Enhancing Forensic Readiness in IoT-Enabled Organizations: A Real-Time Model

Authors:

*Oyeyemi Kuku (MSc)[1] Dr Alexandros Chrysikos[2] and Dr Shahram Salekzamankhani[3]

[1] London Metropolitan University, 166-220 Holloway Road, London N7 8DB, UK

oyk0012@my.londonmet.ac.uk

[2] London Metropolitan University, 166-220 Holloway Road, London N7 8DB, UK

a.chrysikos@londonmet.ac.uk

[3] London Metropolitan University, 166-220 Holloway Road, London N7 8DB, UK

s.salekzamankhani@londonmet.ac.uk

Abstract

The increase in the intensity of cyberattacks has raised the need for conducting thorough digital forensic investigations to collect evidence and locate the source of the attack. The research presents a digital forensic readiness model that creates a realistic organisation scenario where multiple devices are connected and exposed to potential attackers. Digital forensic tools such as WAZUH and SPLUNK have been applied to gather the evidence. The proposed digital forensic readiness model targets organisational complexities, readiness processes, and compliance with ISO standards. ISO/IEC 27043:2015 emerges as a crucial standard for incident investigation concepts and procedures, offering a general framework adaptable to IoT environments. The research also shows that due to the changing and varied nature of IoT environments, conventional security approaches may not be enough, calling for alternative ways of risk evaluation.

Keywords Digital Forensic Model, Digital Readiness Model, Digital Investigation, IoT, Cyberattack

TABLE OF CONTENTS

1.1. Introduction 5

1.2. Background 6

1.2.1 Digital Forensic Readiness 6

1.2.2. Application and Use of IoT in an Organisation and Home Applications 7

1.2.3. Digital Forensic Investigation 8

1.2.4. Forensic IoT Process 9

1.2.5 Readiness process groups in ISO/IEC 27043 10

1.2.6 Summary 11

1.3. Research Design 12

1.3.1 Proposed Model 12

1.4. Experiment 14

1.4.1. Detection of Unauthorized Process at WAZUH and Forensic Analysis 15

1.4.2Reporting File Integrity Monitoring (FIM) Process. 16

1.5. Implications 17

1.6 Limitations 17

1.7. Discussion of Findings 18

1.8. Conclusion 19

1.9. Recommendation for Further Research 19

References 21

Appendix A: List Of Abbreviations 24

1.1. Introduction

Cyber security has become a significant concern due to an alarming increase in the number and complexity of cyber attacks. Sophisticated tools are being used to design attacks, increasing the efficiency of hit rates.(Abomhara and Køien, 2015). As technology advances and becomes more sophisticated, the threat posed by cybercriminals also increases. Cyber threats include (Singh et al., 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 trick people into providing sensitive information, such as passwords or credit card numbers.
- **Ransomware:** it is malicious software that is used to encrypt files on a computer against which a demand can be made to attain a decryption (Imperva, 2022).

The impact of cyber security is significant in terms of financial losses and damage to reputation. Businesses experiencing 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. To counter the issues, organisations can adopt Digital Forensic Readiness (DFR) models that aid in conducting digital forensic investigation (DFI) (Ngobeni et al., 2010). A DFR model aids in conducting a digital investigation to identify and track the attackers.

The DFI involves presenting, documenting, analysing, preserving, and identifying data for evidence. Digital forensics (DF) generally comprises four steps, as shown in Figure 1: identifying the digital assets involved in digital crime, acquiring digital devices and related assets, analysing data in digital systems related to the crime, storing information, and reporting.

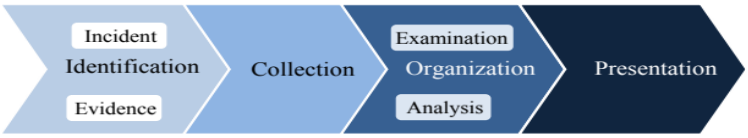

Fig.1: The Digital Forensic Flow Process (Zawoad et al., 2015)

The increase in the number of cyber attacks and the corresponding damage to an organisation's security and finances has had a profound impact on the working of organisations, resulting in an increasing need to conduct research that would aid in developing a more comprehensive and effective DFR model and readiness model which would enhance security and aid in digital forensic investigation. The current

study aims to create a real-time readiness model for IoT-enabled organisations and aid forensic investigation analysis. Specifically, the objectives are:

1. To examine the current digital forensics readiness model/frameworks and categorise their respective strengths and weaknesses.
2. To develop a comprehensive DFR model that can be customised to meet specific requirements of various organisations.
3. To evaluate the proposed DFR model's effectiveness in enhancing an organisation's capabilities to react to a cyber incident.
4. Develop a readiness model based on IoT applications for an organisation's security and technology.
5. To evaluate the performance of the readiness model concerning forensic investigation.

1.2. Background

The Internet of Things (IoT) is the next big revolution in the world of the Internet. The purpose of IoT was to make the Internet safer and reduce risk; however, the emergence of IoT botnet has resulted in changing it from life support to the Internet of Vulnerabilities for cybercriminals(Angrishi, 2017). Kebande et al., (2020) investigated the 2016 MIRAI cyber attack in which approximately 4000 IoT-based devices were infected. They revealed that the infection was responsible for launching a Distributed Denial of Service attack impacting several major service providers such as Netflix and Paypal. In continuation of this, Sgurevet al.,(2020) comment that it is essential to continue improving investigation techniques for digital forensics as the complexity of the attacks is increasing. The findings of Ghelani's (2022) research concluded that cyber-attacks constantly threaten organisations, and it is imperative to enhance digital security.

According to a study published by Spear Project (2021), UK companies lose around £27 billion annually to cybercrime. The cost of cybercrime in the EU has also risen to €50,000 per incident. The data also shows that companies affected by cyber crimes cost departments an average of €50,000 in the period of 2019-2020. Most organisations' approach to cyber incidents currently focuses on business continuity and disaster recovery. However, this approach often includes actions contrary to the principles of judicial investigation. Organisations can respond to cyber incidents by conducting a forensic investigation (Zainudin et al., 2022).

1.2.1 Digital Forensic Readiness

DFR represents the pre-incident plan implemented during the lifecycle of a DFI (Figure 2) to reduce the cost of investigation and aid in the identification of digital

evidence, storage and preservation of evidence and analysis of the information collected. Moutharopoulous et al. (2014) explained DFR as a tool that has the ability to manage digital evidence in a manner that enables the conduction of cost-effective and efficient investigation. DFR in IoT-enabled organisations is still evolving, and the ISO/IEC 27043 provides international standards for the DFR process (ISO, 2015). Given that cyber-attacks cannot be prevented altogether, with adequate planning on using forensic analysis, the organisation's digital forensic readiness capabilities can be strengthened, reducing the impact of cyberat-tacks(Karie et al., 2017).

