due to unusual traffic or unauthorised access attempts (Palo Alto Networks, 2023).

Therefore, real-time intervention is possible, and the risk of a breach is minimised. Another primary function of the gateway is optimised data flow: it filters data packets, aggregates them, and prioritises rapid delivery to the intended recipients. This is particularly important in IoT environments, where vast amounts of data are generated and transmitted. It also ensures that security protocols and policies are followed, serving as a checkpoint in enforcing encryption standards and authentication requirements. Importantly, secure and efficient data transition handling is critical to ensuring the reliability and resilience of IoT-enabled organisational networks. Thus, we conclude that the gateway is not just a bridge but also a vital control point through which IoT data is pumped, with restricted access at all levels to its ultimate end destination.

- SIEM Server

The SIEM server serves as a cornerstone of the IoT network's security architecture. The SIEM server enhances monitoring, detection, and response actions to security threats by gathering, analysing, and managing electronic evidence. Crucial for maintaining

the confidentiality, integrity, and availability of data in the IoT ecosystem. Continuous data collection from IoT devices, gateways, firewalls, and other components is then hosted by the SIEM server. This data acquisition collates activities into a single direction, providing visualisation for networked users so that different patterns can be identified and anomalies rooted out, which might lead to potential threats (Umar, 2023). Most of the time, the SIEM system can also incorporate advanced analytics and machine learning algorithms to enhance its detection capabilities, identifying real-time locations where vulnerabilities and suspicious activities can be recognised using the AI infrastructure.

In addition to monitoring and detecting events, the SIEM server can also respond quickly to incidents. When a threat is identified, the system generates alerts and provides detailed insights into its nature. This empowers security teams to act promptly and be well-informed, minimising the impact of the threat. The SIEM server is also an essential component of regulatory compliance. That is, by maintaining very detailed logs of all network activity and providing a competent reporting engine, the organisation can meet its legal and industry-specific security requirements. The SIEM server is an indispensable tool that helps to improve the security posture of networks enabled by IoT-based devices. This means that real-time insights, automated threat detection, and incident response processes promise an entire network that is robust against the ever-changing topology of cyber threats (Mallick and Nath, 2024).

- Firewall

There are terms that some individuals have never known; a firewall, serving as the first line of defence for the IoT-enabled organisational network against external attacks, plays the role of the gatekeeper for incoming and outgoing data packets while enforcing security measures such that only recognised modes of traffic may enter (Academy Fynd, 2023). The role is crucial to safeguarding the network's integrity and security against vulnerabilities and cyber threats. One type of firewall monitors and controls traffic and network flows within an organisation’s networks in accordance with set security rules. It would analyse the content and origin of data packets and determine whether the activity is potentially harmful, unauthorised access attempts,

malware, or phishing. This ensures that sensitive data is highly protected within the network, making it inaccessible to malicious actors. Given that devices continue to communicate and transmit data in an IoT-enabled environment, the firewall plays a crucial role. It protects vast amounts of data being exchanged and guards against interception or tampering by malicious actors. Also, this would ensure that organisational security policies and regulations are implemented through encryption standards and user authentication protocols.

Yet, a firewall is the first line of defence for IoT-enabled organisational networks against external attacks. It acts as a gatekeeper, analysing incoming and outgoing data packets as waves travel into and out of the network, while enforcing security measures that allow authorised traffic to access the network. The role is vital to preserving and protecting the network shield against potential vulnerabilities and cyberattacks. Among the more significant tasks, a firewall involves monitoring and controlling network traffic using defined security rules. The analysis of the content and source data packets would, therefore, identify and block potential threats like system or unauthorised access (Oluwasanmi Richard Arogundade, 2023). So it becomes accepted that sensitive information within the network will not be accessed or corrupted by malicious characters.

In environments where an IoT device constantly communicates and sends information, the firewall is one of its most essential functions. It establishes a boundary around data, enabling continuity at the fuzzy edges of digital media being exchanged. In addition, the firewall ensures that an organisation's security policy adheres to encryption standards and user authentication protocols. A firewall would be the first line of defence for IoT-trained organisational networks against outside attacks. It would act as a gatekeeper for incoming and outgoing data packets, enforcing rules governing traffic to and from the networks and establishing a security measure that permits recognised modes of traffic access. This is crucial in preserving and protecting the network from potential vulnerabilities and cyberattacks. Among the most critical functions of a firewall is monitoring and controlling network traffic in accordance with previously defined security rules. It would analyse the content and

origin of data packets and determine whether the activity is potentially harmful, such as unauthorised access attempts, malware, or phishing. This ensures that sensitive data is very well protected.

Besides strengthening security, the firewall boosts the performance of the network by sifting through irrelevant or malicious traffic to reduce congestion while ensuring that resources get allocated to legitimate activities; it integrates well with other security tools, such as SIEM systems, to further strengthen it and thus offers a complete approach toward threat detection and response. Of course, the firewall is part of the extensive security infrastructure that protects an IoT network. Acting as a strong barrier against external threats, it securely transmits data within this boundary, thereby protecting the organisation's assets and enabling the safe operation of IoT devices (Lu, 2023).

- Internet

The internet is the backbone that connects users, devices, and systems worldwide, facilitating communication and data sharing. In an organised network that encapsulates IoT connectivity, the internet will provide a channel for external resources, services, and users to access and engage with the IoT system. It enables users to remotely monitor and control IoT devices, access the data they generate, and perform various network management tasks. However, the internet connects users or IoT devices on one side to other external devices on the other, posing a security risk. Cyberattacks such as data breaches, unauthorised access, and Denial-of-service attacks can exploit opportunities in the communication path between IoT systems and the outside world (Sadhu, Yanambaka, and Abdelgawad, 2022). All such risks are managed effectively through a firewall. It monitors and controls all perimeter traffic, both to and from the network, ensuring that only legitimate and authorised data can flow in or out. It filters and inspects internet traffic to block potentially damaging packets and malicious activities. Furthermore, the internet is, without a doubt, the primary platform for most cloud-based services, a characteristic that IoT networks often rely on for storage, computation, and processing power. Cloudflare, integrated into various IoT architectures, optimises internet traffic and enhances security by

shielding the network from external threats. Organisations utilising the internet can extend their IoT network beyond their physical infrastructure, thereby providing remote access to devices, data, and services via a secure, efficient communication channel. The internet thus becomes a vital infrastructure for the potential interrelatedness of all IoT systems and, with it, many additional security-related solutions, ensuring that audiovisual, visual, and structural interactions remain secure and reliable (Williams and Douglass, 2022).

- Cisco Switch (Local Network)

This switch is crucial for connecting the IoT server to the organisation's internal network. It is the point of connectivity for all data flowing from IoT devices across the network, ensuring that information is secure and well managed. It also helps organise and direct traffic based on network needs to improve performance and security.

The local Cisco switch is responsible for distributing IoT logs to end users. These logs contain essential data generated by IoT devices and the IoT server, which can be used to monitor device performance, analyse trends, or detect anomalies. Routing these logs through the network ensures that authorised users within the organisation can access the information in a timely and secure manner. The device enforces several security-related communication protocols, including Transport Layer Security (TLS) and Simple Mail Transfer Protocol (SMTP) (Abiodun et al., 2021). TLS encrypts all data transmitted over the open network; hence, even if malicious users can intercept the traffic, they cannot extract any valuable information from it. SMTP is also the most common protocol for email, enabling the transmission of alerts and notifications related to IoT operations and ensuring the confidentiality and reliability of messages. The Cisco switch is integrated into the SIEM (Security Information and Event Management) system, providing broader network security coverage. With the switch connected to the SIEM system, all possible threats to the system, such as suspicious activity and unauthorised access attempts, can be detected and handled simultaneously, thereby securing the network as a whole. This configuration will also enable continuous monitoring of all IoT devices and the entire network, providing a secure, stable, and tamper-proof environment for information sharing.

- Local Network

The local internal network is part of the organisation, linking systems and devices such as end-user workstations, administrative networks, the finance network, and other departmental resources. It makes a significant contribution to communication, collaboration, and the effective use of resources among different users within the organisation. The local network provides all of the above by giving a safe and effective environment for data exchange. IoT data and logs are kept understandable, available, and usable in real time, thus accessible to internal stakeholders. Usually, specific sub-networks are created within a local area network based on organisational functions or purposes. For instance, an End-User Network provides access to IoT data and services for employees who generally work. At the same time, the Admin Network provides more specialised access for administrators to manage and maintain the IoT infrastructure (Li et al., 2022). There are also Finance and Marketing Networks that provide services to the relevant departments, supplying the necessary data and resources to enable them to perform their roles effectively. In general, the sub-networks mentioned above are crucial for providing separation and access control to systems, ensuring that sensitive information is available only to authorised users.

According to these strict security protocols, each sub-network has maintained data integrity while keeping the entire system secure against potential breaches. This enables the SIEM system to reside on the local network, allowing round-the-clock monitoring of network activity. The analysis of such data would, among other things, include input from IoT devices, switches, security events and incidents, and network appliances. It will then identify this as anomalous behaviour or a threat and raise alarms in real time to security staff for immediate response, thereby mitigating incidents and reducing the likelihood of breaches. While security ensures that communication utilises established channels within the local network for operational continuity, it also ensures that internal communication channels are fast, reliable, and resilient. By segmenting organisational functions into separate sub-networks, the system can handle varying traffic loads and maintain optimal performance even during peak usage. Thus, the local network is significant for the organisation because

it serves as a link between the daily operations and security within an IoT-enabled enterprise (Mhaskar, Alabbad and Khedri, 2021).

7.9.2 Data Flow and Security Architecture of an IoT-Enabled Organisational Network

Various communication processes and security protocols enable the effective deployment of internet-connected devices (IoT networks) within an organisation. In this architecture, IoT devices can transmit real-time data to a proprietary IoT server for analysis and control. To secure the data, several layers, including firewalls, access management, control, and a prominent SIEM system, are integral to this network. The network is subdivided into several subnets that cater to a range of organisational needs, including administration, finance, marketing, and end-user operations, thereby enhancing performance and security. Additionally, network traffic is managed by a Cisco switch and routed through Cloudflare to provide enhanced security and performance. There are three main IT security objectives relevant to the design: confidentiality, availability, and integrity of organisational information. This architecture also emphasises continuous supervision, frequent data recording, and reporting of secure email flows, such as SMTP/TLS and S/MIME. Many of the components in this diagram are familiar; it broadly illustrates the classical IoT architecture, featuring multiple layers of data flow and network management, all of which are ready for digital forensics. However, the focus is on secure communication throughout the organisational network.

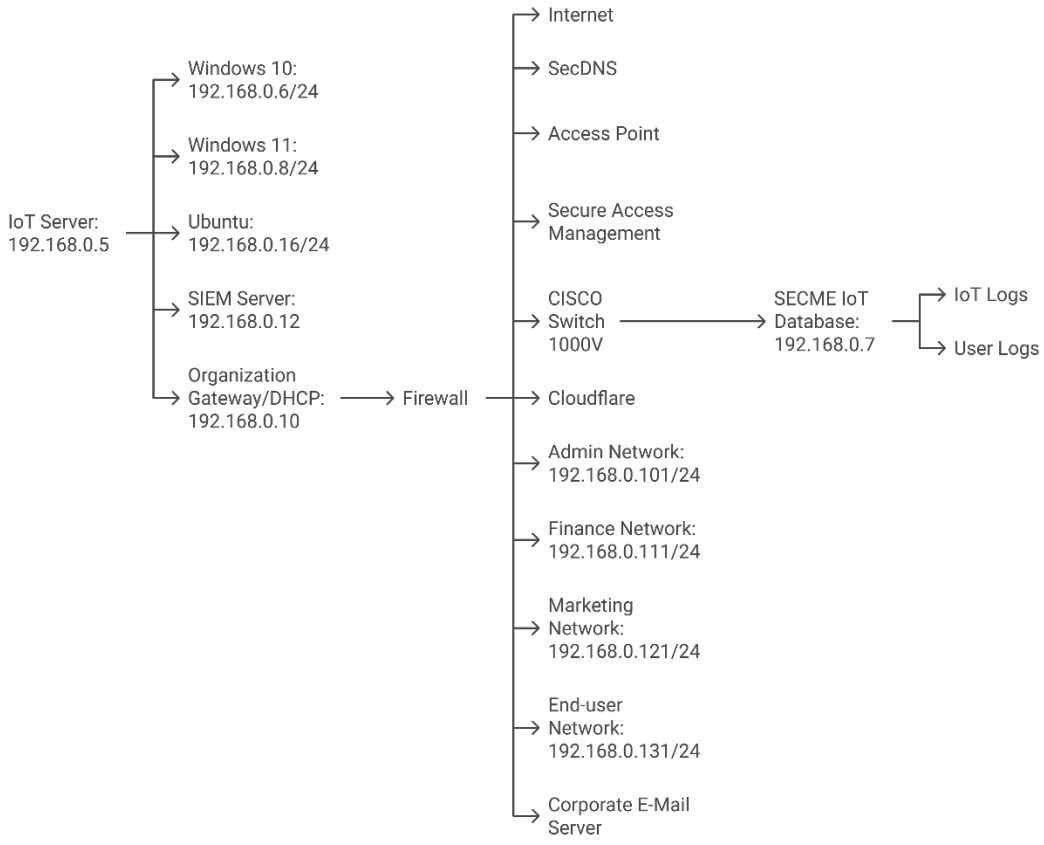

Figure 86: Digital Forensic Readiness in IoT-Enabled Organisations Network Structure

Figure 86 illustrates the network architecture and data flow in an organisation that uses Internet of Things (IoT) devices. Then the various components and their interactions are described further down:

- IoT Devices Subnet

This area network serves all the organisation's IoT devices. This area comprises the physical devices that serve as nodes for collecting and transmitting real-time data. These devices run Windows 10 through Windows 11 and also support Ubuntu. They're tailored to the organisation's needs. The general private address space comprises addresses such as 192.168.0.6/24 and 192.168.0.16/24 on an IoT subnet. These IP addresses will enable an IoT server to exchange data flows with connected IoT devices. Such devices are equipped with numerous sensors and software that detect physical conditions or activities and report the resulting data to the IoT server. Examples of IoT devices used in an organisation include smart thermostats, security

cameras, environmental monitoring sensors, and other innovative systems embedded within the organisation. These devices will be equipped to perform tasks such as temperature, humidity, and motion tracking; some will depend on the use case within the organisation, including monitoring network status. These systems will continuously collect and transmit data to the IoT central server, ensuring real-time visibility into an organisation's operations and equipment. IoT devices are essential for operational and production efficiency gains, as they provide the most timely information to improve decision-making, automate processes, and optimise the use of people and materials. For example, sensors installed on machinery in a factory environment can help predict equipment failures, thereby reducing downtime and maintenance costs. On the other hand, environmental monitoring devices can alert the organisation to critical conditions, such as temperature changes or water leakage, that would otherwise go unnoticed and cause enormous financial damage or operational disruption (Baek, Kanampiu, and Kim, 2021).

Security is the foremost concern for IoT devices, as they continuously transmit data and are directly connected to the network. These devices run on the following operating systems: Windows 10, Windows 11, and Ubuntu. These are essential security systems; they include embedded security features such as firewalls and encryption tools, as well as access control mechanisms that protect the device from unauthorised access or cyberattacks. Hackers can still access such IoT devices despite these protections, as they are always connected to the network. Thus, continuous monitoring, regular firmware updates, and integration with security systems, such as a SIEM, are crucial steps for identifying and mitigating potential threats. The latest component of the overall architecture is an IoT Devices Subnet within the organisation's network architecture. Provide real-time data collection and continuous monitoring; IoT devices will improve operational efficiency, safety, and decision-making. However, being integrated into the network requires robust security measures to address vulnerabilities and protect organisational assets (Sarwar et al., 2023).

- SIEM Server

The SIEM Server, or Security Information and Event Management server, is a key component of the network infrastructure and serves as the primary focus for improving the organisation's security posture. It is associated with a Cisco Switch 1000V and assigned the address 192.168.0.12, to which the SIEM Server is connected. As is typical, a central focus of SIEM server capabilities is the detection and response to real-time security incidents. Such unusual behaviour may include unauthorised access attempts, abnormal data flows, or unauthorised activities, as well as the use of sophisticated analytical tools and algorithms that the SIEM system can detect. Therefore, security control administrators or network managers can act on potential threats at the earliest possible time, before they mature into full-blown security incidents. An example scenario would involve triggering an alert to the security team when systems detect abnormal behaviour in the amount of data transmitted outside the systems; this allows them to investigate the cause and prevent data exfiltration. The association between the SIEM server and the Cisco 1000V switch is critical to ensuring optimal network management. The switch, as a high-performance device, handles data traffic across different network segments. It ensures that security data collected by the SIEM server is effectively routed across the network for smooth, low-latency communication (López Velásquez et al., 2023).

Monitoring traffic patterns using the Cisco Switch 1000V can help the SIEM server gain insights into typical network behaviour, such as which devices generate the most traffic or which communication paths are most vulnerable to attack. Another factor in compliance and forensic investigations is the SIEM server's ability to perform deep log analysis. With highly detailed logs of security events, an SIEM system enables organisations to maintain an audit trail for reference during security audits or after incident investigations. It also helps identify vulnerabilities that could be exploited by attackers and corrected before incidents occur. In addition to threat detection and compliance, the SIEM can be supplemented by other security tools, such as IDS or IPS, to strengthen the security posture. This means that a more comprehensive cybersecurity approach will replace the existing multiple systems that protect the network against various threats. The SIEM server serves as a central component in securing a network by identifying, analysing, and responding to security events as

they occur; it also provides crucial visibility into network health and helps the organisation efficiently identify and neutralise potential security threats to infrastructure. Furthermore, the use of the Cisco Switch 1000V enhances the robustness of the SIEM server's data flow, thereby improving network storage and management (Sun, Ansari, and Wang, 2016).

- Organisation Gateway/DHCP

The organisation has recognised the address 192.168.0.10 as the gateway/DHCP address. It performs vital functions, including controlling traffic and ensuring optimal network configuration. The gateway links are visible as connected to the Firewall and the Cisco Switch 1000V, and they also support DHCP. It is also becoming a hub for all flows related to entering and exiting the previous local area network. A primary role is to assign IP addresses to newly connected devices on the local network, thereby ensuring communication between these devices and network resources. Additionally, it allows hosts to independently assign IP addresses to the network, enabling a device to connect to the host network without requiring administrator intervention. The Firewall is responsible for filtering and protecting all datagram traffic at the gateway level. A firewall operates in the DMZ, regulating traffic between internal and external networks. At the same time, it regulates data within the network, enforcing security policies to prevent unauthorised access to information. Traffic forwarding is performed based on the firewall’s decision to inspect it, allowing authentic and authorised requests into the network while discouraging potential threats.

The gateway also connects to the Cisco Switch 1000V, which intelligently and efficiently manages traffic, routing it across various network segments to maintain high performance and low latency. This switch, in addition to ensuring a secure and optimised data flow, also enables the effective utilisation of an organisation's resources by leveraging available network resources. Essentially, this Organisation Gateway/DHCP is the primary point of network access and administration. This device was designed to facilitate the connection of new devices to the network and relies primarily on its capabilities, such as a firewall, to protect the organisation from

external threats and ensure device security. Its role includes traffic management and dynamic IP address allocation, making it essential to a secure and efficient network.

- Firewall

Firewalls are crucial to an organisation's security, as they control the flow of external traffic and determine which traffic is permitted to access the internal network. This establishes a perimeter-based filter between external and internal networks, monitoring incoming and outgoing traffic in accordance with predefined policies. This ensures that only legitimate traffic can enter the internal network and that unauthorised traffic, such as hacking attempts and malware infections, cannot. It connects directly to both the Organisation Gateway/DHCP and the internet, enabling it to monitor all network traffic and security protocols, ensuring the entire system remains intact. Only legitimate and permitted traffic can flow through the organisation between the internal networks and the outside world. The firewall thereby creates an organised, secure digital environment (Alsaqour, Motmi and Abdelhaq, 2021).

- Internet

An internet connection serves as the gateway to external communication and data exchange, providing direct access to a vast array of online resources, services, and communication tools. Nevertheless, there is increased connectivity, as anyone can access the organisation, given that the internet is open to malicious actors. To prevent these risks, the firewall plays a crucial role in controlling Internet traffic. Moreover, the Private Communication Technology is adopted to enable secure email communications, with S/MIME over SMTP/TLS as the client protocol. This combined feature ensures the confidentiality and integrity of email messages containing highly private information, preventing interception or modification in transit on the World Wide Web.

- LAN (Local Area Network)

The Local Area Network (LAN) is a component of the organisational network that provides connectivity within a specific geographical region, such as a building or campus. It transfers data between computers, IoT devices, and servers, and supports

resource sharing. LAN is connected to Cloudflare, a service that enhances security and improves link performance. Cloudflare also offers additional services, including DDoS mitigation, content delivery, and threat protection, which enhance LAN security against cyber threats and increase data processing rates. Another part of the LAN is the Access Point (AP), which enables devices connected to the LAN to connect wirelessly, including laptops, smartphones, and IoT devices. These would allow these devices to be securely connected to the network and to communicate with other devices, both wired and wireless, within the LAN. Furthermore, SecDNS, the secure Domain Name System, is implemented on the LAN to enhance security. SecDNS ensures that DNS queries are handled efficiently, preventing DNS spoofing and other threats that compromise the network's integrity. Taken together, these protective features ensure safe, reliable, and fast network access while safeguarding the organisation against vulnerabilities, resulting in improved LAN performance (BAJRAMI, IDRIZI and RUSHITI, 2024).

- Secure Access Management

Secure access management encompasses all essential aspects of secure data access for individual end users, including their permissions. It speaks to the authentication of the one-time and convenient conditions under which each method will be used to gain access to information. Such a security component should be stringent enough to limit access to sensitive data and even services to authorised users. SAM would perform gatekeeping to provide user access to resources, rather than to individual premises or users, and to efficiently and effectively control access across all locations and the entire geography within each site. Secure Access Control establishes a robust connection between IoT devices and Cisco 1000V switches for network-wide user access management. Centralised access control within SAM maintains system integrity and significantly reduces the risk of major threats by preventing unauthorised access.

- IoT Server

The IoT Server is centralised to capture and process all data generated by IoT devices connected to a network. The data exchange between IoT devices and other network components is secured by the IoT Server, which is connected to the Secure Access

Management system. Collecting, storing, and processing real-time data generated by IoT devices, while overseeing their interactions with the broader network, are key functions of the IoT Server. The server encrypts communication between IoT devices, ensuring it is secure and free from threats. Hence, the safe management of data flow ensures network integrity in interactions and mitigates the risk of data breaches or data loss. Additionally, it will be connected to the network infrastructure to send and receive data from other resources within the organisational network (Elgazzar et al., 2022).

- Cisco Switch 1000V

The Cisco Switch 1000V is a fundamental component of a network, enabling reliable connection and data transmission between devices. Secure Access Management is connected to other elements of the system, including the SIEM Server, Organisation Gateway/DHCP, and IoT Logs/Users Logs. The switch enhances data flow and traffic management, ensuring data packets flow freely and safely within the network. This means that the Cisco Switch 1000V can handle both high-bandwidth and high-security demands, optimising the network for proper device launch and rights. This is useful for controlling network loads, distinguishing between essential network traffic and less important traffic, and reducing the occurrence of jams, which in turn means the system runs smoothly for users (Janwar, 2021).

- IoT Logs/Users Logs

The IoT Logs and User Logs are, therefore, foundational to security and compliance in an IoT network. These logs are located at IP address 192.168.7.0 and contain system information and activity logs for IoT devices and other users. In IoT, Logs collect data on the states of IoT devices, data consumption, and data exchange. For users, logs collect data including user entries, login details, and system interactions. These logs are beneficial for analysis and, in particular, for monitoring to detect abnormalities or security issues. These are also useful for collecting evidence in digital forensics investigations. These logs are stored at the organisational level and analysed to ensure forensic readiness and to take proactive steps to prevent unauthorised access or malicious activity (Saxena, 2021).

- Corporate E-Mail Server

It serves as an integrated, end-to-end Corporate Email Server for secure email communications within the company, ensuring that messages exchanged between users are confidential and protected from unauthorised interception through encryption protocols, such as Secure/Multipurpose Internet Mail Extensions (S/MIME) over SMTP/TLS. In this way, the Corporate E-Mail Server protects sensitive information transmitted through email. It inhibits email-related security attacks, including phishing, spoofing, and eavesdropping, while also providing seamless integration with the organisation's network infrastructure, which underpins reliable, efficient, and secure email delivery and receipt for all users. On the other hand, being a communication server, the Corporate E-Mail Server interfaces seamlessly with the network infrastructure and provides different benefits and features that enhance communication security (Altulaihan et al., 2023).

- Sub-Networks

The organisational network is divided into several sub-networks to provide efficient resource provision, security, and optimal performance. These sub-networks are established to correspond to a particular department or functional unit. This segmentation facilitates efficient control and administration by dividing networks into functional resource-management units (Redondi, Arcia-Moret,and Manzoni, 2019). The Admin Network (IP range: 192.168.0.101-192.168.0.110, /24) is used for administrative purposes and all types of organisational management. By isolating this network from other sub-networks, administrative resources and personnel can access other isolated network resources, thereby minimising external access to administrative resources while keeping vital operations secure and running without interruption. The Admin Network is typically more secure, with a firewall and strict controls over systems, applications, and information.

The Finance Network (IP range: 192.168.0.111-192.168.0.120,/24) was specifically designed for the finance department to facilitate connectivity to financial systems, records, databases, and related services. This network can be easily configured to implement measures to protect the financial information it contains, such as

encryption, firewalls, and access controls. The organisation's financial operations are contained, reducing management's vulnerability to external attackers or internal fraudsters regarding sensitive financial data. The Marketing Network (IP range: 192.168.0.121-192.168.0.140,/24) is dedicated to marketing, providing access to tools, customers, and other systems that support marketing activities. It helps the marketing team fulfil their responsibilities by preventing data pollution and unauthorised access to other departmental assets (Pascucci, Savelli, and Gistri, 2023).

The End-user Network (IP range: 192.168.0.141-192.168.0.160, /24) is assigned to general users and provides internet access, intranet services, and employee devices. This sub-network can be configured to consist solely of end users, facilitating traffic control and securing employees' access to other sub-networks that house the organisation's essential systems. Dividing the network into these sub-networks is beneficial for security reasons in the event of a breach. It is easier to manage resources for each department and ensure that each department operates under the best security measures within that network, in their own best interests and operational requirements (Barricelli et al., 2019).

7.9.3 Enhancing Forensic Readiness in IoT Ecosystems

The growing use of IoT technologies means organisations are under pressure to protect assets and data against emerging cyber threats. Of course, IoT has many benefits, but it also poses additional risks and is a weak point for hackers. To counter these vulnerabilities, it is necessary to develop and refine forensic investigation procedures that effectively address the challenges posed by IoT. Criminal investigations involving computers and other digital technologies have introduced new psychological, temporal, and epistemological challenges for managing and analysing digital evidence. In this regard, while organisations have adopted several measures and controls to enhance security, they remain vulnerable to internal and external security risks. It is crucial to develop specific rules to manage resources and direct cybersecurity activities at present. This discussion focuses on two key areas: comparing several DFR models and applying DFR in IoT contexts.

7.9.4 Analysis of DFR Models

In a more specific context, digital forensic readiness refers to how an organisation should equip and mobilise to gather and process digital evidence accurately and efficiently. The main processes of the IoT DFR Model include organisational procedures for establishing an IoT system, preparing an IoT system architecture, and ensuring compliance with ISO/IEC 27043. These points emphasise the importance of paying attention to data and incident checks, as well as implementing appropriate risk-prevention strategies for IoT systems. The IoT is experiencing a higher rate of cyber threats that must be mitigated or eliminated by DFR to establish efficient responses to cyber incidents (Atta and Talamo, 2020). As will be shown in the systematisation of the pertinent academic and practitioner literature, existing DFR models and frameworks address some aspects of forensic readiness but overlook others, including ISO standardisation, readiness processes, and forensic practice. These shortcomings are well captured in the proposed IoT DFR model, which focuses on organisational complexities, readiness mechanisms and compliance. ISO/IEC 27043: Incident Investigation Procedure Essential Standards, as enshrined in the 2015 guideline, are considered general standards applicable to IoT systems. Integrating DFR processes into digital investigative workflows is essential for achieving optimal results from digital evidence while minimising the impact of forensic investigations on business operations.

7.9.5 Analysis of Achieving DFR in IoT-Based Environments

DFR is a critical performance goal in IoT settings, and it requires employing several strategies to capture and process historical and current data. IoT sensor monitoring, which involves ZigBee-based systems, is a good example of such techniques, utilising temperature, humidity, and light sensors (Yun and Won, 2012). Such sensors transmit information to central nodes without physical cables, and environmental factors can be valuable for forensics. Furthermore, IoT devices communicate via packets over the network, and packet analysis can be used to track activities and interactions in the IoT domain. However, routers, Wi-Fi modules, and microcontrollers may be viewed as merely components that continuously collect data and identify potential attack precursors. Subsequently, assessing and monitoring IoT network protocols and services enables investigators to understand how different types of networks, such as

Wireless Sensor Networks (WSNs) and Body Sensor Networks (BSNs), operate and to identify potential sources of digital forensic evidence. IDS plays a crucial role in IoT environments by filtering various types of intrusions and promptly notifying administrators. Other added layers include mechanisms for detecting false alarms, which, in turn, lead to considerable improvements in incident detection, enabling organised equipment to respond to any cyber incident (Jahangeer et al., 2023).

Processing time in the DFR model refers to the time required for a developed system to perform optimally in forensic exercises. The factors that affect its performance depend on the length and the relative difficulty of the inputs fed to algorithms and processes. Although the CPU's time is not quantified, the Time Complexity provides information about how the system behaves when the breach occurs. For example, the multiplicity of operations in forensic processes may lead to temporal variability. For example, the time between an event trigger initiating an event and the start of a forensic investigation provides valuable insight into the efficiency of DFR systems. Every device and system in the proposed model must be capable of transmitting event data with criticality levels, critical, medium and low, for quick investigation.

Prior articles have compared the IoT DFR with different forensic readiness models. These include planning, Identification of scenarios, Storage of Digital evidence, Pre-incident analysis, and Forensic reporting, which together constitute Cloud Forensic Readiness as a Service (CFRaaS). However, many works do not consider the functional requirements manifested in usable combat tools and applications, focusing instead on general abstractions of an incident (Kebande and Venter, 2019). The IoT DFR model proposed in this paper outlines the necessary procedural steps, including the custody chain, information processes, and physical examinations. It also focuses on authentication and authorisation, including access control, which are key areas of security management for IoT devices. In addition, it adheres to the legal and regulatory requirements outlined in ISO/IEC 27043 standards and emphasises the need for specific forensic policies tailored to the organisation's needs. In contrast to other models, the proposed model recommends extensive training for organisational staff to ensure efficient investigations. (Kebande, Menza and Venter, 2018). The

proposed generic and customisable model can respond to meet needs and address the challenges that IoT systems pose to organisations. In turn, the proposed DFR model addresses existing gaps in readiness, compliance, and the standardisation of processes for digital evidence management in IoT-enabled organisations. In addition to enhancing readiness for forensic investigations, this approach minimises legitimate business impacts during investigations and integrates security into business processes as efficiently as possible.

7.10 Chapter Summary

While the evaluation results demonstrate the effectiveness of the proposed model, several real-world deployment challenges are identified. These include the complexity of managing heterogeneous IoT devices, integration with legacy systems, resource and performance overheads associated with continuous monitoring, and the need for organisational buy-in across multiple stakeholders. Legal and regulatory variations across jurisdictions may also influence the implementation of forensic readiness processes in practice. Addressing these challenges requires phased deployment strategies, policy alignment, and continuous organisational commitment to forensic readiness.

This chapter presents the final phase of the research by critically evaluating the proposed Digital Forensic Readiness (DFR) model against industry-recognised standards and performance benchmarks. The integration of DFR with International Standards such as ISO/IEC 27043 underscores the model's alignment with global best practices for information security management and incident response. This alignment reinforces the credibility, scalability, and relevance of the proposed model within real-world organisational settings. Various evaluation metrics were used to assess the system's technical performance, including detection accuracy, false-positive rates, response time, and overall system effectiveness. These metrics provided a structured approach to assessing the extent to which the DFR model enhances forensic readiness and supports timely incident detection and management.

The chapter also assessed the Automated Proactive Readiness Model (APRM), which concentrates on enhancing organisational resilience through predictive capabilities,

continuous monitoring, and automated response mechanisms. The performance analysis showed that the APRM notably boosts an organisation's ability to efficiently detect, contain, and investigate security incidents. The evaluation confirmed the effectiveness of the proposed DFR model in strengthening cybersecurity posture, aligning with international standards, and delivering measurable improvements in incident detection and response. The Automated Proactive Readiness Model is regarded as a promising method for improving forensic readiness via automated, scalable handling. Although the proposed APRM demonstrates superior detection capabilities, as indicated by its perfect recall score, reducing its false-positive rate remains crucial for operational efficiency. Furthermore, selecting suitable classification methods, such as deep learning approaches like MLP, can further improve the accuracy of forensic investigations; however, considerations related to computational overhead must be addressed to ensure real-time applicability. The insights from this chapter establish a foundation for future research and practical applications aimed at advancing digital forensic readiness in complex, evolving threat landscapes.

The evaluation of the implementation results synthesises the research outcomes concerning enabling File Auditing on Windows machines and Wazuh for FIM to identify suspicious file deletions while maintaining forensic records. These tools, when properly configured, offer extensive coverage and real-time detection of modifications or deletions to crucial documents, which is essential for security analysis. The research holds significant value in advancing network security and digital forensics by providing practical guidelines for integrating these tools into existing security systems. It emphasises the importance of prompt investigation into potential threats to safeguard data. Therefore, the study recommends organisations adopt File Auditing and Wazuh, along with training for IT and security personnel to read logs and review policies periodically. The study underscores the importance of such tools in cybersecurity and for DFIs, which should encourage further research into updated methods for monitoring and auditing tools that enable effective management of emerging security risks.

8.0 Conclusion and Future Work

8.1 Conclusion

This research addressed the growing need for Digital Forensic Readiness (DFR) within IoT-enabled organisational environments by developing, implementing, and evaluating a standards-aligned Digital Forensic Readiness Model grounded in ISO/IEC 27043. The increasing adoption of Internet of Things technologies across organisational infrastructures has significantly expanded the cyberattack surface, creating substantial challenges for evidence identification, preservation, investigation, and legal admissibility. Existing approaches primarily focused on cybersecurity detection mechanisms or post-incident forensic investigations, while limited attention was given to proactive forensic readiness capable of supporting real-time evidence generation and preservation within complex IoT ecosystems.

To address this gap, this study proposed a comprehensive DFR model integrating organisational governance, technical infrastructure, security monitoring, and forensic investigation processes into a unified readiness model. The model operationalised ISO/IEC 27043 readiness principles within an IoT-enabled organisational environment and demonstrated how forensic readiness can function as a continuous organisational capability rather than a reactive post-incident activity.

The proposed model was implemented using real-world security monitoring and forensic tools, including Wazuh and Splunk, within controlled organisational attack scenarios involving brute-force attacks, DDoS attacks, and other cyber threat activities. The implementation demonstrated the practical feasibility of integrating real-time monitoring, forensic evidence acquisition, secure log preservation, and chain-of-custody management into a unified forensic readiness workflow. The research further incorporated machine learning techniques to support cyberattack detection and forensic evidence prioritisation, thereby enhancing investigative efficiency and automation capabilities.

Experimental evaluation demonstrated that the proposed model improved organisational forensic readiness by reducing investigation time, enhancing evidence traceability, supporting automated evidence preservation, and strengthening incident

response capabilities. The results also highlighted the importance of integrating forensic readiness directly into organisational cybersecurity architectures to improve resilience against evolving cyber threats. Furthermore, the study confirmed the applicability of ISO/IEC 27043 as a foundational standard for operationalising digital forensic readiness within distributed IoT ecosystems.

Overall, the research contributes to addressing the increasing forensic challenges associated with modern IoT-enabled organisational infrastructures and demonstrates the practical value of combining forensic readiness, cybersecurity monitoring, machine learning, and standards-based governance into a unified model for proactive digital investigation support.

8.2 Contribution to Knowledge

This research significantly advances knowledge on Digital Forensic Readiness (DFR), especially for IoT-enabled organisations, by presenting and validating the Automated Proactive Readiness Model (APRM). The growing complexity of IoT environments introduces new challenges for digital forensic preparedness, including large data volumes, diverse device interactions, and changing security threats. This dissertation tackles these issues by proposing a scalable, automated forensic-readiness model designed for modern, interconnected infrastructures. The main contributions of this study are as follows:

1. Development of the Automated Proactive Readiness Model (APRM) for IoT Environments

This research presents APRM as a new, intelligent, and scalable model specifically created to enhance forensic readiness in IoT-enabled organisations. Unlike traditional DFR models, which rely heavily on static processes and manual efforts, APRM integrates real-time monitoring, automated evidence collection, and machine-learning-based anomaly detection to offer an adaptive, proactive approach for spotting and investigating cyber incidents within complex IoT ecosystems.

2. Advancement of Automated Evidence Preservation Techniques

The APRM introduces automated systems for evidence preservation, lowering the risk of data loss during incidents and maintaining the integrity and legality of forensic

artefacts. Integrating automated evidence collection into the detection process fills a vital gap in current forensic readiness models, where evidence gathering often takes place after an incident and is vulnerable to delays or damage.

3. Enhancement of Forensic Readiness with International Compliance Alignment

This research integrates international standards, such as ISO/IEC 27043, into the APRM, ensuring that all evidence handling and investigative processes comply with recognised global legal and technical requirements. By aligning the model with established best practices, the study produces a readiness model that not only improves technical capabilities but also strengthens the legal credibility of forensic procedures.

4. Empirical Validation Through Performance Metrics in IoT Security

The research offers comprehensive empirical evidence of APRM's effectiveness through rigorous evaluation metrics, including accuracy, precision, recall, specificity, and F1 score. The system demonstrated strong performance, achieving 81.99% accuracy, 100% recall, and 84.52% F1 score, highlighting its robustness in detecting cyberattacks while maintaining operational efficiency. These results add to the body of knowledge by establishing measurable benchmarks for future forensic-readiness models in Internet of Things (IoT) settings.

5. Addressing Scalability and Resource Optimisation Challenges

The APRM's capacity to scale across large IoT environments without affecting performance marks a significant advancement over current DFR models. By automating routine investigative tasks and optimising resource use, the model allows organisations to stay prepared for forensic investigations without overburdening technical teams, even as device and data volumes grow.

6. Wazuh and File Auditing Utilised to Improve FIM

This research significantly enhances our understanding of network security and digital forensics by offering a comprehensive, realistic overview of how Wazuh and File Auditing can be used to improve FIM and identify suspicious behaviours. As organisations adopt more sophisticated IT environments, such as distributed networks and diverse endpoints, the need for effective monitoring solutions to ensure security and forensic readiness is growing rapidly. This study addresses these

concerns with key recommendations and a model for successfully deploying new, advanced tools within existing security systems. The paper also makes a substantial contribution to the knowledge base by presenting a detailed analysis of Wazuh's FIM architecture, which is vital for monitoring unauthorised changes to critical files and directories. Additionally, it provides detailed instructions for managing file auditing in the Windows Group Policy Editor, illustrating concepts step by step and linking theory to practice. These measures can be adopted by organisations, regardless of their technical expertise, to ensure effective implementation. By explaining how to set up Wazuh agents and the central server, the study simplifies deployment, making it easier for organisations to strengthen their security.

7. Bridging the Gap Between Digital Forensics and IoT Security

This research advances the growing field of digital forensics and IoT security by introducing a unified model that enables both proactive threat detection and forensic investigations. While current models typically address these areas separately, APRM integrates them, enabling organisations to transition seamlessly from incident detection to forensic response.

This research addressed the growing need for Digital Forensic Readiness (DFR) within IoT-enabled organisational environments by developing, implementing, and evaluating a standards-aligned Digital Forensic Readiness Model grounded in ISO/IEC 27043. The increasing adoption of Internet of Things technologies across organisational infrastructures has significantly expanded the cyberattack surface, creating substantial challenges for the identification, preservation, investigation, and legal admissibility of evidence. Existing approaches primarily focused on cybersecurity detection mechanisms or post-incident forensic investigations, while giving limited attention to proactive forensic readiness that supports real-time evidence generation and preservation within complex IoT ecosystems.

To address this gap, this study proposed a comprehensive DFR model integrating organisational governance, technical infrastructure, security monitoring, and forensic investigation processes into a unified readiness model. The model operationalised ISO/IEC 27043 readiness principles within an IoT-enabled organisational

environment and demonstrated how forensic readiness can function as a continuous organisational capability rather than a reactive post-incident activity.

The proposed model was implemented using real-world security monitoring and forensic tools, including Wazuh and Splunk, in controlled organisational attack scenarios involving brute-force and DDoS attacks, as well as other cyber threat activities. The implementation demonstrated the practical feasibility of integrating real-time monitoring, forensic evidence acquisition, secure log preservation, and chain-of-custody management into a unified forensic readiness workflow. The research further incorporated machine learning techniques to support cyberattack detection and the prioritisation of forensic evidence, thereby enhancing investigative efficiency and automation capabilities.

Experimental evaluation demonstrated that the proposed model improved organisational forensic readiness by reducing investigation time, enhancing evidence traceability, supporting automated evidence preservation, and strengthening incident response capabilities. The results also highlighted the importance of integrating forensic readiness directly into organisational cybersecurity architectures to improve resilience against evolving cyber threats. Furthermore, the study confirmed the applicability of ISO/IEC 27043 as a foundational standard for operationalising digital forensic readiness within distributed IoT ecosystems.

Overall, the research contributes to addressing the growing forensic challenges posed by modern IoT-enabled organisational infrastructures and demonstrates the practical value of combining forensic readiness, cybersecurity monitoring, machine learning, and standards-based governance into a unified model to support proactive digital investigation.

8.3 Implications of the study

The results of this study have significant implications across various sectors, including organisations, technology, policy, and academia, especially in Internet of Things (IoT) environments. Overall, the findings support the view that Digital Forensic Readiness (DFR) should be regarded as an ongoing process that organisations actively develop

and maintain, rather than something to be addressed solely after a security incident. The implications of these studies are outlined below.

1. Organisational and Managerial Implications

From the perspective of an organisation and its leaders, the study highlights the importance of integrating forensic preparedness into daily management and operations.

- Digital forensic readiness should be integrated into official structures, cybersecurity plans, and the organisation's approach to handling incidents.
- Treating DFR as a constant element helps organisations respond to incidents more swiftly, consistently, and in a legally acceptable manner.
- The suggested DFR model offers a flexible framework that can be customised for various IoT environments, aiding organisations in adapting forensic thinking to their specific systems and addressing concerns about applicability.
- Clear roles and responsibilities are necessary to foster confidence and ensure accountability when handling evidence, deciding what to do next, and making investigation choices.
- Good forensic readiness requires teamwork among technical staff, senior managers, legal experts, and compliance personnel.
- Organisations that take a readiness-focused approach are more likely to:
    - ✓ Keep the integrity of evidence during an incident.
    - ✓ Lessen confusion and unclear choices when making decisions.
    - ✓ Ensure accountability throughout the whole investigation process.

These points demonstrate that forensic readiness is not merely a technical issue but also a duty that organisational leaders and managers must assume.

2. Technical and Operational Implications

From a technical and operational perspective, the results underscore the importance of designing IoT systems with forensic preparedness in mind.

- Real-time monitoring and systematic logging are crucial for gathering reliable forensic data in rapidly evolving IoT environments.
- Implementing automatic systems to preserve digital evidence reduces the need

for manual data collection and decreases the risk of losing or corrupting evidence.

- Integrating security monitoring tools with forensic processes aids in swiftly creating, linking, and maintaining digital evidence.
- Machine learning can assist in forensic readiness by:
    - ✓ Assisting in focusing on the most vital forensic data.
    - ✓ Reducing the amount of work needed for investigations.
    - ✓ Making the evidence review process more efficient.
- However, automated analysis tools should serve as support for human experts rather than substitute them.
- Human supervision remains vital for interpreting findings, setting evidence in the proper context, and confirming that investigative decisions are legally justified.

Overall, these insights emphasise the importance of a considered approach that integrates technology with forensic professionals' expertise.

3. Policy, Legal, and Standards Implications

At the policy and standards level, research demonstrates the benefits of aligning forensic readiness efforts with widely accepted international frameworks.

- Making digital forensic readiness (DFR) processes adhere to standards like ISO/IEC 27043 helps establish a reliable and consistent approach to managing forensic tasks, reassuring organisations and legal bodies.
- Following these standards helps to track evidence correctly and improves the likelihood that digital proof will be accepted in legal cases.
- Organisations operating in areas with strict regulations or across various regions benefit from having clear, standard-compliant procedures for forensic work.
- This alignment assists with:
    - ✓ Meeting legal and regulatory obligations.
    - ✓ Collaborating with external investigators.
    - ✓ Communicating effectively with legal and law enforcement authorities.

- Adhering to recognised standards enhances an organisation's reputation and simplifies defending its actions during investigations.

These points indicate that using standards-based methods for forensic readiness is crucial in complex operations.

4. Research and Academic Implications

From an academic perspective, this study advances both the theoretical and practical aspects of digital forensics.

- It links high-level forensic frameworks with practical, operational execution.
- It demonstrates how forensic readiness can be evaluated and measured within real IoT-enabled organisational environments.
- The results emphasise the significance of interdisciplinary research that combines:
    - ✓ Organisational governance.
    - ✓ Technical infrastructure.
    - ✓ Legal and regulatory aspects.
- By making forensic readiness operational, the study lays the foundation for future research into:
    - ✓ Scalable Digital Forensic Readiness (DFR) models.
    - ✓ Automated forensic decision-support systems.
    - ✓ Evaluation metrics for readiness in new digital environments.

The findings of this research have important implications for academia, industry, cybersecurity practitioners, and organisational policymakers.

From an academic perspective, the study contributes to the growing body of knowledge surrounding Digital Forensic Readiness and IoT forensics by providing an empirically validated model grounded in international forensic standards. The research demonstrates that forensic readiness should not be viewed solely as a post-incident forensic activity but rather as a continuous organisational capability integrated into cybersecurity governance and operational processes. This perspective may encourage future researchers to explore proactive forensic architectures, adaptive

evidence-collection systems, and intelligent forensic readiness mechanisms in increasingly complex digital ecosystems.

The research also has methodological implications for future forensic readiness studies. By combining standards-based modelling, experimental implementation, attack simulation, and machine-learning-based analytics, the study presents a multidisciplinary approach to evaluating forensic readiness models in realistic organisational environments. This may support the development of more empirically grounded digital forensic research methodologies.

From an industrial perspective, the proposed model provides practical guidance for organisations seeking to strengthen cyber resilience and improve preparedness for digital investigations. Many organisations currently prioritise threat detection and incident response while lacking structured mechanisms for preserving evidentially reliable forensic data. The findings demonstrate that integrating forensic readiness into organisational security infrastructures can significantly improve investigative efficiency, reduce evidence loss, strengthen chain-of-custody management, and support rapid incident response.

The practical implementation of the model using Wazuh, Splunk, and machine-learning-based analytics also demonstrates that Digital Forensic Readiness can be operationalised with existing security technologies without requiring entirely new infrastructure. This may encourage organisations to incorporate forensic readiness principles into current Security Information and Event Management (SIEM) platforms, intrusion detection systems, and organisational cybersecurity policies.

The study further highlights the growing importance of forensic readiness within IoT-enabled organisational environments where evidence sources are highly distributed, heterogeneous, and dynamic. Organisations deploying smart devices, industrial IoT systems, cloud-native infrastructure, and edge computing technologies must increasingly consider how to proactively generate, preserve, and correlate forensic evidence before cyber incidents occur. Consequently, the proposed model provides

practical insights into how organisations can prepare for future investigative challenges associated with large-scale IoT ecosystems.

The findings also have implications for legal compliance and digital evidence management. The research emphasises the importance of maintaining evidential integrity, preserving metadata, ensuring reliable timestamping, and following chain-of-custody procedures to support legally defensible investigations. This may assist organisations in aligning their cybersecurity operations with international forensic standards, regulatory requirements, and expectations for evidential admissibility.

Finally, the novelty and impact of the proposed model lie in its ability to integrate forensic readiness, cybersecurity monitoring, machine learning analytics, and ISO/IEC 27043 processes into a unified organisational model specifically designed for IoT-enabled environments. Unlike previous conceptual approaches, the model was implemented in practice and experimentally validated, demonstrating both theoretical advancement and real-world applicability. The study therefore establishes a strong foundation for future development of intelligent, scalable, and adaptive Digital Forensic Readiness systems capable of supporting next-generation organisational cybersecurity and forensic investigation requirements.

8.4 Limitations of the Study

Although the proposed Adaptive Proactive Readiness Model (APRM) demonstrated effectiveness in supporting Digital Forensic Readiness (DFR) within IoT-enabled organisational environments, several limitations should be acknowledged. These limitations provide important context for interpreting the findings and highlight areas requiring further investigation.

1. Organisational and Legal Constraints of Digital Forensic Readiness

The successful implementation of Digital Forensic Readiness depends on the organisation's ability to operate within legal, regulatory, and governance requirements. As organisations increasingly operate across multiple jurisdictions, maintaining compliance while preserving digital evidence can become complex. Key challenges include:

- Ensuring compliance with legal, regulatory, and privacy obligations remains a

crucial concern.

- Any forensic readiness practice that conflicts with data protection or privacy laws could result in digital evidence being deemed inadmissible in court.
- Organisations operating across various jurisdictions face additional complexity due to differing legal and regulatory requirements.
- The absence of clear internal policies on evidence collection, storage, and use could leave organisations vulnerable to legal risks.

These constraints highlight the importance of strict legal oversight when implementing forensic readiness strategies.

2. Human Resource and Skills-Related Limitations

The effectiveness of forensic readiness depends heavily on the availability of skilled personnel to manage forensic processes, conduct cybersecurity monitoring, and investigate incidents. Key challenges include:

- A shortage of qualified digital forensic and cybersecurity professionals can hinder the effective deployment and upkeep of DFR capabilities.
- Poorly trained staff may struggle to implement forensic readiness plans accurately and consistently.
- Continuous training and staff awareness are vital to ensure understanding of forensic responsibilities and procedures.
- High staff turnover can further weaken long-term preparedness if knowledge and expertise are not retained within the organisation.

These limitations emphasise the need to invest in people, not just technology.

3. Insider and Organisational Behavioural Risks

Human factors remain one of the most difficult aspects of managing forensic readiness. Both intentional and unintentional actions by employees can affect the effectiveness of forensic monitoring and evidence preservation. Key challenges include:

- Employees may intentionally or unintentionally interfere with forensic monitoring or evidence collection systems.
- Insider misconduct, such as attempts to disable or bypass DFR technologies, can compromise evidential integrity.

- A lack of awareness regarding the purpose and importance of forensic readiness can lead to resistance or non-compliance among staff.
- Poor enforcement of internal controls can weaken the effectiveness of DFR systems.

Addressing behavioural risks relies on a strong organisational culture, clear policies, and effective oversight.

4. Financial and Resource Constraints

The implementation and maintenance of Digital Forensic Readiness capabilities require significant investment in technology, infrastructure, personnel, and governance processes. Key challenges include:

- Substantial financial resources are necessary to obtain advanced forensic and monitoring tools.
- Legacy systems often require modernisation to maintain forensic readiness.
- Ongoing costs for training, system maintenance, and compliance checking can be difficult to sustain.
- Securing long-term funding support from organisational leadership can be challenging, especially when forensic readiness is not regarded as an immediate business priority.

These constraints might hinder the adoption of DFR, particularly in resource-constrained organisations.

5. Data Retention and Evidence Management Challenges

Maintaining sufficient evidence for future investigations while avoiding excessive data collection remains a significant challenge for organisations. Key challenges include:

- Organisations must determine how much data to retain for potential investigations without gathering excessive or unnecessary information.
- Premature data disposal may result in the loss of crucial forensic evidence.
- Keeping data longer than necessary increases legal, financial, and privacy risks.
- Poorly defined data retention policies can undermine both investigative effectiveness and regulatory compliance.

Balancing the availability of evidence with legal and cost considerations remains a significant challenge.

6. Environmental and Contextual Limitations

The proposed model was evaluated in a controlled organisational environment. While this approach ensured consistency and repeatability, it may not fully reflect the complexity of large-scale operational deployments. Key challenges include:

- The experimental setup was arranged within a controlled organisational environment to ensure repeatability, reliability, and adherence to ethical standards.
- Such controlled conditions might not fully capture the operational complexity of large-scale or real-world IoT ecosystems.
- This study did not cover highly heterogeneous environments with extensive device diversity.
- Scenarios involving inter-organisational data exchange and shared forensic responsibilities were not examined.
- Variations in legal and regulatory requirements across different jurisdictions were not fully scrutinised.

These factors could affect the extent to which the findings can be applied to more complex or widespread IoT deployments.

7. Large-Scale Deployment and Resource-Constrained Environment Limitations

Although the proposed model demonstrated positive results in the experimental environment, additional challenges may arise when deploying it in large-scale or resource-constrained IoT environments. Key challenges include:

- Significant increases in log volume, event generation, and evidence storage requirements.
- Computational overhead associated with continuous monitoring and forensic data collection.
- Network bandwidth limitations when transmitting large volumes of forensic data.
- Resource-constrained IoT devices with limited processing power, storage, and battery capacity.

- Increased complexity when integrating devices from multiple vendors using different protocols and architectures
- Sector-specific operational constraints within healthcare, manufacturing, transportation, and critical infrastructure environments.
- Scalability concerns relating to evidence management, event correlation, and forensic analysis across thousands of devices.
- Additional financial costs associated with large-scale deployments.

8. Need for Broader Validation

Although the model was successfully implemented and evaluated in this study, further validation is required to establish its broader applicability. Key challenges include:

- Limited evaluation within a single organisational context.
- Lack of long-term operational assessment.
- Absence of large-scale multi-organisational deployments.
- Limited testing across different industry sectors.
- Need for further assessment of scalability, sustainability, and operational impact.
- Requirement for additional validation within highly distributed and resource-constrained IoT environments.

Addressing these limitations through future research and broader real-world deployment would strengthen the evidence base supporting the proposed APRM and improve its applicability across diverse organisational and IoT environments.

8.5 Recommendations for Future Research

This research outlines several directions for future work to enhance, expand, and validate the proposed Digital Forensic Readiness (DFR) model in evolving IoT-enabled environments. As IoT technologies continue to grow across sectors and become more complex, further research is needed to ensure that forensic readiness approaches remain effective, scalable, and legally sound.

1. Large-Scale and Real-World Validation

Future studies should go beyond controlled experimental settings to evaluate the proposed DFR model in more complex operational environments.

- Assess the model in extensive, multi-organisational IoT settings.

- Examine deployments across geographically dispersed and cross-sector infrastructures.
- Assess scalability, interoperability, and long-term operational sustainability.
- Analyse performance overheads in environments with continuous data generation.
- Examine how high device heterogeneity affects forensic readiness procedures.

Such assessments would offer a greater understanding of the model's real-world applicability.

2. Legal and Regulatory Considerations Across Different Jurisdictions

Further research is necessary to tackle legal and regulatory diversity:

- Analyse how variations in data protection laws affect forensic readiness strategies.
- Examine differences in evidential admissibility standards across jurisdictions.
- Analyse incident reporting and disclosure duties across various legal frameworks.
- Perform comparative studies across various regulatory frameworks to improve generalisability.
- Explore adaptation strategies for organisations operating internationally.

These studies would underpin the development of legally sound, internationally applicable forensic readiness models.

3. Advancing Machine Learning for Forensic Readiness

Further advancements in AI and machine learning are crucial for enhancing forensic readiness in IoT environments.

- Develop models that are explainable and interpretable, suitable for forensic and judicial review.
- Create more resilient detection models that lower false positives and false negatives.
- Explore strategies for reducing bias in forensic decision-support systems.
- Align machine learning outputs with legal and evidential standards.
- Enhance contextual awareness in threat detection to more accurately mirror real operational conditions.

- Investigate adaptive learning methods that adapt to changing attack patterns.

Improving these capabilities would enable more precise, efficient, and trustworthy forensic investigations.

4. Automation of Chain-of-Custody and Evidence Provenance

Future research could examine more sophisticated methods of evidence management.

- Examine automated chain-of-custody systems for decentralised IoT environments.
- Investigate secure logging and cryptographic methods to reinforce evidential integrity.
- Evaluate the application of distributed ledger or similar technologies for provenance verification.
- Minimise dependence on manual tasks in multi-organisational investigations.
- Strengthen trust and responsibility in evidence management across administrative borders.

Such approaches are especially pertinent for complex, large-scale forensic investigations.

5. Sector-Specific Uses of Digital Forensic Readiness

Finally, implementing DFR within particular industry contexts is a crucial area for research.

- Create customised DFR solutions for healthcare settings.
- Analyse forensic readiness challenges in smart cities and urban infrastructure.
- Examine applications in critical infrastructure and industrial IoT systems.
- Assess sector-specific regulatory, operational, and evidential requirements.
- Establish best practices through empirical validation in real operational environments.

Sector-focused studies can showcase DFR's adaptability and strengthen its position as a key organisational competency.

6. Standardisation of DFR Models for IoT Environments

Standardisation is an important area for future research.

- Establish best practices for deploying DFR models within IoT platforms.
- Develop realistic and reproducible implementation guidelines.
- Ensure compatibility with existing organisational systems and workflows.

- Align DFR models with recognised standards like ISO/IEC 27043.
- Establish performance evaluation metrics, such as:
    - ✓ Evidence response time.
    - ✓ System resilience.
    - ✓ Resilience against attacks.

Standardised methods would promote consistency, reliability, and legal validity.

7. Ongoing Enhancement of Current Methods

Given the rapid development of IoT technologies, the continuous improvement of forensic methods remains essential.

- Adapt forensic methods to support heterogeneous devices, protocols, and platforms.
- Incorporate feedback from industry practitioners to improve real-world applicability.
- Conduct empirical studies focused on validation rather than theoretical enhancement alone.
- Create realistic forensic scenarios that simulate IoT-related cyber incidents.
- Combine AI, machine learning, and blockchain technologies to:
    - ✓ Improve detection accuracy.
    - ✓ Reduce human error.
    - ✓ Strengthen evidence integrity

Ongoing improvement ensures that forensic readiness remains aligned with emerging threats and technologies.

Although this research successfully designed, implemented, and evaluated an ISO/IEC 27043-aligned Digital Forensic Readiness (DFR) Model for IoT-enabled organisational environments, the rapid evolution of IoT ecosystems, distributed computing infrastructures, and intelligent cyber threats creates several opportunities for further investigation and enhancement. Future research should focus on improving the scalability, automation, adaptability, and real-world applicability of digital forensic readiness within increasingly complex organisational environments.

One important direction for future work involves the integration of the proposed model within cloud-native IoT infrastructures. Modern organisations are increasingly migrating from traditional on-premise infrastructures toward cloud-based environments that utilise microservices, virtual machines, containerised applications, Kubernetes orchestration, and distributed storage platforms. While cloud-native architectures provide scalability, flexibility, and high availability, they also introduce substantial forensic challenges associated with distributed data generation, virtualised evidence sources, dynamic workload allocation, and multi-tenant environments. In such infrastructures, digital evidence may be generated across multiple cloud regions, containers, APIs, and virtual nodes, making evidence acquisition and preservation significantly more complex than in conventional systems.

Future research should therefore investigate how Digital Forensic Readiness processes can be adapted to support cloud-native organisational architectures while maintaining forensic soundness and evidential integrity. Particular attention should be given to cloud log preservation, forensic acquisition of containerised workloads, virtual machine snapshot integrity, cloud orchestration audit trails, and cross-platform evidence correlation. Additional studies should also examine how international standards such as ISO/IEC 27043 can be operationalised within Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments. Furthermore, legal and jurisdictional challenges related to cross-border cloud evidence storage, privacy regulations, and compliance obligations should be explored in greater detail to strengthen the practical applicability of forensic readiness in global cloud infrastructures.

Another significant area for future development concerns the extension of Digital Forensic Readiness into edge computing environments. Edge computing has emerged as a critical technology for IoT ecosystems because it enables real-time processing closer to IoT devices, thereby reducing network latency, bandwidth consumption, and reliance on centralised cloud infrastructure. However, the decentralised nature of edge computing introduces new forensic challenges, as evidence may be distributed

across numerous lightweight edge nodes with limited computational resources and temporary storage capacity. Additionally, edge devices often operate in highly dynamic environments where data volatility, intermittent connectivity, and physical exposure may compromise the preservation of forensic evidence.

Future research should therefore focus on developing lightweight forensic readiness mechanisms specifically designed for edge-enabled IoT systems. These mechanisms should support real-time evidence acquisition, local event reconstruction, decentralised log management, and secure synchronisation with central forensic repositories without significantly affecting device performance. Researchers should also investigate adaptive evidence-retention strategies that prioritise critical forensic artefacts in resource-constrained environments. Moreover, studies should examine how edge-based forensic readiness can support autonomous industrial systems, smart healthcare infrastructures, intelligent transportation systems, and smart city environments where rapid incident detection and localised evidence collection are essential.

The integration of Artificial Intelligence (AI) and adaptive learning techniques into Digital Forensic Readiness represents another promising direction for future investigation. Although this study employed machine learning models for cyberattack detection and forensic feature prioritisation, future systems could incorporate more advanced AI-driven mechanisms to support intelligent forensic decision-making and autonomous readiness management. As cyber threats continue to evolve in sophistication and scale, static forensic readiness mechanisms may prove insufficient to detect previously unseen attack patterns or to dynamically adapt to changing organisational environments.

Future research should therefore explore the use of deep learning, reinforcement learning, neural networks, and explainable AI techniques to develop adaptive forensic readiness systems that learn from historical incidents and continuously improve evidence collection strategies. Such systems could automatically identify suspicious behavioural patterns, predict emerging attack vectors, prioritise high-value evidence sources, and dynamically adjust monitoring configurations based on threat

intelligence. Explainable AI mechanisms are particularly important in forensic investigations because organisations and legal authorities require transparent and interpretable decision-making processes to support evidential admissibility and accountability. Consequently, future work should investigate how explainable AI can improve trust, transparency, and legal defensibility within AI-driven forensic readiness systems.

Future studies should also investigate the automation of forensic readiness processes across heterogeneous IoT ecosystems. The increasing number of interconnected IoT devices generates massive volumes of logs, metadata, sensor data, and network traces that cannot be managed efficiently through manual investigation processes alone. Automated forensic readiness mechanisms that continuously monitor, correlate, classify, and preserve digital evidence in real time would significantly improve organisational responsiveness and reduce investigative overhead.

Research in this area should focus on automated evidence-orchestration models that integrate data from multiple IoT devices, cloud services, security monitoring platforms, and forensic repositories into unified investigative pipelines. Future systems could employ intelligent event correlation, automated chain-of-custody generation, dynamic evidence tagging, and policy-driven forensic workflows to streamline investigation procedures. Additionally, technologies such as blockchain and distributed ledger systems could be explored to strengthen evidence immutability, timestamp verification, and forensic auditability within decentralised environments. These approaches may significantly enhance organisational trust in digital evidence while reducing opportunities for evidence tampering or manipulation.

Scalability remains another critical area requiring further investigation. While the proposed Digital Forensic Readiness Model demonstrated effectiveness within controlled experimental environments, future work should evaluate the model in large-scale organisational deployments involving thousands of interconnected IoT devices operating across geographically distributed infrastructures. Large-scale environments may introduce performance bottlenecks associated with log

aggregation, evidence indexing, storage management, and real-time forensic analytics. Therefore, future research should examine scalable forensic architectures capable of handling high-volume evidence streams while maintaining rapid response times and efficient resource utilisation.

Further research should also explore the interoperability of forensic readiness models across different IoT vendors, communication protocols, and security platforms. The heterogeneous nature of IoT environments continues to present substantial challenges because devices often utilise proprietary architectures and inconsistent logging mechanisms. Standardised forensic interfaces, interoperable evidence formats, and unified forensic metadata models could improve cross-platform investigations and facilitate collaborative forensic analysis between organisations and law enforcement agencies.

Additionally, future work should investigate sector-specific implementations of Digital Forensic Readiness. Different industries, including healthcare, finance, manufacturing, transportation, energy, and smart cities, face unique operational, regulatory, and security challenges. For example, healthcare environments require strict compliance with patient privacy regulations, while industrial IoT infrastructures prioritise operational continuity and safety-critical monitoring. Future studies should therefore evaluate how Digital Forensic Readiness models can be customised to address the specific forensic, operational, and compliance requirements of different sectors.

Another important area for future investigation involves legal admissibility and regulatory compliance in real-time forensic evidence collection. As forensic readiness mechanisms increasingly rely on automated collection, distributed infrastructures, and AI-driven analytics, organisations must ensure that evidence remains legally admissible within judicial and regulatory contexts. Future research should therefore examine legal frameworks governing digital evidence collection, privacy preservation, forensic accountability, and cross-jurisdictional evidence sharing. Particular attention should be given to compliance with international standards and

regulations such as GDPR, ISO/IEC 27043, ISO/IEC 27037, and NIST digital forensic guidelines.

Finally, future work should involve long-term empirical evaluation of the proposed model in operational organisational environments. While controlled experimental scenarios provide valuable validation, longitudinal real-world deployments would enable researchers to assess the model's effectiveness under evolving cyber threats, changing organisational requirements, and varying operational conditions. Such evaluations would provide deeper insight into deployment complexity, user adoption, maintenance requirements, scalability limitations, and practical organisational benefits associated with Digital Forensic Readiness in modern IoT ecosystems.

Overall, future advancements in cloud-native computing, edge intelligence, AI-driven automation, and scalable forensic orchestration are expected to significantly transform Digital Forensic Readiness in the coming years. Continued research in these areas will contribute toward the development of more intelligent, adaptive, scalable, and legally defensible forensic readiness models capable of supporting the next generation of IoT-enabled organisational environments.

8.6 Concluding Summary

This research was motivated by the evolution of IoT-enabled organisations and the growing challenges this evolution presents for DFR. As IoT infrastructures become more complex, distributed, and dynamic, traditional reactive digital forensic methods are becoming less effective for supporting timely, reliable, and legally defensible investigations. This study introduces a validated, standards-compliant, and practical approach to Digital Forensic Readiness for IoT-enabled organisations. By demonstrating how forensic readiness can be integrated into organisational and technical frameworks, the research makes significant contributions to both digital forensic theory and practice. Through the development and evaluation of the Automated Proactive Readiness Model (APRM), the study shows how forensic readiness can be practically embedded within organisational processes, real-time security monitoring, and IoT infrastructures in accordance with ISO/IEC 27043.

The empirical results confirm that APRM improves evidence integrity, traceability, and chain-of-custody compliance while reducing investigation effort and response time. The integration of machine learning further supports intelligent evidence prioritisation without replacing human forensic judgement. Despite limitations related to scalability and environmental diversity, this work offers both theoretical progress and practical guidance, positioning forensic readiness as a crucial component of cybersecurity and organisational resilience in modern IoT environments. The findings of this research will assist organisations in enhancing cyber resilience, strengthening investigative capabilities, and preparing for the evolving challenges of IoT-driven digital environments.

9.0 References

Ab Rahman, N.H., Glisson, W.B., Yang, Y. and Choo, K.K.R. (2016) 'Forensic-by-Design Framework for Cyber-Physical Cloud Systems', *IEEE Cloud Computing*, 3(1), pp. 50–59. Available at: https://doi.org/10.1109/MCC.2016.5.

Abbass, W., Bakraouy, Z., Baina, A. and Bellafkih, M. (2019) 'Assessing the internet of things security risks', *Journal of Communications*, 14(10), pp. 958–964. Available at: https://doi.org/10.12720/jcm.14.10.958-964.

Abiodun, O.I., Abiodun, E.O., Alawida, M., Alkhawaldeh, R.S. and Arshad, H. (2021) 'A Review on the Security of the Internet of Things: Challenges and Solutions', *Wireless Personal Communications*, 119(3), pp. 2603–2637. Available at: https://doi.org/10.1007/s11277-021-08348-9.

Abomhara, M. and Køien, G.M. (2015) 'Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks', *Journal of Cyber Security and Mobility*, 4(1), pp. 65–88. Available at: https://doi.org/10.13052/jcsm2245-1439.414.

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M. and Alshehhi, A. (2021) 'A novel SETA-based gamification framework to raise cybersecurity awareness', *International Journal of Information Technology*, 13(6), pp. 2371–2380. Available at: https://doi.org/10.1007/s41870-021-00760-5.

Academy Fynd (2023) 'What Does a Firewall Do_ Types, Functions, Benefits, and Best Practices in Cybersecurity'. Available at: https://www.fynd.academy/blog/a-firewall-protects-which-of-the-following-attacks (Accessed: 21 November 2024).

Adeyemi R. Ikuesan, H.S.V. (no date) *2017 IEEE Conference on Applications, Information and Network Security : AINS 2007 : 13th-14th November 2017, Miri Marriott Resort & Spa, Miri, Sarawak, Malaysia*.

Ahmed, A.A., Farhan, K., Jabbar, W.A., Al-Othmani, A. and Abdulrahman, A.G. (2024) 'IoT Forensics: Current Perspectives and Future Directions', *Sensors*, 24(16), p. 5210. Available at: https://doi.org/10.3390/s24165210.

Akgün, M. and Çıalayan, M.U. (2015) 'Providing destructive privacy and scalability in RFID systems using PUFs', *Ad Hoc Networks*, 32, pp. 32–42. Available at: https://doi.org/10.1016/j.adhoc.2015.02.001.

Alahi, M.E.E., Sukkuea, A., Tina, F.W., Nag, A., Kurdthongmee, W., Suwannarat, K. and Mukhopadhyay, S.C. (2023) 'Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends', *Sensors*, 23(11), p. 5206. Available at: https://doi.org/10.3390/s23115206.

Aldawood, H. and Skinner, G. (2019) 'Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues', *Future Internet*, 11(3), p. 73. Available at: https://doi.org/10.3390/fi11030073.

Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M. and Wills, G. (2019) 'IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions', *Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*. SCITEPRESS - Science and Technology Publications, pp. 106–115. Available at: https://doi.org/10.5220/0007905401060115.

Alghamdi, M.I. (2020) 'Digital forensics in cyber security-recent trends, threats, and opportunities', 8(3), pp. 1321–1330.

Alghamdi, M.I. (2021) *Digital Forensics in Cyber Security-Recent Trends, Threats, and Opportunities*. Available at: www.intechopen.com.

Allioui, H. and Mourdi, Y. (2023) 'Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey', *Sensors*, 23(19), p. 8015. Available at: https://doi.org/10.3390/s23198015.

Al-Mahrouqi, A., Abdalla, S. and Kechadi, T. (2015) 'Cyberspace Forensics Readiness and Security Awareness Model', *International Journal of Advanced Computer Science and Applications*, 6(6). Available at: https://doi.org/10.14569/IJACSA.2015.060617.

Al-Masri, E., Bai, Y. and Li, J. (2018) 'A fog-based digital forensics investigation framework for IoT systems', *Proceedings - 3rd IEEE International Conference on Smart Cloud, SmartCloud 2018*. Institute of Electrical and Electronics Engineers Inc., pp. 196–201. Available at: https://doi.org/10.1109/SmartCloud.2018.00040.

Alqahtani, M., Gumaei, A., Mathkour, H. and Ismail, M.M. Ben (2019) 'A genetic-based extreme gradient boosting model for detecting intrusions in wireless sensor networks', *Sensors (Switzerland)*, 19(20). Available at: https://doi.org/10.3390/s19204383.

Alruwaili, A. (2019) 'A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS', *International Journal of Advanced Research in Computer Science*, 10(5), pp. 1–3. Available at: https://doi.org/10.26483/ijarcs.v10i5.6476.

Alsaqour, R., Motmi, A. and Abdelhaq, M. (2021) 'A Systematic Study of Network Firewall and Its Implementation', *IJCSNS International Journal of Computer Science and Network Security*, 21(4). Available at: https://doi.org/10.22937/IJCSNS.2021.21.4.24.

Alshar'e, M. (2023) 'CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001', *Applied computing Journal*, pp. 245–255. Available at: https://doi.org/10.52098/acj.202364.

Altulaihan, E., Alismail, A., Hafizur Rahman, M.M. and Ibrahim, A.A. (2023) 'Email Security Issues, Tools, and Techniques Used in Investigation', *Sustainability*, 15(13), p. 10612. Available at: https://doi.org/10.3390/su151310612.

Amin (2013) *Difference Between Model and Framework Model vs Framework*. Available at: https://www.differencebetween.com/difference-between-model-and-vs-framework/ (Accessed: 5 February 2023).

Angrishi, K. (2017) 'Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets'. Available at: http://arxiv.org/abs/1702.03681.

Antony, A. and S., S. (2020) 'A Review on IoT Operating Systems', *International Journal of Computer Applications*, 176(24), pp. 33–40. Available at: https://doi.org/10.5120/ijca2020920245.

Ariffin, K.A.Z. and Ahmad, F.H. (2021) 'Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0', *Computers and Security*, 105. Available at: https://doi.org/10.1016/j.cose.2021.102237.

Atlam, H.F., El-Din Hemdan, E., Alenezi, A., Alassafi, M.O. and Wills, G.B. (2020) 'Internet of Things Forensics: A Review', *Internet of Things (Netherlands)*. Elsevier B.V. Available at: https://doi.org/10.1016/j.iot.2020.100220.

Atta, N. and Talamo, C. (2020) 'Digital Transformation in Facility Management (FM). IoT and Big Data for Service Innovation', pp. 267–278. Available at: https://doi.org/10.1007/978-3-030-33570-0_24.

Aziz, B., Blackwell, C. and Islam, S. (2013) 'A Framework for Digital Forensics and Investigations', *International Journal of Digital Crime and Forensics*, 5(2), pp. 1–22. Available at: https://doi.org/10.4018/jdcf.2013040101.

Baek, J., Kanampiu, M.W. and Kim, C. (2021) 'A Secure Internet of Things Smart Home Network: Design and Configuration', *Applied Sciences*, 11(14), p. 6280. Available at: https://doi.org/10.3390/app11146280.

BAJRAMI, E., IDRIZI, F. and RUSHITI, A. (2024) 'ENHANCING WEBSITE SPEED AND SECURITY WITH CLOUDFLARE CDN: A CASE STUDY ON WORDPRESS WEBSITES', *Journal of Natural Sciences and Mathematics of UT-JNSM*, 9(17–18), pp. 294–304. Available at: https://doi.org/10.62792/ut.jnsm.v9.i17-18.p2824.

Barricelli, B.R., Cassano, F., Fogli, D. and Piccinno, A. (2019) 'End-user development, end-user programming and end-user software engineering: A systematic mapping study', *Journal of Systems and Software*, 149, pp. 101–137. Available at: https://doi.org/10.1016/j.jss.2018.11.041.

Berger, C., Eichhammer, P., Reiser, H.P., Domaschka, J., Hauck, F.J. and Habiger, G. (2022) 'A Survey on Resilience in the IoT', *ACM Computing Surveys*, 54(7), pp. 1–39. Available at: https://doi.org/10.1145/3462513.

Biau, G. and Scornet, E. (2015) 'A Random Forest Guided Tour'. Available at: http://arxiv.org/abs/1511.05741.

Bokefode, J.D., Bhise, A.S., Satarkar, P.A. and Modani, D.G. (2016) 'Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption', *Procedia Computer Science*. Elsevier B.V., pp. 43–50. Available at: https://doi.org/10.1016/j.procs.2016.06.007.

Bröring, A., Seeger, J., Papoutsakis, M., Fysarakis, K. and Caracalli, A. (2020) 'Networking-Aware IoT Application Development', *Sensors*, 20(3), p. 897. Available at: https://doi.org/10.3390/s20030897.

Carrier, B.D. (2006) *A HYPOTHESIS-BASED APPROACH TO DIGITAL FORENSIC INVESTIGATIONS*.

Cassell, C., Cunliffe, A. and Grandy, G. (2018) *The SAGE Handbook of Qualitative Business and Management Research Methods: History and Traditions*, *The SAGE Handbook of Qualitative Business*

and Management Research Methods: History and Traditions. SAGE Publications Ltd. Available at: https://doi.org/10.4135/9781526430212.

Chen, T. and Guestrin, C. (2016) 'XGBoost: A Scalable Tree Boosting System'. Available at: https://doi.org/10.1145/2939672.2939785.

Chi, H., Aderibigbe, T. and Granville, B.C. (2019) 'A Framework for IoT Data Acquisition and Forensics Analysis', *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*. Institute of Electrical and Electronics Engineers Inc., pp. 5142–5146. Available at: https://doi.org/10.1109/BigData.2018.8622019.

CHIEN, H.-Y., WU, T.-C. and HSU, C.-L. (2015) 'RFID Authentication with Un-Traceability and Forward Secrecy in the Partial-Distributed-Server Model', *IEICE Transactions on Information and Systems*, E98.D(4), pp. 750–759. Available at: https://doi.org/10.1587/transinf.2014ICI0001.

Cochrane, T., Foster, P., Chhabra, V., Lemercier, M., Salvi, C. and Lyons, T. (2021) 'SK-Tree: a systematic malware detection algorithm on streaming trees via the signature kernel'. Available at: http://arxiv.org/abs/2102.07904.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S. (2018) 'Internet of Things security and forensics: Challenges and opportunities', *Future Generation Computer Systems*. Elsevier B.V., pp. 544–546. Available at: https://doi.org/10.1016/j.future.2017.07.060.

Creswell, J.W. (2009) 'Research Design Qualitative and Quantitative Approaches. Thousand Oaks. CA Sage.'

Devos, L., Meert, W. and Davis, J. (2022) 'Adversarial Example Detection in Deployed Tree Ensembles'. Available at: http://arxiv.org/abs/2206.13083.

Dimitriadis, A., Ivezic, N., Kulvatunyou, B. and Mavridis, I. (2020) 'D4I - Digital forensics framework for reviewing and investigating cyber attacks', *Array*, 5, p. 100015. Available at: https://doi.org/10.1016/j.array.2019.100015.

Dionísio, N., Alves, F., Ferreira, P.M. and Bessani, A. (2019) *Cyberthreat Detection from Twitter using Deep Neural Networks*. Available at: http://www.ieee.org/publications.

Du, X., Le, Q. and Scanlon, M. (2020) 'Automated Artefact Relevancy Determination from Artefact Metadata and Associated Timeline Events', *International Conference on Cyber Security*

and Protection of Digital Services, Cyber Security 2020. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/CyberSecurity49315.2020.9138874.

Dunn Cavelty, M. and Egloff, F.J. (2019) *The Politics of Cybersecurity: Balancing Different Roles of the State*.

Dunn Cavelty, M. and Wenger, A. (2020) 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science', *Contemporary Security Policy*, 41(1), pp. 5–32. Available at: https://doi.org/10.1080/13523260.2019.1678855.

Elgazzar, K., Khalil, H., Alghamdi, T., Badr, A., Abdelkader, G., Elewah, A. and Buyya, R. (2022) 'Revisiting the internet of things: New trends, opportunities and grand challenges', *Frontiers in the Internet of Things*, 1. Available at: https://doi.org/10.3389/friot.2022.1073780.

Felipe Diaz Lopez, A. (2017) *Are You Ready? A Proposed Framework For The Assessment Of Digital Forensic Readiness*. Available at: https://egrove.olemiss.edu/etd/1061.

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I. (2020) 'Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management', *Risk Analysis*, 40(1), pp. 183–199. Available at: https://doi.org/10.1111/risa.12891.

Ghelani, D. (2022) 'Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review', *American Journal of Science, Engineering and Technology*, 3(6), pp. 12–19. Available at: https://doi.org/10.11648/j.XXXX.2022XXXX.XX.

Ghosh, S., Yadav, S., Wang, X., Chakrabarty, B. and Kadıoğlu, S. (2022) 'Dichotomic Pattern Mining Integrated With Constraint Reasoning for Digital Behavior Analysis', *Frontiers in Artificial Intelligence*, 5. Available at: https://doi.org/10.3389/frai.2022.868085.

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021) 'Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures', *Sensors*, 21(14), p. 4759. Available at: https://doi.org/10.3390/s21144759.

Gooley, Jason., Yanch, Dana., Schuemann, Dustin. and Curran, John. (2020) *Cisco Software-Defined Wide Area Networks Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN*. Cisco Press.

Grigaliunas, S., Toldinas, J., Venckauskas, A., Morkevicius, N. and Damasevicius, R. (2021) 'Digital Evidence Object Model for Situation Awareness and Decision Making in Digital Forensics Investigation', *IEEE Intelligent Systems*, 36(5), pp. 39–48. Available at: https://doi.org/10.1109/MIS.2020.3020008.

Grobler, C.P. and Louwrens, C.P. (2007) 'Digital Forensic Readiness as a Component of Information Security Best Practice', pp. 13–24. Available at: https://doi.org/10.1007/978-0-387-72367-9_2.

Gugueoth, V., Safavat, S. and Shetty, S. (2023) 'Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects', *ICT Express*, 9(5), pp. 941–960. Available at: https://doi.org/10.1016/j.icte.2023.03.006.

Harbawi, M. and Varol, A. (2017) 'An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework', *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/ISDFS.2017.7916508.

He, W. and Zhang, Z. (Justin) (2019) 'Enterprise cybersecurity training and awareness programs: Recommendations for success', *Journal of Organizational Computing and Electronic Commerce*, 29(4), pp. 249–257. Available at: https://doi.org/10.1080/10919392.2019.1611528.

Hogland (2016) *Difference between Model and Framework*. Available at: https://www.stepbystep.com/difference-between-model-and-framework-93062/ (Accessed: 5 March 2023).

Hossain, M., Hasan, R. and Zawoad, S. (2018) 'Probe-IoT: A public digital ledger based forensic investigation framework for IoT', *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*. Institute of Electrical and Electronics Engineers Inc., pp. 1–2. Available at: https://doi.org/10.1109/INFCOMW.2018.8406875.

Hossain, M., Karim, Y. and Hasan, R. (2018) 'FIF-IoT: A forensic investigation framework for IoT using a public digital ledger', *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*. Institute of Electrical and Electronics Engineers Inc., pp. 33–40. Available at: https://doi.org/10.1109/ICIOT.2018.00012.

Hsu, C.-W. and Yeh, C.-C. (2017) 'Understanding the factors affecting the adoption of the Internet of Things', *Technology Analysis & Strategic Management*, 29(9), pp. 1089–1102. Available at: https://doi.org/10.1080/09537325.2016.1269160.

Imperva (2022) *Cyber Security Threats What are Cyber Security Threats?* Available at: https://www.imperva.com/learn/application-security/cyber-security-threats/.

Iqbal, M., Suhail, S. and Matulevicius, R. (2024) 'Proactive Security Approach for IoV by Leveraging Deception-based Digital Twins and Blockchain', *Proceedings of the 19th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, pp. 1–11. Available at: https://doi.org/10.1145/3664476.3670473.

Islam Jahidul Md., M.Md., K.A.D.C.B. and Kabir Sumaiya (no date) '2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT 2019) : May 3-5, 2019, Dhaka, Bangladesh.'

ISO (2015) 'International Standard, Information Technology – Security Techniques – Incident Investigation Principles and Processes'. Available at: ISO.org (Accessed: 15 March 2023).

Iwendi, C., Khan, S., Anajemba, J.H., Mittal, M., Alenezi, M. and Alazab, M. (2020) 'The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems', *Sensors (Switzerland)*, 20(9). Available at: https://doi.org/10.3390/s20092559.

Jabraeil Jamali, M.A., Bahrami, B., Heidari, A., Allahverdizadeh, P. and Norouzi, F. (2020) 'Towards the Internet of Things: Architectures, Security, and Applications', in M.A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi (eds.), pp. 9–31.

Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M. and Hashemi, S.H. (2023) 'A Review on the Security of IoT Networks: From Network Layer's Perspective', *IEEE Access*, 11, pp. 71073–71087. Available at: https://doi.org/10.1109/ACCESS.2023.3246180.

Jang-Jaccard, J. and Nepal, S. (2014) 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences*. Academic Press Inc., pp. 973–993. Available at: https://doi.org/10.1016/j.jcss.2014.02.005.

Janwar, I. (2021) 'Man in the Middle Attack using DHCP'. Available at: https://www.academia.edu/4903478/Man_in_the_Middle_Attack_using_DHCP (Accessed: 21 June 2024).

Jeyanthi, N. (2016) 'Internet of Things (IoT) as Interconnection of Threats (IoT)', *Security and Privacy in Internet of Things (IoTs)*. CRC Press, pp. 3–21. Available at: https://doi.org/10.1201/b19516-3.

Karie, N.M. and Karume, S.M. (2017) *Digital Forensic Readiness in Organizations DIGITAL FORENSIC READINESS IN ORGANIZATIONS: ISSUES AND CHALLENGES*.

Karie, N.M. and Valli, C. (2021) 'Digital Forensic Readiness Implementation in SDN: Issues and Challenges'. Available at: https://doi.org/10.48550/arxiv.2107.13759.

Karie, N.M. and Venter, H.S. (2015) 'Taxonomy of Challenges for Digital Forensics', *Journal of Forensic Sciences*, 60(4), pp. 885–893. Available at: https://doi.org/10.1111/1556-4029.12809.

Kebande, V.R., Karie, N.M. and Venter, H.S. (2018) 'Adding Digital Forensic Readiness as a Security Component to The IoT Domain', 8(1).

Kebande, V.R., Menza, N.K. and Venter, H.S. (2018) 'Functional Requirements for Adding Digital Forensic Readiness as a Security Component in IoT Environments', *International Journal on Advanced Science, Engineering and Information Technology*, 8(2), p. 342. Available at: https://doi.org/10.18517/ijaseit.8.2.2121.

Kebande, V.R., Mudau, P.P., Ikuesan, R.A., Venter, H.S. and Choo, K.-K.R. (2020) 'Holistic digital forensic readiness framework for IoT-enabled organizations', *Forensic Science International: Reports*, 2, p. 100117. Available at: https://doi.org/10.1016/j.fsir.2020.100117.

Kebande, V.R. and Ray, I. (2016) 'A generic digital forensic investigation framework for Internet of Things (IoT)', *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*. Institute of Electrical and Electronics Engineers Inc., pp. 356–362. Available at: https://doi.org/10.1109/FiCloud.2016.57.

Kebande, V.R. and Venter, H.S. (2018) 'Novel digital forensic readiness technique in the cloud environment', *Australian Journal of Forensic Sciences*, 50(5), pp. 552–591. Available at: https://doi.org/10.1080/00450618.2016.1267797.

Kebande, V.R. and Venter, H.S. (2019) 'A comparative analysis of Digital Forensic Readiness Models using CFRaaS as a baseline', *WIREs Forensic Science*, 1(6). Available at: https://doi.org/10.1002/wfs2.1350.

Khanna, A. and Dave, D.M. (2024) 'Enhancing Resilience in IoT Architectures for Critical IT Systems: A Comprehensive Review', *International Journal of Computer Trends and Technology*, 72(5), pp. 223–231. Available at: https://doi.org/10.14445/22312803/IJCTT-V72I5P128.

Kim, J.H. (2017) 'A Survey of IoT Security: Risks, Requirements, Trends, and Key Technologies', *Journal of Industrial Integration and Management*, 02(02), p. 1750008. Available at: https://doi.org/10.1142/S2424862217500087.

Kim, S., Park, M., Lee, S. and Kim, J. (2020) 'Smart Home Forensics—Data Analysis of IoT Devices', *Electronics 2020, Vol. 9, Page 1215*, 9(8), p. 1215. Available at: https://doi.org/10.3390/ELECTRONICS9081215.

Kumar, S., Tiwari, P. and Zymbler, M. (2019) 'Internet of Things is a revolutionary approach for future technology enhancement: a review', *Journal of Big Data*, 6(1), p. 111. Available at: https://doi.org/10.1186/s40537-019-0268-2.

Lazzez, A. and Slimani, T. (2015) 'Forensics Investigation of Web Application Security Attacks', *International Journal of Computer Network and Information Security*, 7(3), pp. 10–17. Available at: https://doi.org/10.5815/ijcnis.2015.03.02.

Leedy, P.D. and Ormrod, J.Ellis. (2001) *Practical research : planning and design*.

Lezzi, M., Lazoi, M. and Corallo, A. (2018) 'Cybersecurity for Industry 4.0 in the current literature: A reference framework', *Computers in Industry*. Elsevier B.V., pp. 97–110. Available at: https://doi.org/10.1016/j.compind.2018.09.004.

Li, J., Liang, W., Xu, Z., Jia, X. and Zhou, W. (2022) 'Service Provisioning for Multi-source IoT Applications in Mobile Edge Computing', *ACM Transactions on Sensor Networks*, 18(2), pp. 1–25. Available at: https://doi.org/10.1145/3484200.

Liepiņš, R., Bojārs, U., Grūzītis, N., Čerāns, K. and Celms, E. (2016) 'Towards Self-explanatory Ontology Visualization with Contextual Verbalization'. Available at: https://doi.org/10.1007/978-3-319-40180-5_1.

Lilli, E. (2020) 'President Obama and US cyber security policy', *Journal of Cyber Policy*, 5(2), pp. 265–284. Available at: https://doi.org/10.1080/23738871.2020.1778759.

Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M. (2016) 'Current Challenges and Future Research Areas for Digital Forensic Investigation'. Available at: http://arxiv.org/abs/1604.03850.

Lin, H. and Bergmann, N.W. (2016) 'IoT privacy and security challenges for smart home environments', *Information (Switzerland)*, 7(3). Available at: https://doi.org/10.3390/info7030044.

López Velásquez, J.M., Martínez Monterrubio, S.M., Sánchez Crespo, L.E. and Garcia Rosado, D. (2023) 'Systematic review of SIEM technology: SIEM-SC birth', *International Journal of Information Security*, 22(3), pp. 691–711. Available at: https://doi.org/10.1007/s10207-022-00657-9.

Lu, Y. (2023) 'Security and Privacy of Internet of Things: A Review of Challenges and Solutions', *Journal of Cyber Security and Mobility* [Preprint]. Available at: https://doi.org/10.13052/jcsm2245-1439.1261.

Luo, S. and Choi, T. (2022) 'E-commerce supply chains with considerations of cyber-security: Should governments play a role?', *Production and Operations Management*, 31(5), pp. 2107–2126. Available at: https://doi.org/10.1111/poms.13666.

Lyu, X., Ding, Y. and Yang, S.H. (2019) 'Safety and security risk assessment in cyberphysical systems', *IET Cyber-Physical Systems: Theory and Applications*. Institution of Engineering and Technology, pp. 221–232. Available at: https://doi.org/10.1049/iet-cps.2018.5068.

Makura, S., Venter, H.S., Kebande, V.R., Karie, N.M., Ikuesan, R.A. and Alawadi, S. (2021) 'Digital forensic readiness in operational cloud leveraging ISO / IEC 27043 guidelines on security monitoring', *Security and Privacy*, 4(3). Available at: https://doi.org/10.1002/spy2.149.

Malik, A.W., Bhatti, D.S., Park, T.-J., Ishtiaq, H.U., Ryou, J.-C. and Kim, K.-I. (2024) 'Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges', *Sensors*, 24(2), p. 433. Available at: https://doi.org/10.3390/s24020433.

Mallick, A.I. and Nath, R. (2024) 'Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments'. Available at: www.worldscientificnews.com (Accessed: 10 November 2024).

ManageEngine (2024) 'What is an incident response and 4 phases in the IR plan'. Available at: https://www.manageengine.com/products/service-desk/it-incident-management/what-is-incident-response.html (Accessed: 17 December 2024).

Manning, E. (2023) *Optimizing Incident Management Processes for Effective Cybersecurity Incident Response MSc Research Project*. Available at: https://norma.ncirl.ie/7296/ (Accessed: 21 July 2024).

Maria Jones, G., Godfrey Winster, S. and Santhosh Kumar, S.V.N. (2019) 'Analysis of Mobile Environment for Ensuring Cyber-Security in IoT-Based Digital Forensics', pp. 145–152. Available at: https://doi.org/10.1007/978-981-13-3600-3_14.

Meffert, C., Clark, D., Baggili, I. and Breitinger, F. (2017) 'Forensic state acquisition from internet of things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition', *ACM International Conference Proceeding Series*. Association for Computing Machinery. Available at: https://doi.org/10.1145/3098954.3104053.

Mhaskar, N., Alabbad, M. and Khedri, R. (2021) 'A Formal Approach to Network Segmentation', *Computers & Security*, 103, p. 102162. Available at: https://doi.org/10.1016/j.cose.2020.102162.

Mishra, A., Alzoubi, Y.I., Gill, A.Q. and Anwar, M.J. (2022) 'Cybersecurity Enterprises Policies: A Comparative Study', *Sensors*, 22(2), p. 538. Available at: https://doi.org/10.3390/s22020538.

Mouhtaropoulos, A., Li, C.-T. and Grobler, M. (2014) *Digital Forensic Readiness: Are We There Yet?*, *JICLT Journal of International Commercial Law and Technology*. Available at: http://www.cesg.gov.uk/products_services/iatp/documents/data_handling_review.pdf.

Munodawafa, F. and Awad, A.I. (2018) 'Security risk assessment within hybrid data centers: A case study of delay sensitive applications', *Journal of Information Security and Applications*, 43, pp. 61–72. Available at: https://doi.org/10.1016/j.jisa.2018.10.008.

Ngobeni, S., Venter, H. and Burke, I. (2010) *IFIP AICT 337 - A Forensic Readiness Model for Wireless Networks*.

Nik Zulkipli, N.H. and Wills, G.B. (2021) 'An Exploratory Study on Readiness Framework in IoT Forensics', *Procedia Computer Science*. Elsevier B.V., pp. 966–973. Available at: https://doi.org/10.1016/j.procs.2021.01.086.

Nugroho, H.A., Briliyant, O.C. and Sunaringtyas, S.U. (2023) 'A Novel Digital Forensic Readiness (DFR) Framework for e-Government', *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*. IEEE, pp. 184–189. Available at: https://doi.org/10.1109/ICoCICs58778.2023.10276423.

Nurse, J.R.C., Creese, S. and De Roure, D. (2017) 'Security Risk Assessment in Internet of Things Systems', *IT Professional*, 19(5), pp. 20–26. Available at: https://doi.org/10.1109/MITP.2017.3680959.

Olushola O B (2019) 'Factors affecting IoT adoption', 21(6), pp. 19–24. Available at: https://doi.org/10.9790/0661-2106011924.

Oluwasanmi Richard Arogundade (2023) 'Network Security Concepts, Dangers, and Defense Best Practical', *Computer Engineering and Intelligent Systems* [Preprint]. Available at: https://doi.org/10.7176/CEIS/14-2-03.

Oriwoh, E. and Sant, P. (2013) 'The forensics edge management system: A concept and design', *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, pp. 544–550. Available at: https://doi.org/10.1109/UIC-ATC.2013.71.

Palo Alto Metworks (2023) *What is Security Information and Event Management (SIEM) Integration?* Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-security-information-event-management-siem-integration (Accessed: 21 October 2024).

Pandey, A.K., Tripathi, A.K., Kapil, G., Singh, V., Khan, Mohd.W., Agrawal, A., Kumar, R. and Khan, R.A. (2020) 'Current Challenges of Digital Forensics in Cyber Security', pp. 31–46. Available at: https://doi.org/10.4018/978-1-7998-1558-7.ch003.

Pascucci, F., Savelli, E. and Gistri, G. (2023) 'How digital technologies reshape marketing: evidence from a qualitative investigation', *Italian Journal of Marketing* [Preprint]. Available at: https://doi.org/10.1007/s43039-023-00063-6.

Radanliev, P., Charles De Roure, D., Maple, C., Nurse, J.R.C., Nicolescu, R. and Ani, U. (2019) 'Cyber Risk in IoT Systems'. Available at: https://doi.org/10.20944/preprints201903.0104.v1.

Radouan Ait Mouha, R.A. (2021) 'Internet of Things (IoT)', *Journal of Data Analysis and Information Processing*, 09(02), pp. 77–101. Available at: https://doi.org/10.4236/jdaip.2021.92006.

Rahi, S. (2017) 'Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development', *International Journal of Economics & Management Sciences*, 06(02). Available at: https://doi.org/10.4172/2162-6359.1000403.

Rajan, R., Rana, N.P., Parameswar, N., Dhir, S., Sushil and Dwivedi, Y.K. (2021) 'Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management', *Technological Forecasting and Social Change*, 170, p. 120872. Available at: https://doi.org/10.1016/j.techfore.2021.120872.

Ravi, V., Kolla, K. and Software Engineer, S. (2022) 'International Journal of Research in IT and Management (IJRIM) International Journal of Research in IT and Management (IJRIM) A Comparative Analysis of OS Forensics Tools', 12. Available at: http://euroasiapub.orghttp://www.euroasiapub.org.

Razaque, A., Al Ajlan, A., Melaoune, N., Alotaibi, M., Alotaibi, B., Dias, I., Oad, A., Hariri, S. and Zhao, C. (2021) 'Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain-Enabled Cybersecurity Awareness System', *Applied Sciences*, 11(17), p. 7880. Available at: https://doi.org/10.3390/app11177880.

Razib, M. Al, Javeed, D., Khan, M.T., Alkanhel, R. and Muthanna, M.S.A. (2022) 'Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework', *IEEE Access*, 10, pp. 53015–53026. Available at: https://doi.org/10.1109/ACCESS.2022.3172304.

Redondi, A.E.C., Arcia-Moret, A. and Manzoni, P. (2019) 'Towards a Scaled IoT Pub/Sub Architecture for 5G Networks: the Case of Multiaccess Edge Computing'. Available at: http://arxiv.org/abs/1902.07022.

Rondeau, C.M., Temple, M.A. and Lopez, J. (2019) 'Industrial IoT cross-layer forensic investigation', *WIREs Forensic Science*, 1(1). Available at: https://doi.org/10.1002/wfs2.1322.

Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J. (2017) 'A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)', *2017 International Conference on Information Systems and Computer Science (INCISCOS)*. IEEE, pp. 253–259. Available at: https://doi.org/10.1109/INCISCOS.2017.20.

Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Jeimy J. Cano M. (2021) 'An Effective Cybersecurity Training Model to Support an Organizational Awareness Program', *Research Anthology on Artificial Intelligence Applications in Security*. IGI Global, pp. 174–188. Available at: https://doi.org/10.4018/978-1-7998-7705-9.ch008.

Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A. (2022) 'Internet of Things: Security and Solutions Survey', *Sensors*, 22(19), p. 7433. Available at: https://doi.org/10.3390/s22197433.

Sadineni, L., Pilli, E.S. and Battula, R.B. (2021) 'Ready-IoT: A Novel Forensic Readiness Model for Internet of Things', *7th IEEE World Forum on Internet of Things, WF-IoT 2021*. Institute of Electrical and Electronics Engineers Inc., pp. 89–94. Available at: https://doi.org/10.1109/WF-IoT51360.2021.9595902.

Salama, U., Yao, L. and Paik, H.Y. (2022) 'A Multilevel Collective Framework for Internet of Things Digital Forensic Investigation', *Computer*, 55(2), pp. 44–53. Available at: https://doi.org/10.1109/MC.2021.3095492.

Salayma, M. (2024) 'Risk and threat mitigation techniques in internet of things (IoT) environments: a survey', *Frontiers in the Internet of Things*, 2. Available at: https://doi.org/10.3389/friot.2023.1306018.

Santana, D., Suthaharan, S. and Mohanty, S. (2018) 'What we learn from learning - Understanding capabilities and limitations of machine learning in botnet attacks'. Available at: http://arxiv.org/abs/1805.01333.

Sarwar, K., Yongchareon, S., Yu, J. and Ur Rehman, S. (2023) 'A Survey on Privacy Preservation in Fog-Enabled Internet of Things', *ACM Computing Surveys*, 55(1), pp. 1–39. Available at: https://doi.org/10.1145/3474554.

Sato, Y., Stapleton, G., Jamnik, M., Shams, Z. and Blake, A. (2023) 'Human Visual Consistency-Checking in the Real World Ontologies', *Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC*. IEEE Computer Society, pp. 249–251. Available at: https://doi.org/10.1109/VL-HCC57772.2023.00044.

Saxena, M. (2021) *IOT DYNAMIC LOG FILE ANALYSIS: SECURITY APPROACH FOR ANOMALY DETECTION IN MULTI SENSOR ENVIRONMENT*, *International Research Journal of Modernization in Engineering Technology and Science*. Available at: www.irjmets.com.

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M. and Stiller, B. (2022) 'Landscape of IoT security', *Computer Science Review*. Elsevier Ireland Ltd. Available at: https://doi.org/10.1016/j.cosrev.2022.100467.

Servida, F. and Casey, E. (2019) 'IoT forensic challenges and opportunities for digital traces', *Digital Investigation*, 28, pp. S22–S29. Available at: https://doi.org/10.1016/j.diin.2019.01.012.

Sgurev, V., IEEE Systems, M., Institute of Electrical and Electronics Engineers. Bulgaria Section. IM/CS/SMC Joint Chapter, Institute of Electrical and Electronics Engineers. Bulgaria Section. CIS Chapter and Institute of Electrical and Electronics Engineers (no date) *2020 IEEE 10th International Conference on Intelligent Systems (IS) : proceedings*.

Shah, I.A., Malik, F.A. and Ahmad, S.A. (2016) 'Enhancing security in IoT based Home automation using Reed Solomon Codes', *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, pp. 1639–1642. Available at: https://doi.org/10.1109/WiSPNET.2016.7566417.

Shah, Mohammad, Shah, Mohd, Leau, Y.-B., Anbar, M. and Bin-Salem, A. (2023) 'Security and Integrity Attacks in Named Data Networking: A Survey'. Available at: https://doi.org/10.1109/ACCESS.2021.DOI.

Shancang Li and Li Da Xu (2017) *Securing the Internet of Things*.

Sharma, B.K., Joseph, M.A., Jacob, B. and Miranda, B. (2019) 'Emerging trends in Digital Forensic and Cyber security- An Overview', *2019 Sixth HCT Information Technology Trends (ITT)*. IEEE, pp. 309–313. Available at: https://doi.org/10.1109/ITT48889.2019.9075101.

Singh, A., Ikuesan, A.R. and Venter, H.S. (2019) 'Digital Forensic Readiness Framework for Ransomware Investigation', *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*. Springer Verlag, pp. 91–105. Available at: https://doi.org/10.1007/978-3-030-05487-8_5.

Singh Kumar Shanu, Irfan Annie and Dayal Neelam (2019) *Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks*. IEEE.

Singh, N., Buyya, R. and Kim, H. (2024) 'Securing Cloud-Based Internet of Things: Challenges and Mitigations'. Available at: http://arxiv.org/abs/2402.00356.

Sneesl, R., Jusoh, Y.Y., Jabar, M.A., Abdullah, S. and Bukar, U.A. (2022) 'Factors Affecting the Adoption of IoT-Based Smart Campus: An Investigation Using Analytical Hierarchical Process (AHP)', *Sustainability*, 14(14), p. 8359. Available at: https://doi.org/10.3390/su14148359.

Soltani, S. and Seno, S.A.H. (2019) 'A formal model for event reconstruction in digital forensic investigation', *Digital Investigation*, 30, pp. 148–160. Available at: https://doi.org/10.1016/j.diin.2019.07.006.

Soltani, S., Seno, S.A.H. and Yazdi, H.S. (2019) 'Event reconstruction using temporal pattern of file system modification', *IET Information Security*, 13(3), pp. 201–212. Available at: https://doi.org/10.1049/iet-ifs.2018.5209.

Soni, N. (2024) 'IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem', *Computer and Telecommunication Engineering*, 2(4), p. 3070. Available at: https://doi.org/10.54517/cte3070.

SPEAR Project (2021) 'Forensic Readiness in Critical Infrastructures - SPEAR Project'. Available at: https://www.spear2020.eu/News/Details?id=123 (Accessed: 13 May 2023).

Štitilis, D., Pakutinskas, P. and Malinauskaitė, I. (2017) 'EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis', *Security Journal*, 30(4), pp. 1151–1168. Available at: https://doi.org/10.1057/s41284-016-0083-9.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K. (2020) 'A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues', *IEEE Communications Surveys and Tutorials*. Institute of Electrical and Electronics Engineers Inc., pp. 1191–1221. Available at: https://doi.org/10.1109/COMST.2019.2962586.

Sun, X., Ansari, N. and Wang, R. (2016) 'Optimizing Resource Utilization of a Data Center', *IEEE Communications Surveys and Tutorials*. Institute of Electrical and Electronics Engineers Inc., pp. 2822–2846. Available at: https://doi.org/10.1109/COMST.2016.2558203.

Surange Geetanjali and Khatri Pallavi (no date) 'IoT Forensics: A Review on Current Trends, Approaches and Foreseen Challenges', *2021*.

Tabassum, A. and Lebda, W. (2019) 'Security Framework for IoT Devices against Cyber-attacks', *6th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2019)*. Aircc Publishing Corporation, pp. 249–266. Available at: https://doi.org/10.5121/csit.2019.91321.

Teixeira, J.E. and Tavares-Lehmann, A.T.C.P. (2022) 'Industry 4.0 in the European union: Policies and national strategies', *Technological Forecasting and Social Change*, 180, p. 121664. Available at: https://doi.org/10.1016/j.techfore.2022.121664.

Umar, F. (2023) *Cyber-physical security: AI methods for malware/cyber-attacks detection on embedded/IoT applications Candidate Umar Farooq*. Available at: https://webthesis.biblio.polito.it/29544/ (Accessed: 21 October 2024).

Vailshery Lionel Sujay (2022) *Global IoT and non-IoT connections 2010-2025 | Statista*. Available at: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (Accessed: 15 March 2023).

Do Valle, J.M., Souza, G., Fidelis, S., Araujo, A., Cacho, N., Silva, I., Budke, J., Sales, H., Filgueira, M.W., Lopes, F., Araujo, D. and Silva Junior, R. (2020) 'Big Data Platform for Analysing Crime Evidences', *Proceedings - 2020 IEEE 6th International Conference on Big Data Computing Service and Applications, BigDataService 2020*. Institute of Electrical and Electronics Engineers Inc., pp. 113–119. Available at: https://doi.org/10.1109/BigDataService49289.2020.00025.

Vig, V. (2023) *Intelligent IoT Gateway and it's Importance in Today's Connected World.* Available at: https://www.vvdntech.com/blog/intelligent-iot-gateway-and-its-importance-in-todays-connected-world/ (Accessed: 21 January 2024).

Vincze, E.A. (2016) 'Challenges in digital forensics', *Police Practice and Research*, 17(2), pp. 183–194. Available at: https://doi.org/10.1080/15614263.2015.1128163.

Vishwakarma, N.K., Singh, R.K. and Sharma, R.R.K. (2019) 'Internet of things architectures: do organizational strategies matters?', *Business Process Management Journal*, 26(1), pp. 102–131. Available at: https://doi.org/10.1108/BPMJ-03-2018-0092.

Vitorino, J., Silva, M., Maia, E. and Praça, I. (2024) *An Adversarial Robustness Benchmark for Enterprise Network Intrusion Detection*.

Wang, M., Jayaraman, P.P., Ranjan, R., Mitra, K., Zhang, M., Li, E., Khan, S., Pathan, M. and Georgeakopoulos, D. (2015) 'An Overview of Cloud Based Content Delivery Networks: Research Dimensions and State-of-the-Art', pp. 131–158. Available at: https://doi.org/10.1007/978-3-662-46703-9_6.

Wang, R., Bush-Evans, R., Arden-Close, E., Bolat, E., McAlaney, J., Hodge, S., Thomas, S. and Phalp, K. (2023) 'Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications', *Computers in Human Behavior*, 139, p. 107545. Available at: https://doi.org/10.1016/j.chb.2022.107545.

Wazid, M., Katal, A., Goudar, R.H. and Rao, S. (2013) 'Hacktivism trends, digital forensic tools and challenges: A survey', *2013 IEEE CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGIES*. IEEE, pp. 138–144. Available at: https://doi.org/10.1109/CICT.2013.6558078.

Wazuh Inc. (2024) 'Installation guide · Wazuh documentation'. Available at: https://documentation.wazuh.com/current/installation-guide/ (Accessed: 2 April 2024).

Williams, C. (2007) *Research Methods*, *Journal of Business & Economic Research-March*.

Williams, M.D. and Douglass, R. (2022) 'Ensuring the Security of Defense IoT Through Automatic Code Generation', *IoT for Defense and National Security*. Wiley, pp. 307–323. Available at: https://doi.org/10.1002/9781119892199.ch16.

Yang, W., Johnstone, M.N., Sikos, L.F. and Wang, S. (2020) 'Security and Forensics in the Internet of Things: Research Advances and Challenges', *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*. IEEE, pp. 12–17. Available at: https://doi.org/10.1109/ETSecIoT50046.2020.00007.

Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.M.A. and Hong, C.S. (2019) 'Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges', *Future Generation Computer Systems*, 92, pp. 265–275. Available at: https://doi.org/10.1016/j.future.2018.09.058.

Yun, J. and Won, K.-H. (2012) 'Building Environment Analysis Based on Temperature and Humidity for Smart Energy Systems', *Sensors*, 12(10), pp. 13458–13470. Available at: https://doi.org/10.3390/s121013458.

Zainudin, N.M., Hasbullah, N.A., Wook, M., Ramli, S., Afiza, N. and Razali, M. (2022) *Digital Forensic Readiness for Cyber Security Practitioners: An Integrated Model*, *Journal of Positive School Psychology*. Available at: http://journalppw.com.

Zawoad, S. and Hasan, R. (2015) 'FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things', *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*. Institute of Electrical and Electronics Engineers Inc., pp. 279–284. Available at: https://doi.org/10.1109/SCC.2015.46.

Zawoad, S., Hasan, R. and Skjellum, A. (2015) 'OCF: An Open Cloud Forensics Model for Reliable Digital Forensics', *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*. Institute of Electrical and Electronics Engineers Inc., pp. 437–444. Available at: https://doi.org/10.1109/CLOUD.2015.65.

Zia, T., Liu, P. and Han, W. (2017) 'Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)', *Proceedings of the 12th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, pp. 1–7. Available at: https://doi.org/10.1145/3098954.3104052.

Žukauskas, P., Vveinhardt, J. and Andriukaitienė, R. (2018) 'Philosophy and Paradigm of Scientific Research', *Management Culture and Corporate Social Responsibility*. InTech. Available at: https://doi.org/10.5772/intechopen.70628.

Appendix A

A.1 Experimental Tools

Figure A.1 Front View of the Experiment PCs / Servers racked in the Data Centre

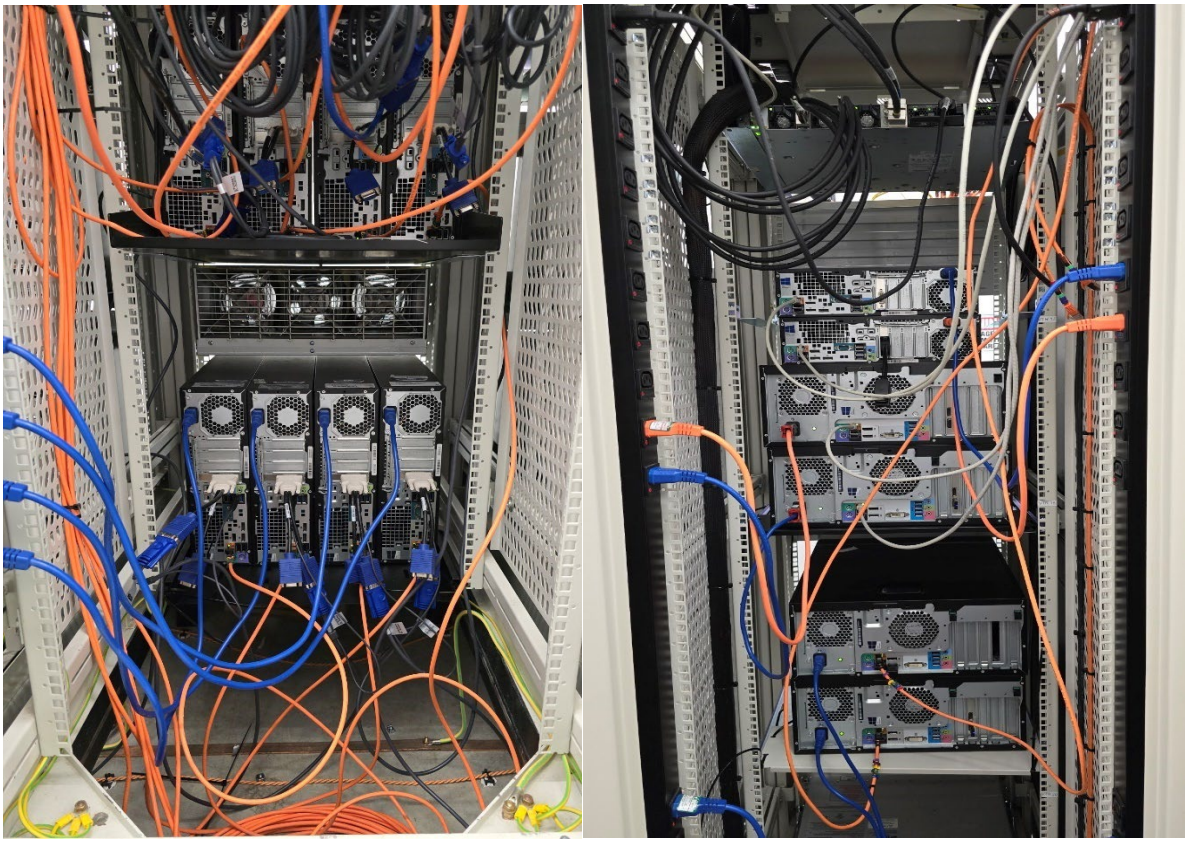

Figure A.2: Rear View of the Experiment PCs / Servers racked in the Data Centre

Utilising Splunk for Digital Forensic Analysis

Any aspiring digital forensic professional will readily recognise that Splunk is not the primary forensic tool for analysing seized hard drive images, given the availability of more advanced computer forensic tools. It is the preferred tool for analysing logs related to events. From an attacker hacking into the system to gaining full control, exploiting a vulnerability, and potential data exfiltration, Splunk can handle it all. It is a formidable tool, both for its advantages and disadvantages. It is crucial that businesses can address a malware incident as it occurs and then initiate automated, proactive responses. Moreover, it reduces the need for manual intervention, enhances automation for best practices to prevent future issues, and generally saves time in the long term (González-Granadillo, González-Zarzosa and Diaz, 2021).

Splunk is renowned in cybersecurity for its log management capabilities. It is used in many Security Operations Centres (SOCs) worldwide and by numerous IT personnel to protect networks and keep systems fully operational. Splunk's extensive features and functionalities make it an ideal tool for digital forensic analysis. It can normalise machine data from various sources, store file data as "blobs" (binary large objects), and allow for pivoting and drill-down analysis.

Although Splunk is not a replacement for the traditional forensic toolset, using it for expert forensic analysis can be invaluable. Combining ease of use with Splunk's ability to understand and parse various logs and data feeds creates a powerful way to quickly analyse multiple elements within an incident. Splunk can also help access data across an operational enterprise environment, even if the data has not been previously recognised as a typical forensic data source. We can also integrate multiple log data sources as needed, which is especially impressive given that the default data input source is usually an indexed log format. A benefit of this flexibility and rich data analysis is the ability to spot and identify attackers as they attempt to move from system to system. Note, however, that this approach is better suited to real-time, present-day analysis of an environment after the logs have been indexed and collected.

Installing and Configuring Splunk for Forensic Analysis

Two Splunk editions are available: the free and enterprise editions. Before downloading and installing Splunk, ensure you have a Linux or Windows operating system, and that your hardware supports 64-bit x86 architecture and 2GB of RAM. Once you confirm the system requirements are suitable for running Splunk on Windows, download the .msi file from Splunk's website and proceed with installation. The steps below outline how to install Splunk on the machine at 192.168.0.10.

1. Download Splunk Enterprise 9.2.1 from https://www.splunk.com/en_us/download/splunk-enterprise.html.
2. Once the setup file is downloaded, run the .msi file to install Splunk.
3. Follow the instructions to choose the desired options.
4. After installing and setting a password, Splunk can be accessed via the Splunk web interface, which is on port 8000 by default.

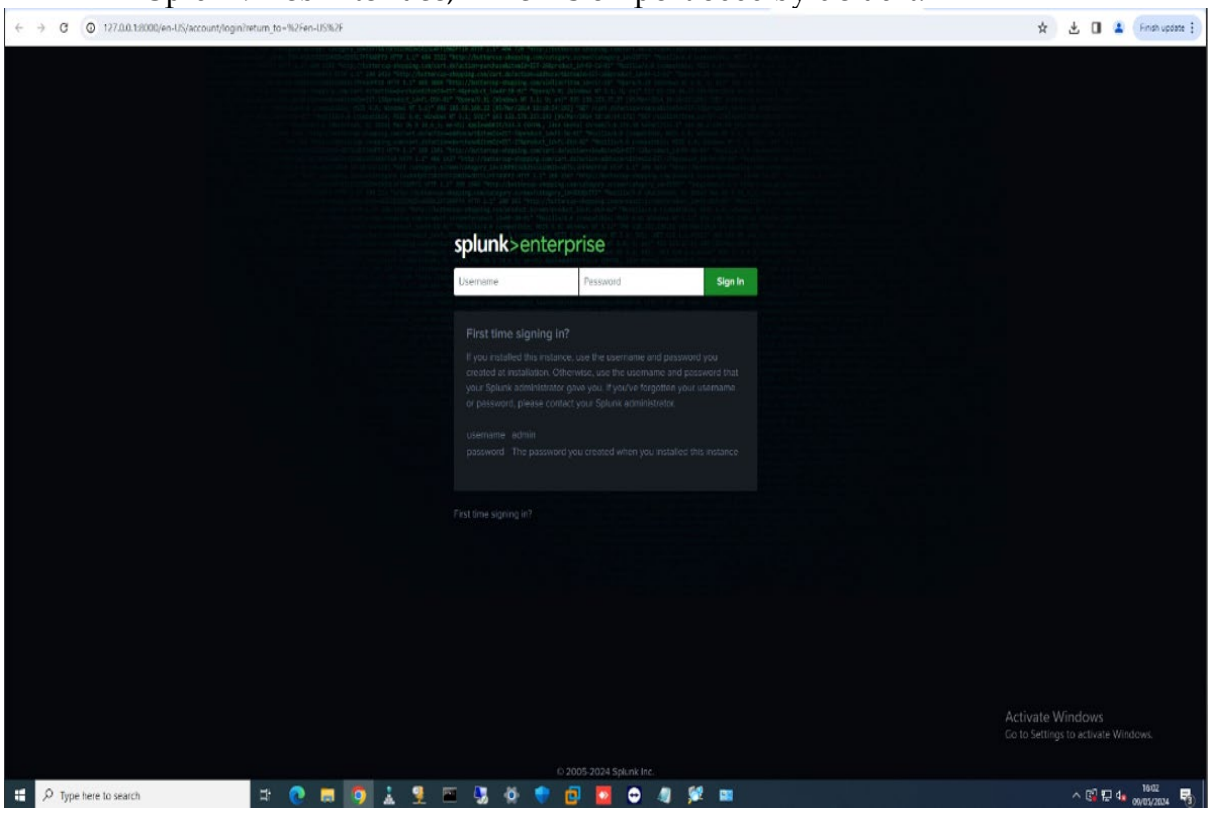

Figure A.3: Accessing Splunk Via Web Interface

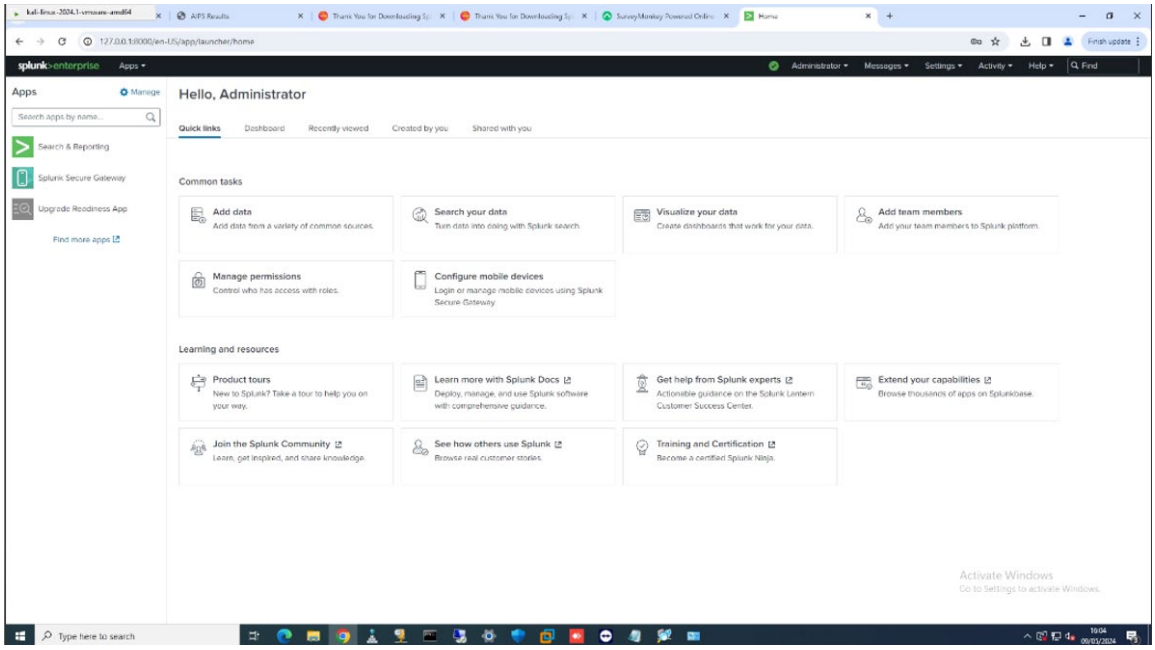

Figure A.4: Splunk Dashboard After Login

Appendix B

B.1 Experimental Configuration and Screenshots

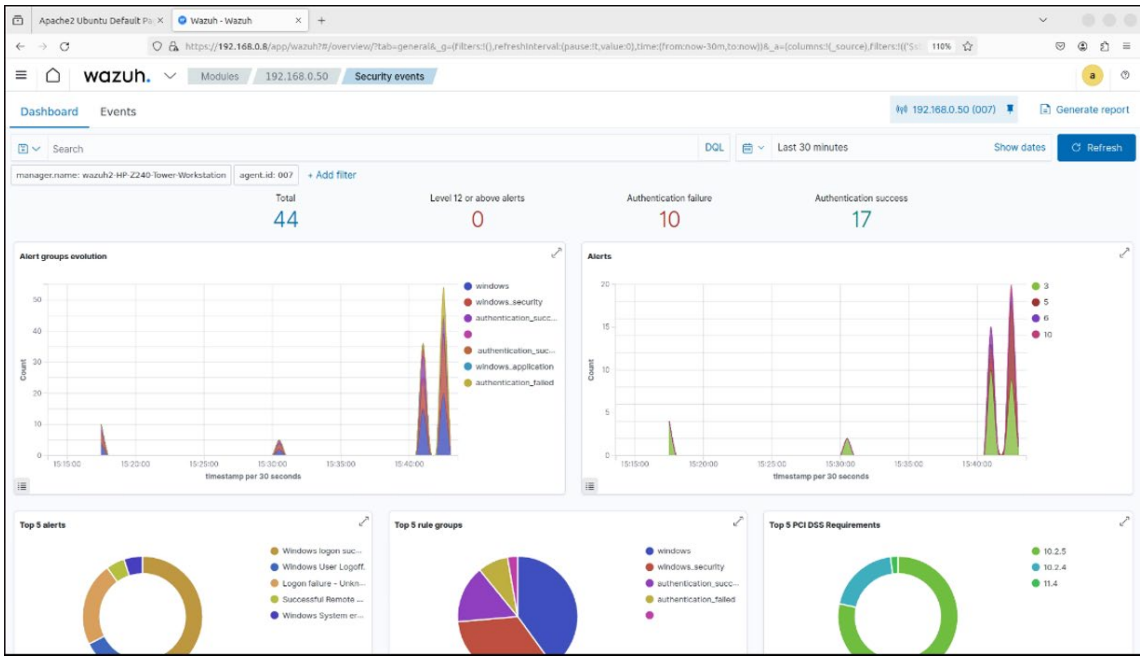

Figure B.1: View of Security Events on the Wazuh Dashboard

Scenario - Detecting and Forensic Investigation of File Integrity Monitoring (FIM) Process

File Integrity Monitoring (FIM) is an integrated security device and system that monitors, measures, and evaluates potential changes to computers, servers, routers, switches, and other network devices. Checking the systems against known-good baseline measures prevents and quantifies unauthorised changes over time. FIM enables real-time and after-the-fact monitoring of files, including local files, OS files, database files, and all other organisations' security device files. Using File Integrity Monitoring logs, it is easy to perform forensic analysis (Shah et al., 2023).

Conducting Forensic Analysis through File Auditing involves several steps. To enable auditing on the Windows Wazuh client machine and perform a forensic investigation, follow the steps below.

Step 1: Enable File Auditing using Local Group Policy Editor (192.168.0.10)

Windows defaults to disabling file auditing features. To enable the feature, you must set up specific group policies to ensure it is available.

Here are the steps:

1. Open Start -> Run, type "gpedit.msc" and press OK.
2. The command will open the Group Policy Editor.
3. Select "Local Computer Policy" > Windows Settings > Advanced Audit Policy Configuration > Object Access.

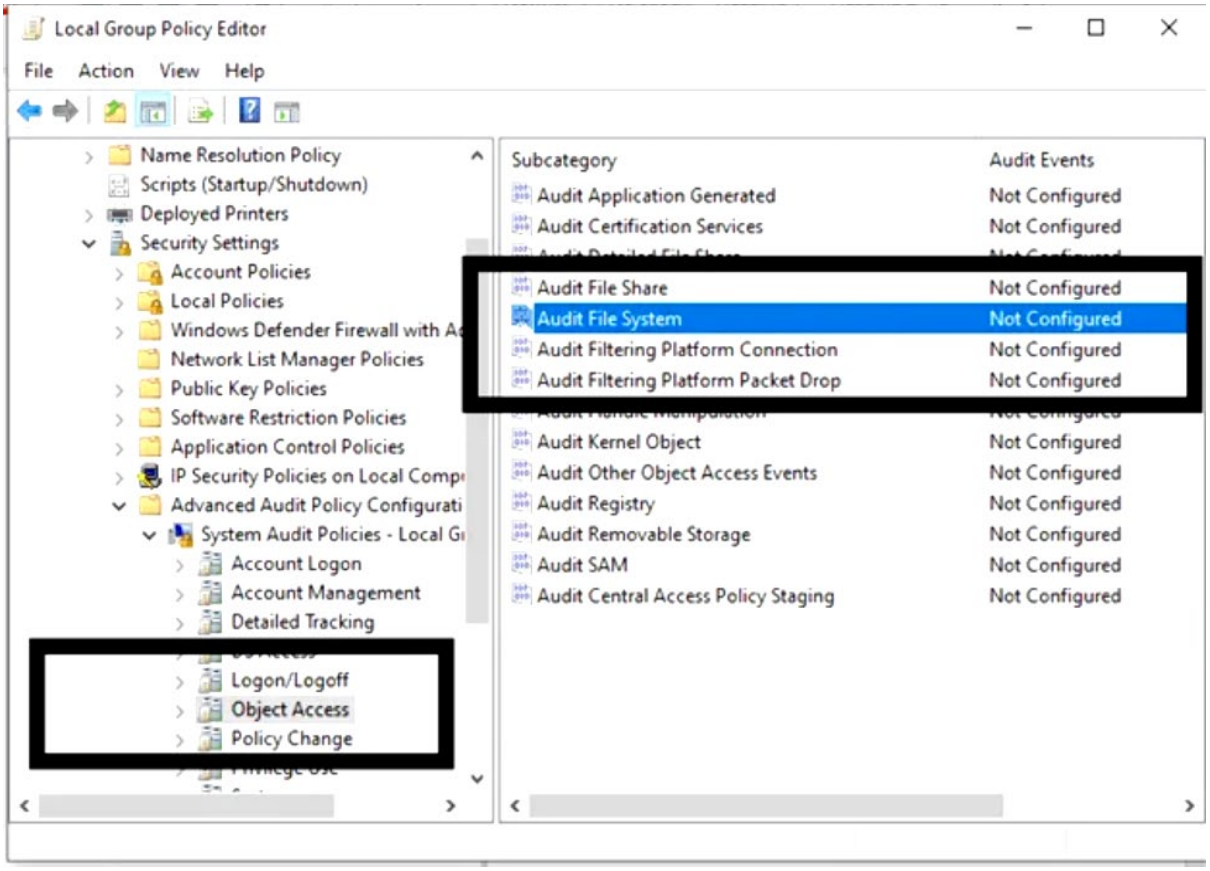

Figure B.2: Local Group Policy Editor

4. Open the Audit File System from the list of subcategories.
5. In the audit file system properties window, check to configure the following audit events and select both Success and Failure.

6. Select Apply and OK, then close the window. After this step, the feature is enabled on your server.

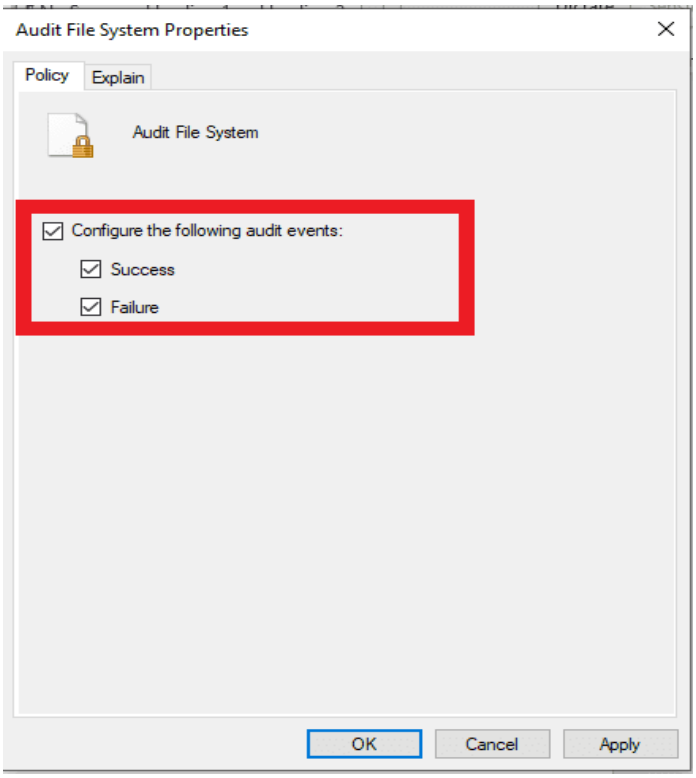

Figure B.3: Audit File System Properties

Step 2: Configure the Desired Folder to Start Auditing

After we have enabled the auditing feature on a folder, it is time to start adding the rule. Let's consider putting it in the first folder, per our folder structure.

1. Open My Computer -> Go to Drive and Select Program Files (x86).
2. Right-click on the desired folder and select properties.
3. In the properties window, select Security and then select Advanced
4. In the "Advanced Security Settings" folder, select the Auditing Tab and click Continue.

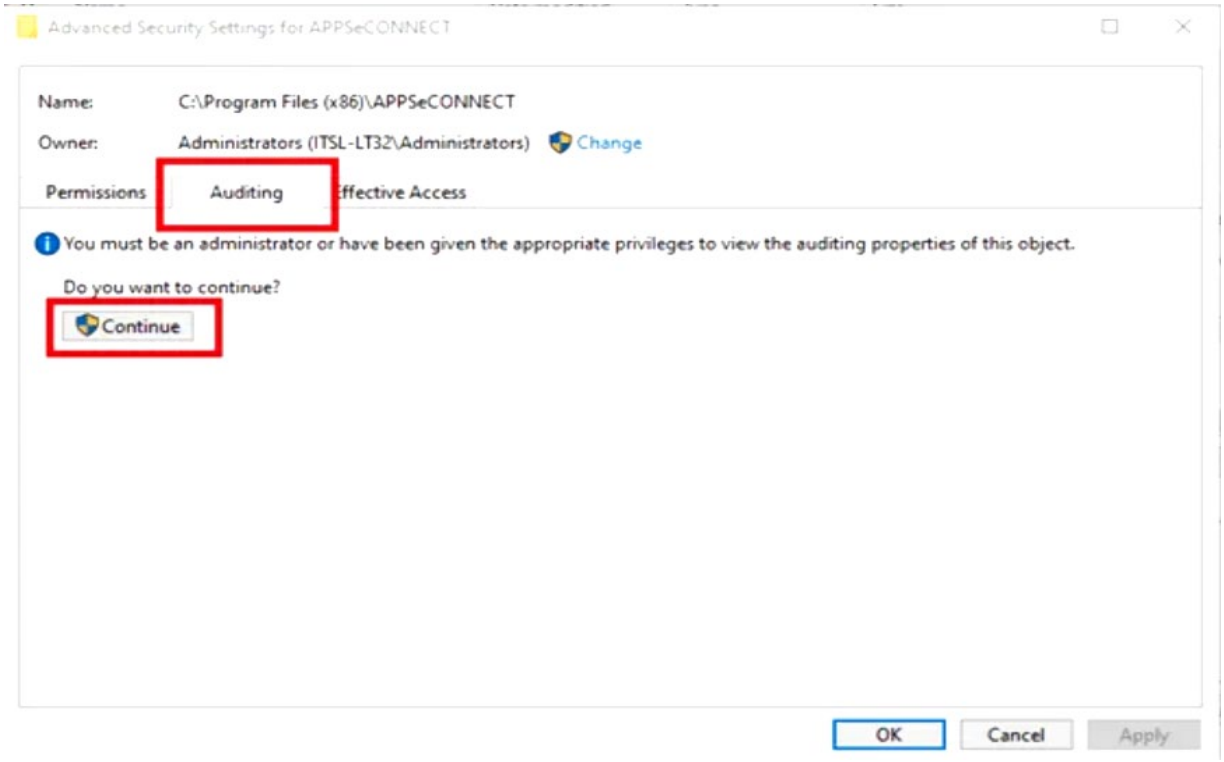

Figure B.4: Advanced Security Settings - Auditing

5. Select "Add" to add a new policy.
6. Select Principle and type in "Everyone" in the window. After you type Everyone, click the "Check Name" button to ensure it is selected correctly.
7. Once selected, click on "Show Advanced Options" and select "Delete subfolders and files" and "Delete" options.
8. Once you select these two options, you can press OK and apply the changes. Your folder will now be audited for deletions.

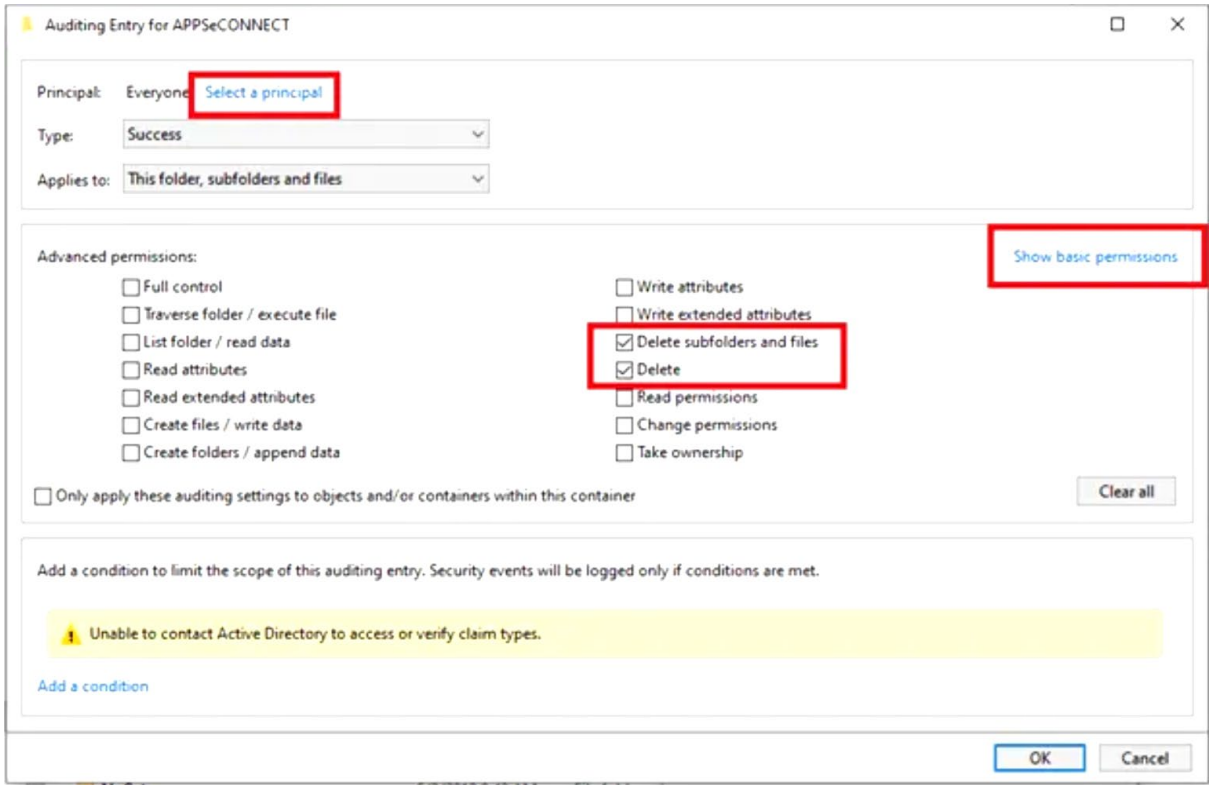

Figure B.5: Advanced Options - Auditing Entry

Step 3: Configure Windows Wazuh Agent

To monitor the desired folder for possible deletion of files. To achieve this task, you can leverage the File Integrity Monitoring component of Wazuh

1. Please edit the Wazuh agent configuration file

   C:\Program Files (x86)\ossec-agent\ossec.conf

   and add the folder to be monitored.

2. This should be within the <syscheck> block. The configuration should look like this:

<directories whodata="yes">C:\Users\administrator\Downloads</directories >

3. Restart the agent after applying the configuration
4. A default rule on the Wazuh server sends alerts when a file is deleted.

Step 4: Configure Linux Wazuh Server

Configure Linux Wazuh Server (192.168.0.8)

1. Add the following rule to the /var/ossec/etc/rules/local_rules.xml file on the Wazuh server. The rules detect file deletion events in the monitored directory and also fire an alert when files are deleted in the monitored folder

```
<group name= "syscheck,">

  <rule id="100050" level="7">

    <if_sid>553</if_sid>

    <field name="file">C:\\Users\\administrator\\Downloads</field>

    <description>File deleted in C:\Users\administrator\Downloads
directory.</description>

  </rule>
```

2. Restart the Wazuh server after adding the rule

Note: Please replace C:\Users\administrator\Downloads on both the Wazuh agent and server with the path of the accounting directory

3. From the Wazuh server, click home, then click agents, and click 192.168.0.10 to see all the events that occurred in the last 15 minutes. You can see below that the Wazuh server can identify and provide evidence of FIM-occurred events.

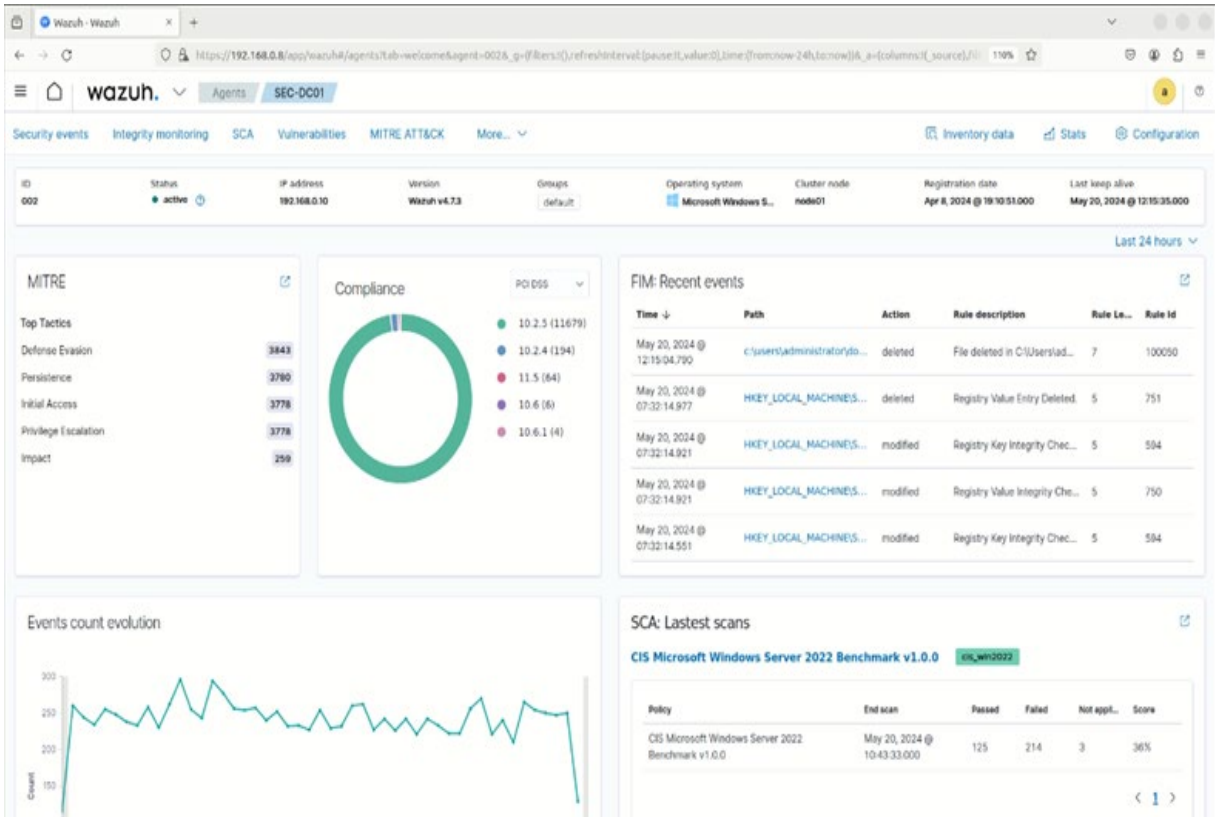

Figure B.6: Evidence of FIM Occurred Events on Wazuh Dashboard

Step 5: Forensic Evidence Event Viewer Log Analysis (192.168.0.10)

The best part of this exercise is that you can check the logs.

1. Open Start -> Run, select "Event Viewer" and click OK.
2. Open Windows Logs -> Security.
3. Using the filter menu, you can identify deleted entries by filtering out the File System Category with Event ID 4663.
4. In the entry, you will see which object was deleted and which executable deleted it. If you see "explorer.exe," it means someone manually deleted the file.
5. You can also identify the logged-in user who deleted the file.

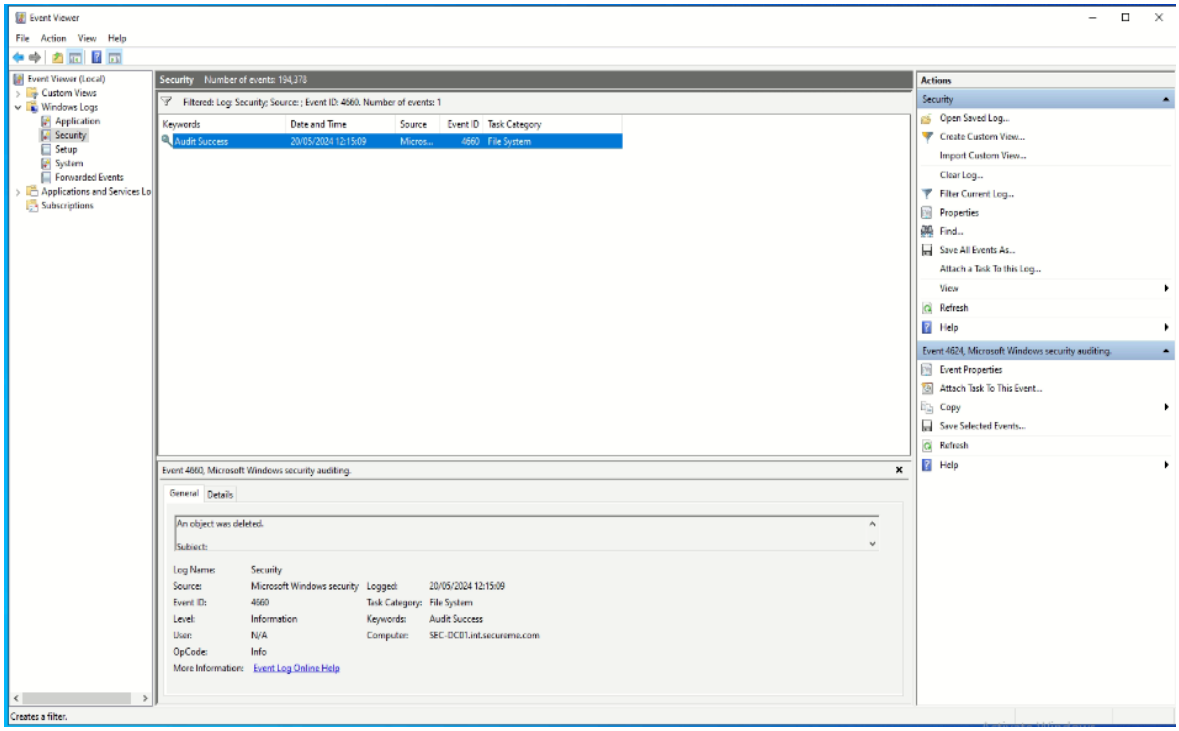

Figure B.7: File System Category with Event ID 4663

Step 6: Extracting Logs for Forensic Investigation from Event Viewer at 192.168.0.10

The following shows the log extraction process from the victim machine via Event Viewer.

1. Click on Start – Run
2. Type in – eventvwr and click ok.
3. To execute the event viewer, we are going to select Windows Log and then Security, as we are only concerned about the network events:

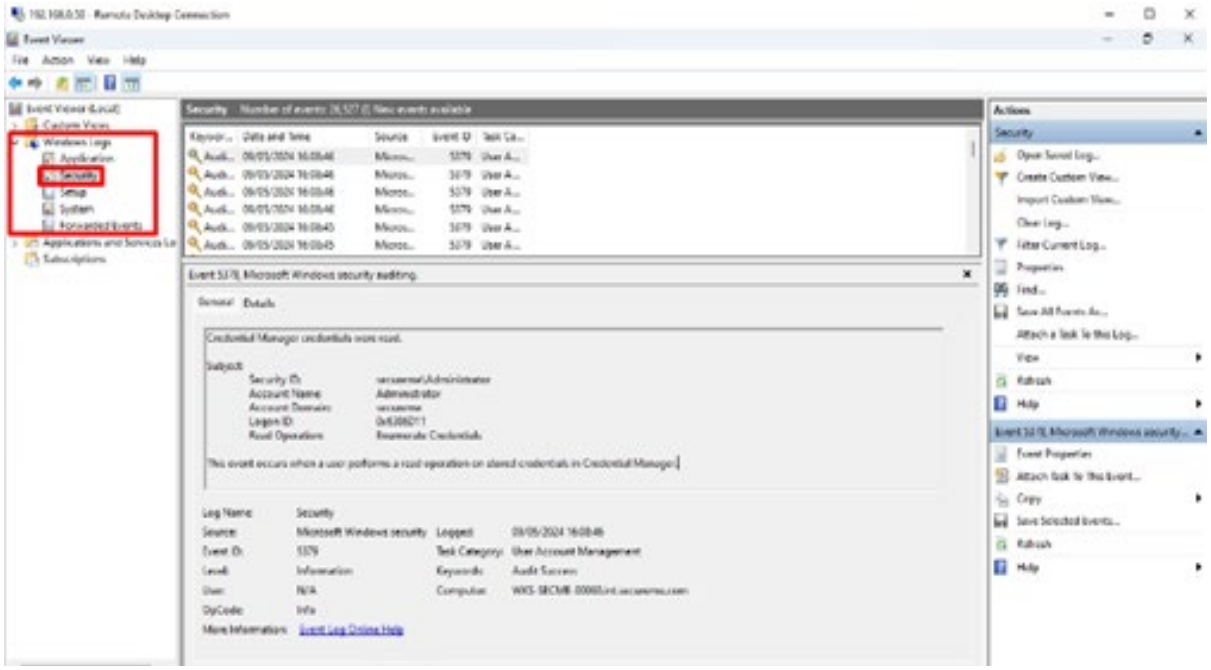

Figure B.8: Event Viewer - Windows Log

4. Then save the event logs.

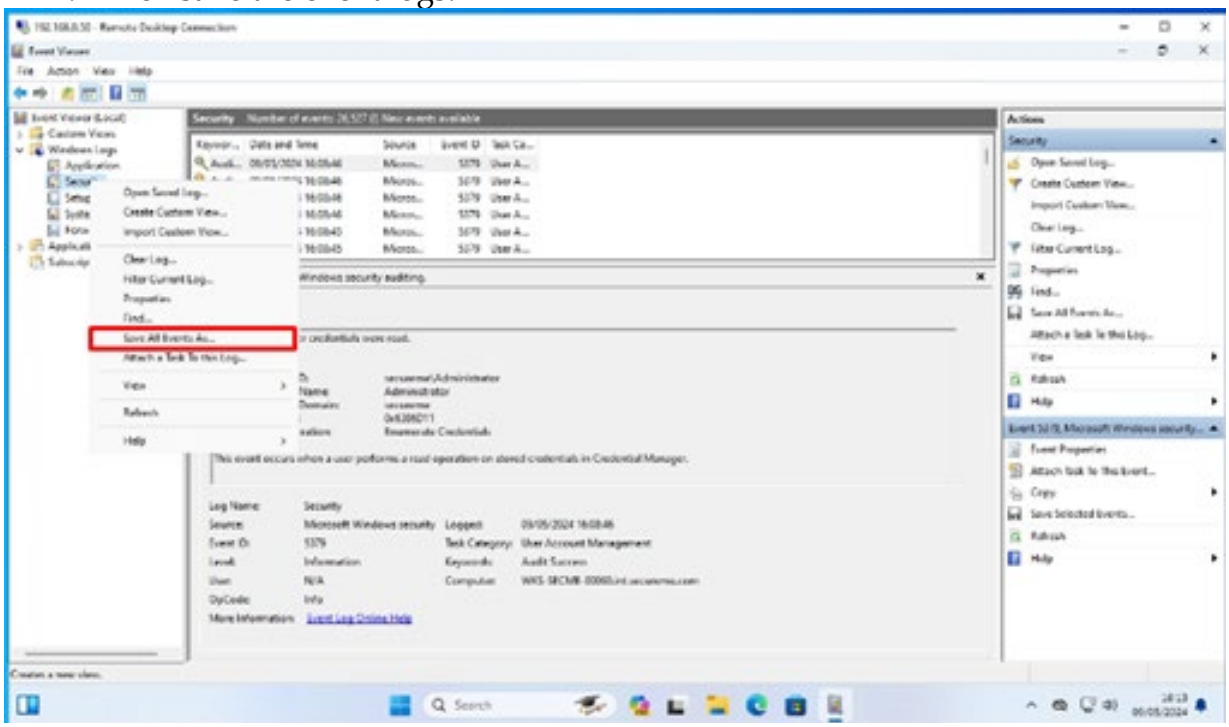

Figure B.9: Event Viewer - Save Logs

5. The extracted logs from the event viewer are saved on the desktop, or you can choose any path you want.
6. Filtering the log using Splunk, we have used a query that filters all the logs of FIM file deletion attempts:

   sourcetype= WinEventLog: Security (EventCode=4660)

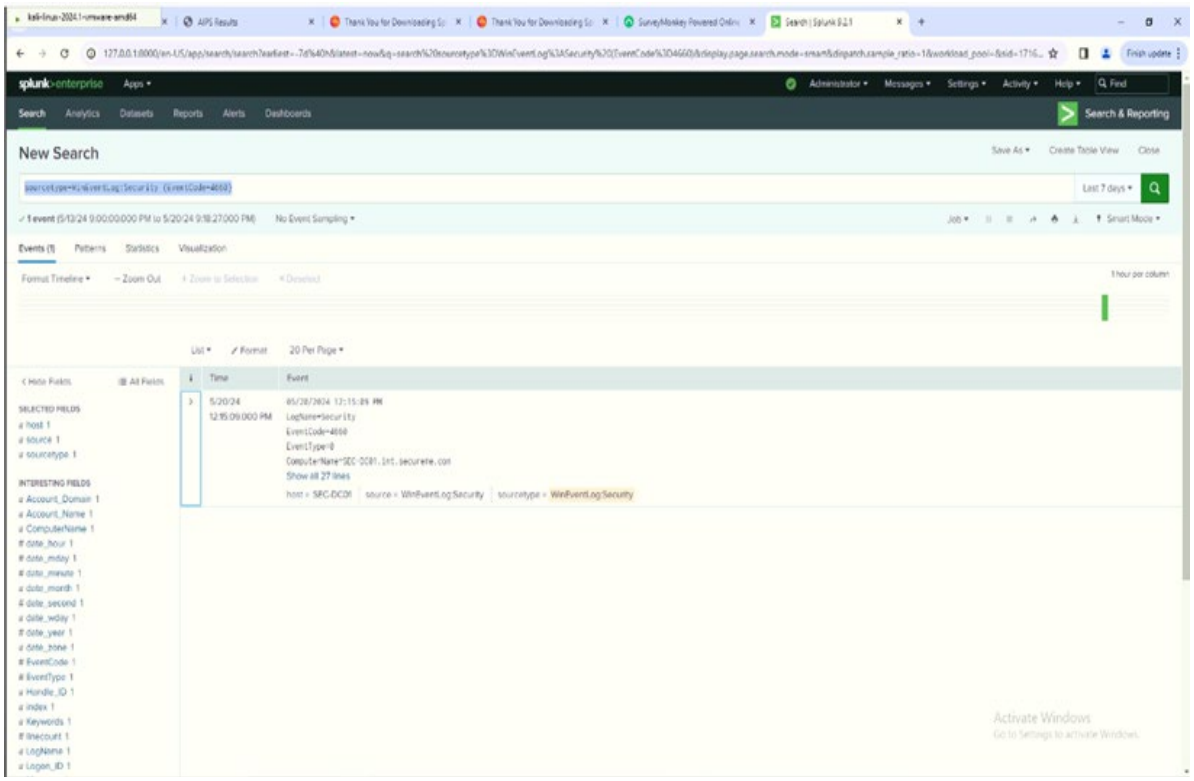

Figure B.10: Filtering the log using Splunk

7. Further forensic evidence using Splunk is shown in the figure below.

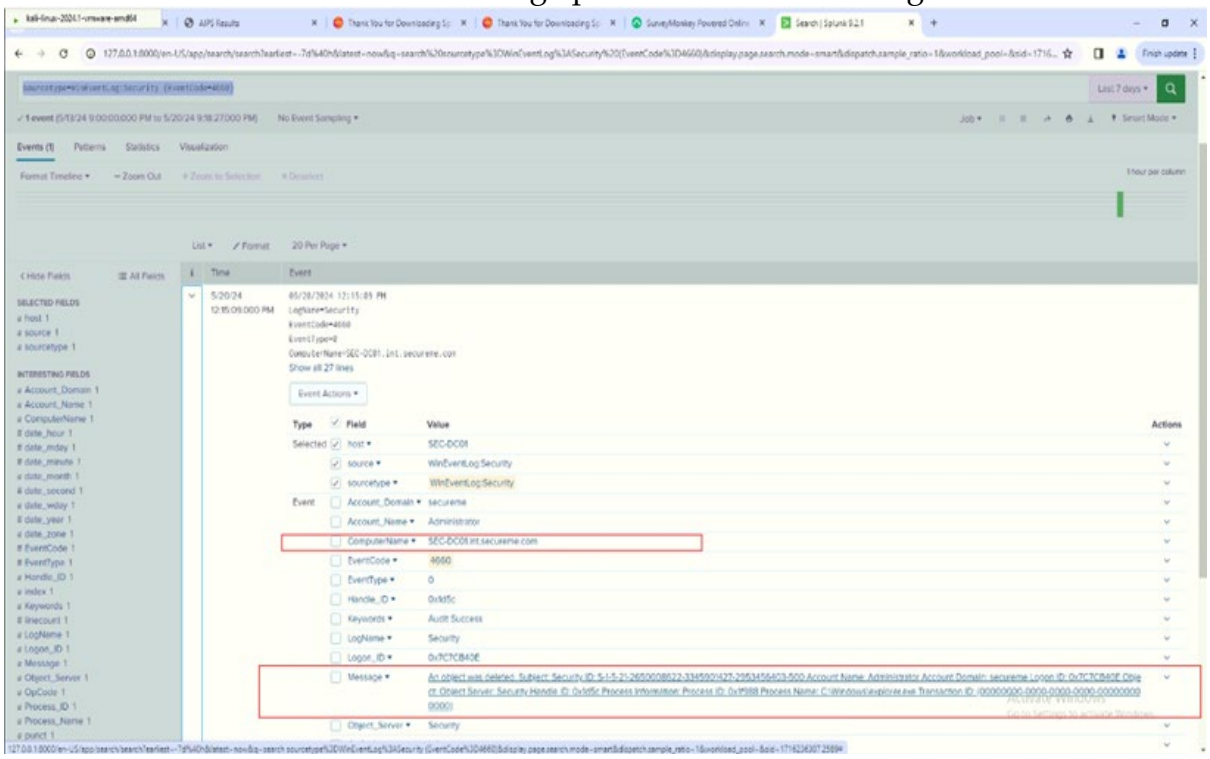

Figure B.11: Forensic Evidence using Splunk

Scenario - Detecting Unauthorised Processes at Wazuh and Forensic Analysis

The Wazuh command monitoring capability runs commands on an endpoint and monitors their output. In this scenario, you use the Wazuh command monitoring capability to detect when Netcat runs on an Ubuntu endpoint. Netcat is a computer networking utility used for port scanning and port listening.

Table B.1: Infrastructure for Unauthorised Processes

Endpoint	Description
WAZUH Client Ubuntu 22.04 192.168.0.9	You configure the Wazuh command monitoring module on this endpoint to detect a running Netcat process.
WAZUH Server 192.168.0.8	WAZUH Server will identify that a malicious process is opening a port which any attacker can exploit

Attack Scenario: Introduction to NetCat

NetCat, often called the "Swiss Army Knife" of networking, is a versatile command-line utility used for reading, writing, redirecting, and performing various other operations on network connections. Developed by Hobbit in 1995, NetCat is renowned for its simplicity and wide range of features, making it an essential tool for network administrators, security professionals, and hackers alike.

The following shows the usage of NetCat as a malicious process at UBUNTU (192.168.0.9):

Install NetCat:

sudo apt install ncat nmap -y

Basic Syntax:

The basic syntax for NetCat commands is:

nc [options] [hostname] [port]

Common Options:

- **-l**: Listen mode, for inbound connections.
- **-p**: Local port number (used with **-l**).

- **-v**: Verbose mode, providing more detailed output.
- **-e**: Executes a program after the connection is established.
- **-z**: Zero-I/O mode, useful for scanning.
- **-n**: Numeric-only IP addresses (no DNS resolution).

Security Considerations:

While NetCat is powerful and versatile, it also poses security risks if used **maliciously**. Attackers can use it to set up backdoors, transfer files illicitly, or scan networks stealthily. Therefore, network administrators should monitor NetCat usage and ensure that their systems are secured against unauthorised access.

Usage of NC.exe, a NetCat Command:

Execute nc.exe to run a malicious process as follows:

nc -l 8000

This is shown below as evidence:

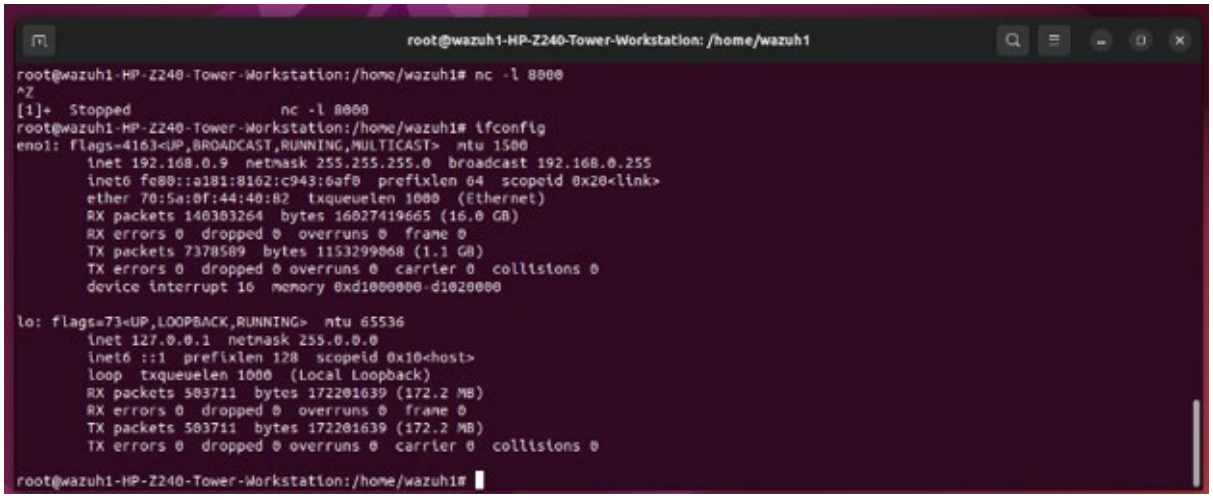

Figure B.12: Execution of nc.exe to Run a Malicious Process

Wazuh Configurations for Detecting Unauthorised Processes on Ubuntu Endpoint

Take the following steps to configure command monitoring and query a list of all running processes on the Ubuntu endpoint.

1. Add the following configuration block to the Wazuh agent /var/ossec/etc/ossec.conf file. This allows us to get a list of running processes periodically:

```
<ossec_config>
        <localfile>
          <log_format>full_command</log_format>
           <alias>process list</alias>
          <command>ps -e -o pid,uname, command</command>
          <frequency>30</frequency>
        </localfile>
</ossec_config>
```

2. Restart the Wazuh agent to apply the changes:

   sudo systemctl restart wazuh-agent

3. Install Netcat and the required dependencies:

   sudo apt install ncat nmap -y

You must follow the steps below on the Wazuh server to create a rule that triggers whenever the Netcat program launches.

1. Add the following rules to the /var/ossec/etc/rules/local_rules.xml file on the Wazuh server:

```
<group name="ossec,">
 <rule id="100050" level="0">
  <if_sid>530</if_sid>
  <match>^ossec: output: 'process list'</match>
  <description>List of running processes.</description>
  <group>process_monitor,</group>
 </rule>

 <rule id="100051" level="7" ignore="900">
  <if_sid>100050</if_sid>
  <match>nc -l</match>
  <description>netcat listening for incoming connections.</description>
  <group>process_monitor,</group>
 </rule>
</group>
```

2. Restart the Wazuh manager to apply the changes:

sudo systemctl restart wazuh-manager

Wazuh Detection of Unauthorised Processes

You can visualise the alert data in the Wazuh dashboard. To do this, go to the Security Events module and add filters to the search bar to query the alerts.

- rule.id:(100051)

or

- rule.id:(533)

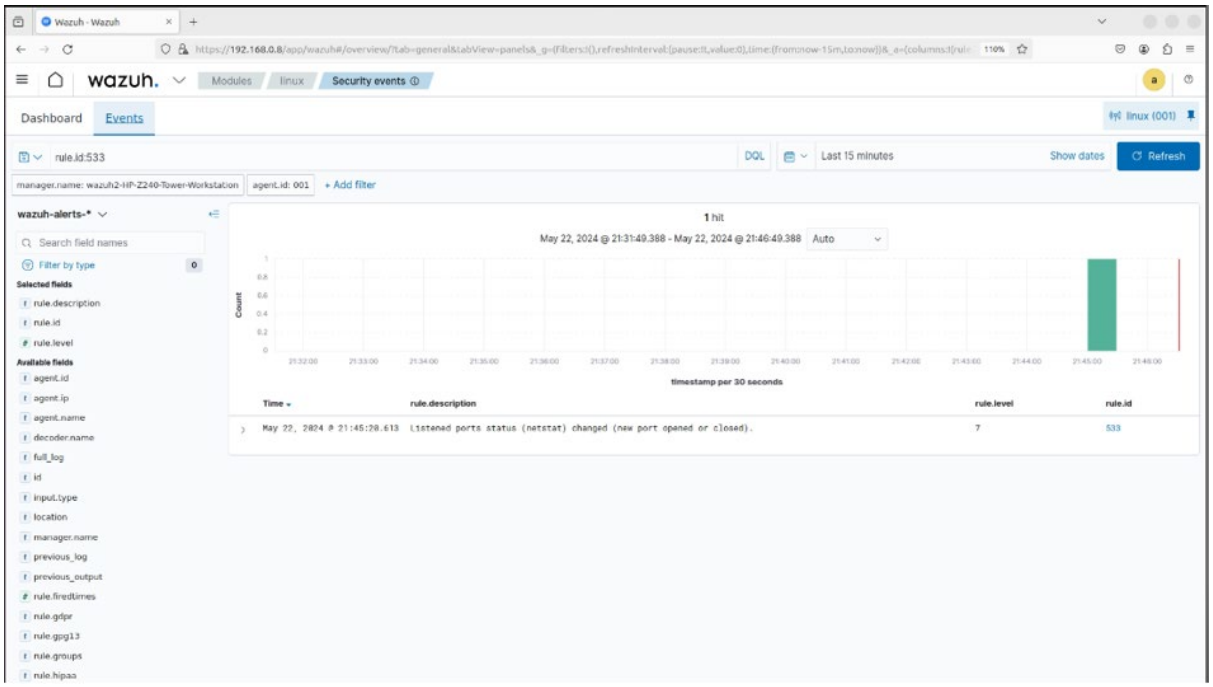

Figure B.13: Security Filters in the Search Bar to Query Alerts

To see more details, expand the log entry as follows:

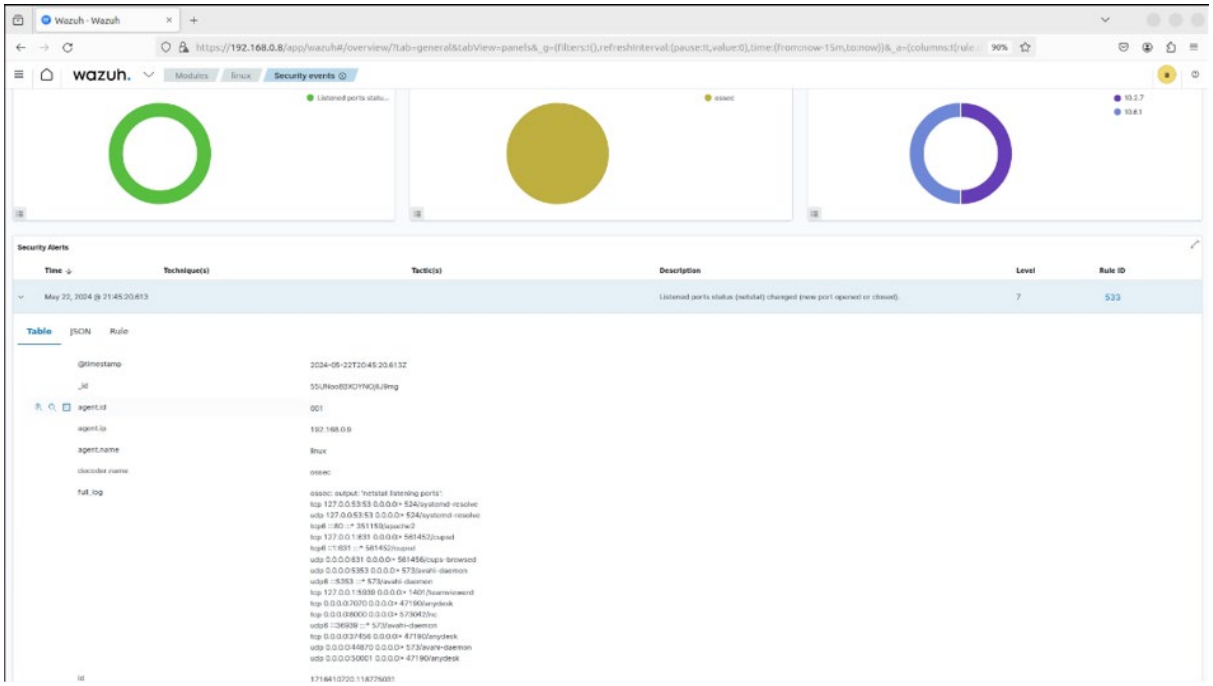

Figure B.14: Expanded Log Entry for Security Filters

Forensic Evidence and Analysis of Unauthorised Processes

Linux logs are used to manually gather forensic evidence. The following UBUNTU logs are critical to conduct forensics:

- **Syslog**: /var/log/syslog – General system log file.
- **Auth.log**: /var/log/auth.log – Logs authentication and sudo commands.
- **Auditd logs**: /var/log/audit/audit.log – Detailed logs if auditd is configured.
- **Bash History**: ~/.bash_history – User-specific command history.

Using auditd (Audit Daemon)

We have used Auditd Logs to gather the evidence against the execution of the nc.exe Malicious process, and details of the Auditd utility are as follows:

auditd is a powerful tool that can provide detailed logging of system activities, including command executions. To log Netcat command executions, you can set up **auditd** rules.

Install auditd

If it's not already installed, you can install **auditd** with:

sudo apt-get install auditd audispd-plugins

Configure auditd Rules

To log Netcat executions, add a rule to **auditd**:

1. Open the **auditd** rules file:

sudo nano /etc/audit/rules.d/audit.rules

2. Add the following lines to log executions of Netcat (**nc**):

-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/nc -k netcat_activity

-a always,exit -F arch=b32 -S execve -F exe=/usr/bin/nc -k netcat_activity

Adjust the path to **nc** if it's different on your system.

3. Restart the **auditd** service to apply the changes:

sudo service auditd restart

Viewing auditd Logs

To view the logs, you can use the **ausearch** command:

ausearch -k netcat_activity

Or you can directly view the audit logs:

sudo cat /var/log/audit/audit.log | grep nc

Or you can view the audit logs with this command:

/var/log# ausearch -k netcat_activity

The output of running this command will provide evidence of the execution of the nc.exe malicious process:

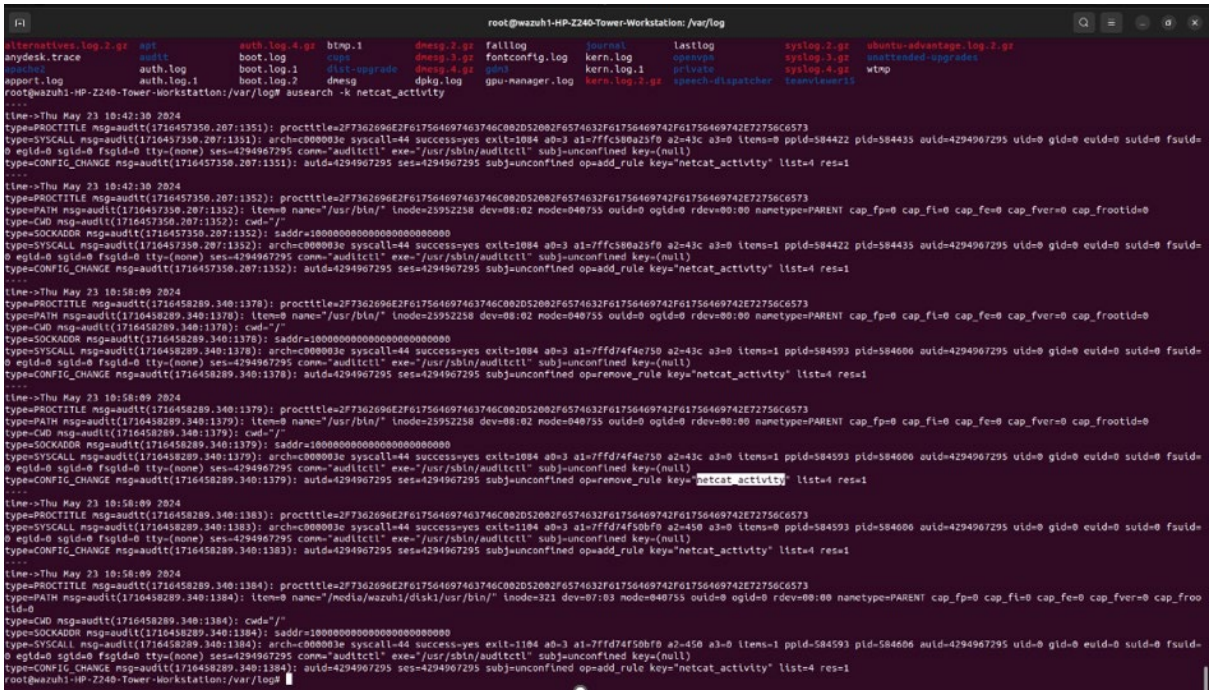

Figure B.15: Evidence of the Execution of nc.exe Malicious Process

Scenario - DOS (Denial of Service) Network Attack, Forensics and Evidence Collection

A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted network by overwhelming it with illegitimate traffic or resource requests. The primary goal of a DoS attack is to render the targeted system or network unavailable to legitimate users, effectively denying them access to the services provided by the targeted resource.

It's the Network Layer version of DOS Attack. This attack targets network infrastructure, such as routers and firewalls, by flooding them with high volumes of traffic or by sending specially crafted packets designed to consume available bandwidth, exhaust network resources, or overwhelm network devices. The infrastructure required for this attack is detailed below.

Table B.2: Infrastructure for DOS Attack

Endpoint	Description
Kali Linux 192.168.0.20	Attacker VM
WAZUH Server 192.168.0.8	Target
Windows 10 192.168.0.10	VM Host
SPLUNK 192.168.0	Investigation

UDP and TCP Packet Crafting Techniques using hping3

Hping3 is a scriptable program written in the Tcl language that allows packets to be received and sent in binary or string format. During network scanning, your first task

will be to scan the target network to determine all possible open ports, live hosts, and running services. Knowledge of packet-crafting techniques may help scan the network beyond the firewall or IDS. This technique aims to perform network scanning and packet crafting using hping3 commands.

For this scenario, the requirements are:

- Kali Linux (Attacker machine) 192.168.0.20
- Windows 10 (Target machine) 192.168.0.10

Packet crafting is a technique for finding vulnerabilities or entry points into a target network. It involves creating custom network packets to test network devices and behaviour.

DOS Attack Scenario: Implementation Step by Step

The following steps were taken to implement the attack scenario.

1. At first, open the Splunk web UI at 192.168.0.10
2. Provide Login Credentials
3. Go to the Home page of Splunk UI.
4. From the Quick Links Tab, click the Add Data button.
5. Now, click the Monitor Button.
6. Now, Click Local Windows Network Monitoring
7. Add In field **Network monitor Name**: IOT-Forensics-SIEM
8. Leave all the checkboxes the same.
9. Click Next from the Top.
10. Then click the review button.
11. Then click the submit button.
12. You will see the following filled info for review.

Table B.3: DOS Attack: Splunk Review Interface

Review	
Input Type	Network Monitor
Collection Name	IOT-Forensics-SIEM
Address Family	ipv4; ipv6
Packet Type	connect; accept
Direction	inbound; outbound
Protocol	tcp; udp
Remote Address	N/A
Process	N/A
User	N/A
App Context	search
Host	SEC-DC01
Index	default

13. Click at home.
14. Click Search and Review.
15. Leave the Splunk UI in this observing state.
16. On the other hand, run Kali VM with IP 192.168.0.20.
17. Write the following script and RUN in SUDO mode as shown in the snapshot

hping3 -c 500 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.10

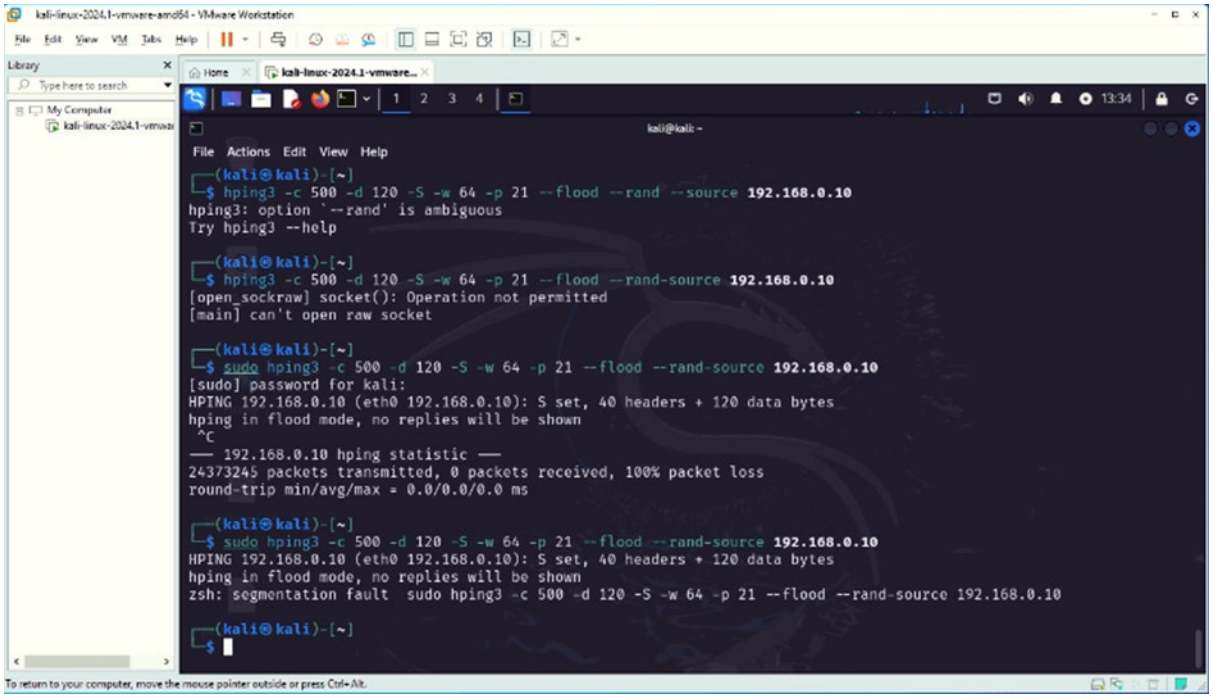

Figure B.16: Snapshot Showing Kali VM running Script

18. Now, at Splunk, go to the search page
19. Under How to Search, click on Data Summary
20. From the sources, select IOT-Forensics-SIEM
21. Here, you can see the listed events fired by the DOS attack launched from Kali.

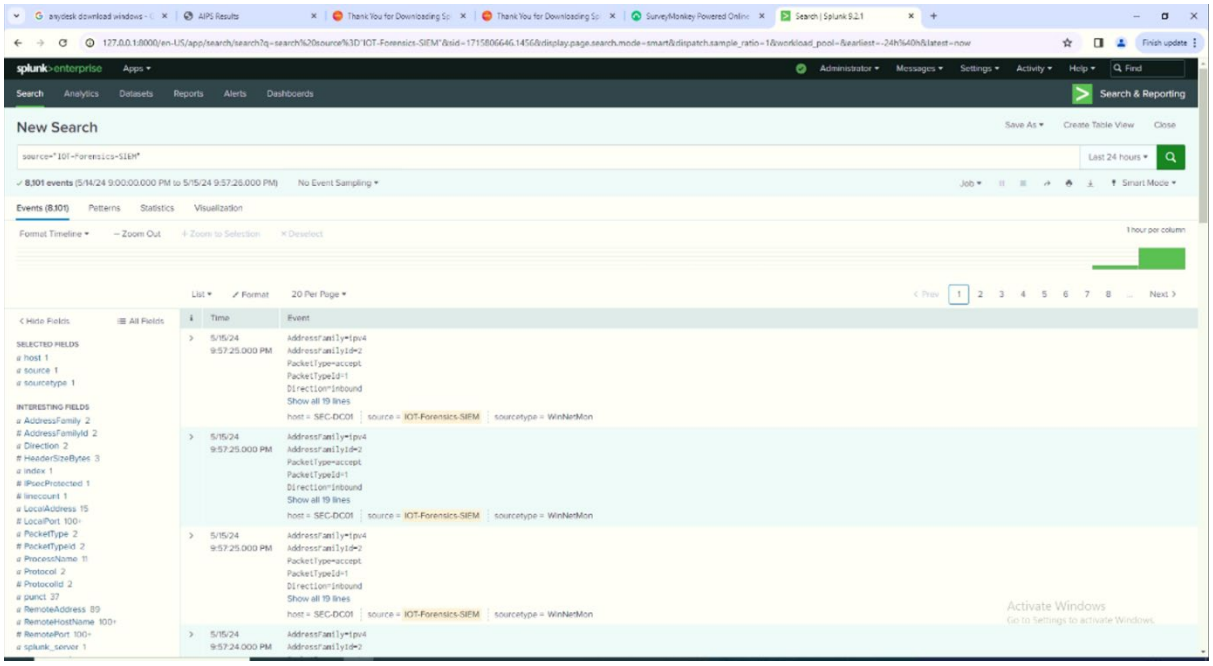

Figure B.17: Events Fired by the DOS Attack Launched from Kali

Also, the number of events logged during the attack can be seen from the following screenshot:

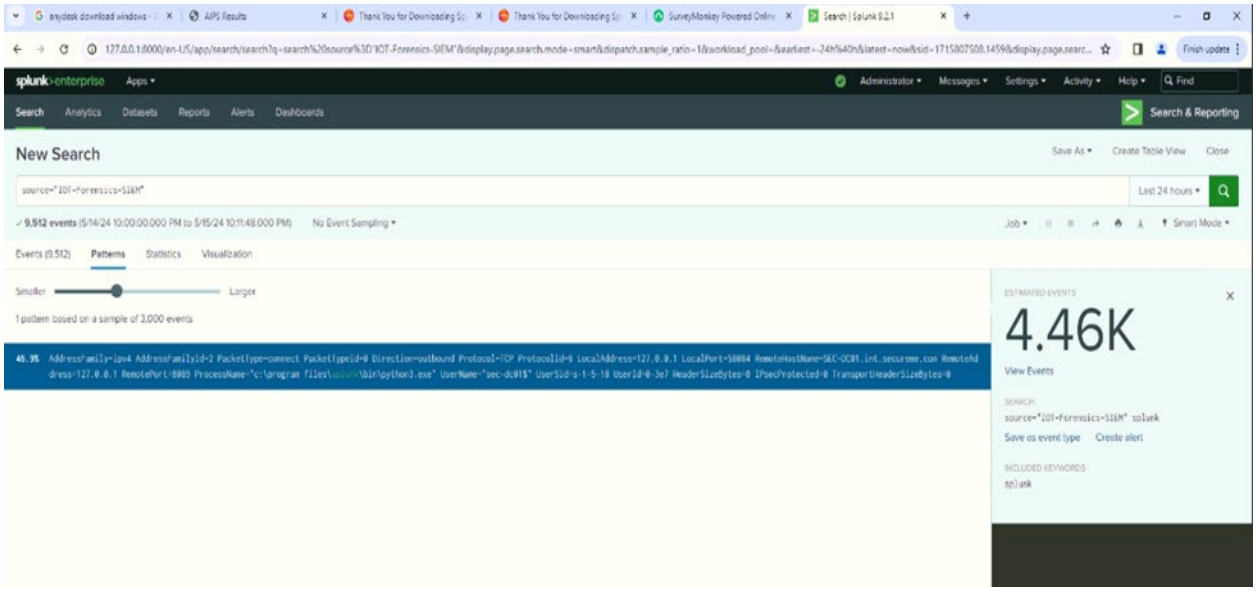

Figure B.18: Number of Events Logged During the DOS Attack

The screenshot below shows the CPU usage on 192.168.0.10 (Victim Machine) as high.

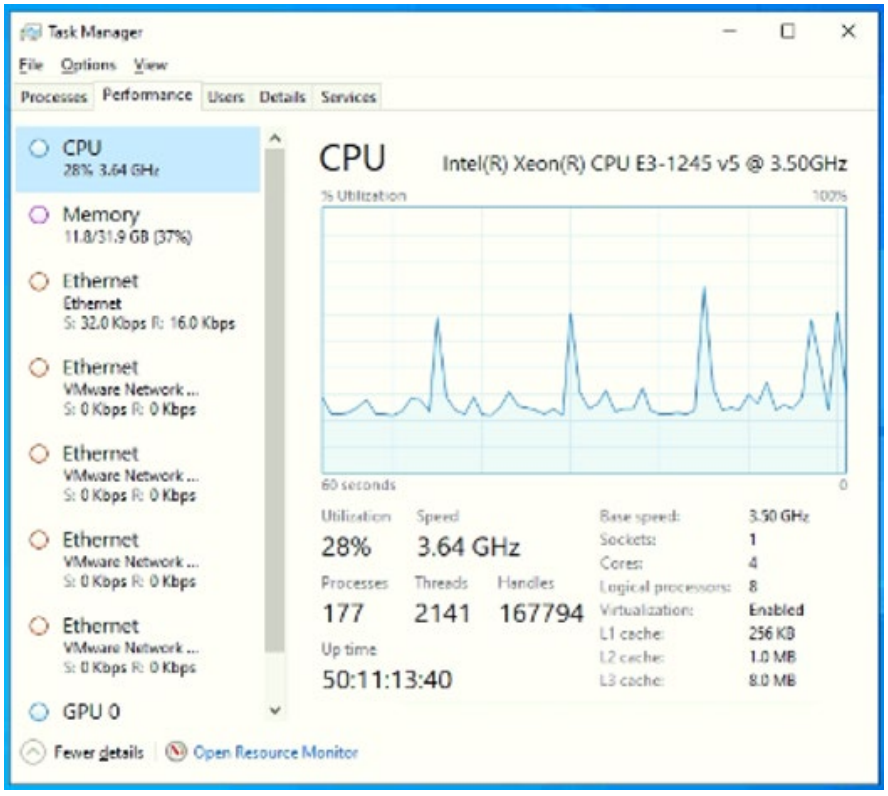

Figure B.19: High CPU Usage on Victim Machine

Appendix C

C.1 Performance Evaluation of Model PoC

In the appendix, model performance is overviewed, including feature importance, a confusion matrix, and key metrics. Figure C.1 shows the 20 most essential features sorted by importance in the model's prediction accuracy estimate based on their importance scores derived from the Random Forest Classifier. Figure C.2 represents the confusion matrix of TP, TN, FP, and FN across classification results. It is colour-coded for clarity and allows for a quick evaluation of the true classifications versus misclassifications in the matrix. The confusion matrix supports the calculation of accuracy, precision, recall, specificity, and F1 score, all of which are important for understanding the model's strengths and weaknesses. Figure C.3 illustrates the Confusion Matrix Calculation Methodology, providing transparency into how evaluation metrics are derived from confusion matrix values and thereby documenting the model's performance. Figure C.4 represents the model's final accuracy and F1 scores on all test instances. The results demonstrate the model's balance between precision and recall, making it a robust tool for intrusion detection.

	Feature	Importance
182546	Fwd Seg Size Min_40	0.010321
455	Dst Port_21	0.009904
203309	Idle Min_0.0	0.009314
181895	Init Bwd Win Byts_219	0.009171
181705	Init Fwd Win Byts_26883	0.009037
191814	Idle Mean_0.0	0.008603
2510	Dst Port_80	0.008143
195590	Idle Std_0.0	0.007474
189183	Active Min_0.0	0.007388
80824	Flow IAT Min_0.0	0.006286
121340	Fwd IAT Min_0.0	0.006176
152829	Fwd Header Len_40	0.006141
23878	TotLen Bwd Pkts_2665	0.005859
182534	Fwd Seg Size Min_20	0.005746
193486	Idle Mean_0	0.005704
200201	Idle Max_0.0	0.005344
181599	Init Fwd Win Byts_32738	0.005066
176155	RST Flag Cnt_1	0.004959
184794	Active Mean_0.0	0.004817
176189	Down/Up Ratio_1	0.004596

Figure C. 1

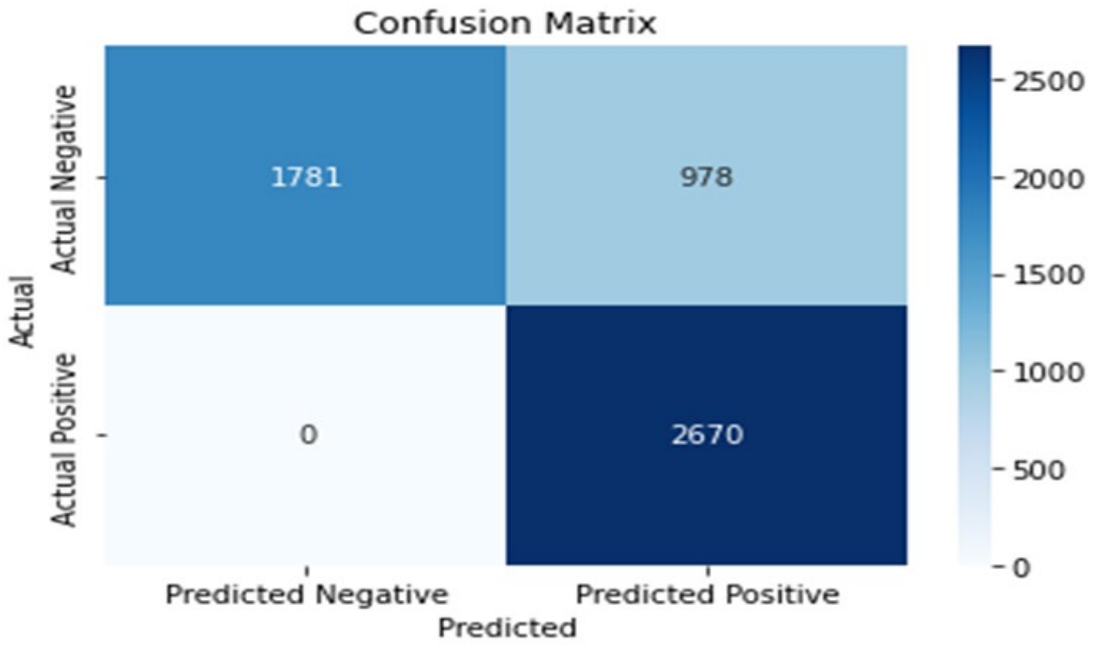

Figure C.2

```
# Step 2: Calculate the metrics based on the counts
total = tp_count + tn_count + fp_count + fn_count

accuracy = (tp_count + tn_count) / total if total > 0 else 0
precision = tp_count / (tp_count + fp_count) if (tp_count + fp_count) > 0 else 0
recall = tp_count / (tp_count + fn_count) if (tp_count + fn_count) > 0 else 0
specificity = tn_count / (tn_count + fp_count) if (tn_count + fp_count) > 0 else 0
f1_score = 2 * (precision * recall) / (precision + recall) if (precision + recall) > 0 else 0
```

Figure C.3

```
Accuracy: 0.8198563271320686
Precision: 0.7319078947368421
Recall (Sensitivity): 1.0
Specificity: 0.6455237404856832
F1 Score: 0.845204178537512
```

Figure C.4

Code: For 20 important features,

import Pandas as a PD

from Sklearn.ensemble import RandomForestClassifier

from sklearn.model_selection import train_test_split

```
from mlxtend.feature_selection import SequentialFeatureSelector as SFS
import matplotlib.pyplot as plt

# Step 1: Load the dataset
df = pd.read_csv("")

# Display the shape of the original DataFrame
print("Original DataFrame shape:", df.shape)

# Drop the last 4 columns
df_dropped = df.iloc[:, :-4]

# Display the shape after dropping
print("New DataFrame shape after dropping last 4 columns:", df_dropped.shape)

# Display the last few rows of the new DataFrame
print(df_dropped.tail())
# Display unique attack types in the 'Label' column
unique_attacks = df['Label'].unique()

# Display the unique attack types
print("Unique Attack Types:", unique_attacks)

# Optionally, to count the occurrences of each attack type
attack_counts = df['Label'].value_counts()
print("\nAttack Counts:\n", attack_counts)

# Import necessary libraries
import pandas as pd

from sklearn.preprocessing import LabelEncoder
```

```
import seaborn as sns

# Step 1: Preprocess the data
# Encode the 'Label' column (target) using LabelEncoder
label_encoder = LabelEncoder()
df['Label'] = label_encoder.fit_transform(df['Label'])

# Separate features (X) and target (y)
X = df.drop(columns=['Label'])
y = df['Label']

# Handle any categorical features by using one-hot encoding
X = pd.get_dummies(X)

# Step 2: Split the data into training and test sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)

# Step 3: Train a Random Forest Classifier
rf = RandomForestClassifier(n_estimators=100, random_state=42)
rf.fit(X_train, y_train)

# Step 4: Extract feature importances
importances = rf.feature_importances_

# Create a DataFrame for feature importance
feature_importances_df = pd.DataFrame({
    'Feature': X.columns,
    'Importance': importances
})
```

```
# Sort by importance
feature_importances_df = feature_importances_df.sort_values(by='Importance',
ascending=False)

# Step 5: Visualize the top 20 important features
plt.figure(figsize=(10, 8))
sns.barplot(x='Importance', y='Feature', data=feature_importances_df.head(20),
palette='viridis')
plt.title('Top 20 Important Features')
plt.show()

# Optionally print the top 20 features and their importance
print(feature_importances_df.head(20))
```

Code: For evaluation matrix

```
import pandas as pd
import matplotlib.pyplot as plt
from sklearn.metrics import roc_curve, auc

# Step 1: Load the dataset
df = pd.read_csv()
print(df.head())

# Step 1: Count the occurrences of TP, TN, FP, FN from the full dataset
tp_count = df['TP_TN_FP_FN'].value_counts().get('TP', 0)
tn_count = df['TP_TN_FP_FN'].value_counts().get('TN', 0)
fp_count = df['TP_TN_FP_FN'].value_counts().get('FP', 0)
fn_count = df['TP_TN_FP_FN'].value_counts().get('FN', 0)

# Step 2: Calculate the metrics based on the counts
total = tp_count + tn_count + fp_count + fn_count
```

```
accuracy = (tp_count + tn_count) / total if total > 0 else 0
precision = tp_count / (tp_count + fp_count) if (tp_count + fp_count) > 0 else 0
recall = tp_count / (tp_count + fn_count) if (tp_count + fn_count) > 0 else 0
specificity = tn_count / (tn_count + fp_count) if (tn_count + fp_count) > 0 else 0
f1_score = 2 * (precision * recall) / (precision + recall) if (precision + recall) > 0 else 0

# Step 3: Display the results
print(f"True Positives (TP): {tp_count}")
print(f"True Negatives (TN): {tn_count}")
print(f"False Positives (FP): {fp_count}")
print(f"False Negatives (FN): {fn_count}\n")

print(f"Accuracy: {accuracy}")
print(f"Precision: {precision}")
print(f"Recall (Sensitivity): {recall}")
print(f"Specificity: {specificity}")
print(f"F1 Score: {f1_score}")

import matplotlib.pyplot as plt

# Data for the bar plot
counts = {'TP': tp_count, 'TN': tn_count, 'FP': fp_count, 'FN': fn_count}

# Plotting the bar chart
plt.bar(counts.keys(), counts.values(), color=['green', 'blue', 'red', 'orange'])
plt.title('Counts of TP, TN, FP, FN')
plt.xlabel('Categories')
plt.ylabel('Count')
plt.show()

import seaborn as sns
```

```
# Create a confusion matrix based on the counts
conf_matrix = [[tn_count, fp_count], [fn_count, tp_count]]

# Plotting the confusion matrix
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap='Blues', xticklabels=['Predicted
Negative', 'Predicted Positive'], yticklabels=['Actual Negative', 'Actual Positive'])
plt.title('Confusion Matrix')
plt.ylabel('Actual')
plt.xlabel('Predicted')
plt.show()
```

Code: For XGBClassifier

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns

from xgboost import XGBClassifier
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
from sklearn.impute import SimpleImputer

df = pd.read_csv("C:/Users/91746/Downloads/randomized_filtered_dataset.csv",
low_memory=False)

true_headers = set(df.columns)
headerlike_mask = df.apply(lambda row: all(str(row[col]) == col for col in
df.columns), axis=1)
df = df[~headerlike_mask].copy()

if "Flow ID" in df.columns:
   df.drop(columns=["Flow ID"], inplace=True)
```

```
target_le = LabelEncoder()
df['Label'] = target_le.fit_transform(df['Label'])


X = df.drop(columns=['Label'])
y = df['Label']


for col in X.columns:
    X[col] = pd.to_numeric(X[col], errors='ignore')


for col in X.columns:
    if X[col].dtype == 'object':
        le = LabelEncoder()
        X[col] = le.fit_transform(X[col].astype(str))


top_features_per_attack = {}

# Get unique attack types and build mapping (numeric code -> original label)
attack_types = y.unique()
label_mapping = dict(zip(target_le.transform(target_le.classes_), target_le.classes_))


for attack_code in attack_types:
    attack_name = label_mapping[attack_code]
    print(f"Processing attack type: {attack_name}")

    #  binary target: 1 for current attack, 0 for others
    y_binary = (y == attack_code).astype(int)

    # Train-test split (70% train, 30% test)
    X_train, X_test, y_train, y_test = train_test_split(
        X, y_binary, test_size=0.3, random_state=42
    )


    imputer = SimpleImputer(strategy='mean')
    X_train_imputed = imputer.fit_transform(X_train)
    X_test_imputed = imputer.transform(X_test)

    # Convert to float32 to reduce memory usage
    X_train_imputed = X_train_imputed.astype('float32')
    X_test_imputed = X_test_imputed.astype('float32')
```

```
    xgb_clf = XGBClassifier(n_estimators=100,
                            use_label_encoder=False,
                            eval_metric='logloss',
                            random_state=42)
    xgb_clf.fit(X_train_imputed, y_train)


    importances = xgb_clf.feature_importances_
    feature_importances_df = pd.DataFrame({
        'Feature': X.columns,
        'Importance': importances
    })
    top_5_features = feature_importances_df.sort_values(by='Importance',
ascending=False).head(5)
    top_features_per_attack[attack_name] = top_5_features

    print(f"Top 5 features for {attack_name}:")
    print(top_5_features, "\n")


sns.set_style("whitegrid")
for attack, top_features in top_features_per_attack.items():
    plt.figure(figsize=(10, 6))
    sns.barplot(x='Importance', y='Feature', data=top_features, palette='viridis')
    plt.title(f'Top 5 Important Features for {attack} (XGBoost)')
    plt.show()

for attack, top_feats in top_features_per_attack.items():
    print(f"Top 5 features for {attack}:\n{top_feats}\n")
```

Code: For ExtraTreesClassifier

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns

from sklearn.ensemble import ExtraTreesClassifier
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
from sklearn.impute import SimpleImputer


df = pd.read_csv("C:/Users/91746/Downloads/randomized_filtered_dataset.csv",
low_memory=False)
```

```
true_headers = set(df.columns)
headerlike_mask = df.apply(lambda row: all(str(row[col]) == col for col in df.columns), axis=1)
df = df[~headerlike_mask].copy()


if "Flow ID" in df.columns:
    df.drop(columns=["Flow ID"], inplace=True)


target_le = LabelEncoder()
df['Label'] = target_le.fit_transform(df['Label'])


X = df.drop(columns=['Label'])
y = df['Label']


for col in X.columns:
    X[col] = pd.to_numeric(X[col], errors='ignore')


for col in X.columns:
    if X[col].dtype == 'object':
        le = LabelEncoder()
        X[col] = le.fit_transform(X[col].astype(str))


top_features_per_attack = {}

# Get unique attack types and build mapping (numeric code -> original label)
attack_types = y.unique()
label_mapping = dict(zip(target_le.transform(target_le.classes_), target_le.classes_))


for attack_code in attack_types:
    attack_name = label_mapping[attack_code]
    print(f"Processing attack type: {attack_name}")

    # Create a binary target: 1 if current attack, 0 otherwise
    y_binary = (y == attack_code).astype(int)

    # Split data (70% train, 30% test)
    X_train, X_test, y_train, y_test = train_test_split(
```

```
        X, y_binary, test_size=0.3, random_state=42
    )


    imputer = SimpleImputer(strategy='mean')
    X_train_imputed = imputer.fit_transform(X_train)
    X_test_imputed = imputer.transform(X_test)

    # Convert to float32 to reduce memory usage
    X_train_imputed = X_train_imputed.astype('float32')
    X_test_imputed = X_test_imputed.astype('float32')


    etc = ExtraTreesClassifier(n_estimators=100, random_state=42)
    etc.fit(X_train_imputed, y_train)


    importances = etc.feature_importances_
    feature_importances_df = pd.DataFrame({
        'Feature': X.columns,
        'Importance': importances
    })
    top_5_features = feature_importances_df.sort_values(by='Importance',
ascending=False).head(5)
    top_features_per_attack[attack_name] = top_5_features

    print(f"Top 5 features for {attack_name}:")
    print(top_5_features, "\n")


sns.set_style("whitegrid")
for attack, top_features in top_features_per_attack.items():
    plt.figure(figsize=(10, 6))
    sns.barplot(x='Importance', y='Feature', data=top_features, palette='viridis')
    plt.title(f'Top 5 Important Features for {attack} (ExtraTrees)')
    plt.show()


for attack, top_feats in top_features_per_attack.items():
    print(f"Top 5 features for {attack}:\n{top_feats}\n")
```

Code: BaggingClassifier

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
```

```
import seaborn as sns

from sklearn.ensemble import BaggingClassifier
from sklearn.tree import DecisionTreeClassifier
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
from sklearn.impute import SimpleImputer


df = pd.read_csv("C:/Users/91746/Downloads/randomized_filtered_dataset.csv", low_memory=False)


true_headers = set(df.columns)
headerlike_mask = df.apply(lambda row: all(str(row[col]) == col for col in df.columns), axis=1)
df = df[~headerlike_mask].copy()


if "Flow ID" in df.columns:
    df.drop(columns=["Flow ID"], inplace=True)


# 4. Encode the target column 'Label'

target_le = LabelEncoder()
df['Label'] = target_le.fit_transform(df['Label'])



X = df.drop(columns=['Label'])
y = df['Label']


# 6. Convert columns that should be numeric where possible

for col in X.columns:
    X[col] = pd.to_numeric(X[col], errors='ignore')


# 7. Label encode categorical (object-type) columns instead of one-hot encoding

for col in X.columns:
    if X[col].dtype == 'object':
        le = LabelEncoder()
        X[col] = le.fit_transform(X[col].astype(str))
```

```
# 8. Set up a dictionary to store top-5 features per attack type

top_features_per_attack = {}

# Get unique attack types and build mapping (numeric code -> original label)
attack_types = y.unique()
label_mapping = dict(zip(target_le.transform(target_le.classes_), target_le.classes_))


# 9. One-vs-rest loop for each attack type

for attack_code in attack_types:
    attack_name = label_mapping[attack_code]
    print(f"Processing attack type: {attack_name}")

    # Create binary target: 1 if current attack, 0 otherwise
    y_binary = (y == attack_code).astype(int)

    # Train-test split (70% train, 30% test)
    X_train, X_test, y_train, y_test = train_test_split(
        X, y_binary, test_size=0.3, random_state=42
    )


    # 10. Impute missing values using mean strategy

    imputer = SimpleImputer(strategy='mean')
    X_train_imputed = imputer.fit_transform(X_train)
    X_test_imputed = imputer.transform(X_test)

    # Convert to float32 to reduce memory usage
    X_train_imputed = X_train_imputed.astype('float32')
    X_test_imputed = X_test_imputed.astype('float32')

    # ---------------------------
    # 11. Train BaggingClassifier with DecisionTreeClassifier as base estimator
    # ---------------------------
    bag_clf = BaggingClassifier(estimator=DecisionTreeClassifier(),
                                n_estimators=50,
                                random_state=42)
    bag_clf.fit(X_train_imputed, y_train)

    # ---------------------------
    # 12. Compute feature importances by averaging importances from each tree
```

```
    # ---------------------------
    tree_importances = [est.feature_importances_ for est in bag_clf.estimators_]
    importances = np.mean(tree_importances, axis=0)

    feature_importances_df = pd.DataFrame({
        'Feature': X.columns,
        'Importance': importances
    })

    # Sort by importance descending and select top 5 features
    top_5_features = feature_importances_df.sort_values(by='Importance',
ascending=False).head(5)
    top_features_per_attack[attack_name] = top_5_features

    print(f"Top 5 features for {attack_name}:")
    print(top_5_features, "\n")

# ---------------------------
# 13. Plot the top 5 features for each attack type
# ---------------------------
sns.set_style("whitegrid")
for attack, top_features in top_features_per_attack.items():
    plt.figure(figsize=(10, 6))
    sns.barplot(x='Importance', y='Feature', data=top_features, palette='viridis')
    plt.title(f'Top 5 Important Features for {attack} (Bagging)')
    plt.show()

# ---------------------------
# 14. Optionally, print the top features in the console
# ---------------------------
for attack, top_feats in top_features_per_attack.items():
    print(f"Top 5 features for {attack}:\n{top_feats}\n")
```

Code: For RandomForestClassifier

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns

from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelEncoder
from sklearn.impute import SimpleImputer
```

```
df = pd.read_csv("C:/Users/91746/Downloads/randomized_filtered_dataset.csv"
,low_memory=False)


true_headers = set(df.columns)
headerlike_mask = df.apply(lambda row: all(str(row[col]) == col for col in
df.columns), axis=1)
df = df[~headerlike_mask].copy()


if "Flow ID" in df.columns:
   df.drop(columns=["Flow ID"], inplace=True)


target_le = LabelEncoder()
df['Label'] = target_le.fit_transform(df['Label'])


X = df.drop(columns=['Label'])
y = df['Label']


for col in X.columns:a
   X[col] = pd.to_numeric(X[col], errors='ignore')


for col in X.columns:
   if X[col].dtype == 'object':
      le = LabelEncoder()
      X[col] = le.fit_transform(X[col].astype(str))


top_features_per_attack = {}

# Get unique attack types and build mapping (numeric code -> original label)
attack_types = y.unique()
label_mapping = dict(zip(target_le.transform(target_le.classes_), target_le.classes_))


for attack_code in attack_types:
   attack_name = label_mapping[attack_code]
   print(f"Processing attack type: {attack_name}")

   # Create binary target: 1 if current attack, 0 for all others
   y_binary = (y == attack_code).astype(int)
```

```
    # Train-test split (70% train, 30% test)
    X_train, X_test, y_train, y_test = train_test_split(
        X, y_binary, test_size=0.3, random_state=42
    )


    imputer = SimpleImputer(strategy='mean')
    X_train_imputed = imputer.fit_transform(X_train)
    X_test_imputed = imputer.transform(X_test)

    # Convert to float32 to reduce memory usage
    X_train_imputed = X_train_imputed.astype('float32')
    X_test_imputed = X_test_imputed.astype('float32')


    rf = RandomForestClassifier(n_estimators=100, random_state=42)
    rf.fit(X_train_imputed, y_train)


    importances = rf.feature_importances_
    feature_importances_df = pd.DataFrame({
        'Feature': X.columns,
        'Importance': importances
    })
    top_5_features = feature_importances_df.sort_values(by='Importance',
ascending=False).head(5)
    top_features_per_attack[attack_name] = top_5_features

    print(f"Top 5 features for {attack_name}:")
    print(top_5_features, "\n")


sns.set_style("whitegrid")
for attack, top_features in top_features_per_attack.items():
    plt.figure(figsize=(10, 6))
    sns.barplot(x='Importance', y='Feature', data=top_features, palette='viridis')
    plt.title(f'Top 5 Important Features for {attack} (Random Forest)')
    plt.show()

for attack, top_feats in top_features_per_attack.items():
    print(f"Top 5 features for {attack}:\n{top_feats}\n")
```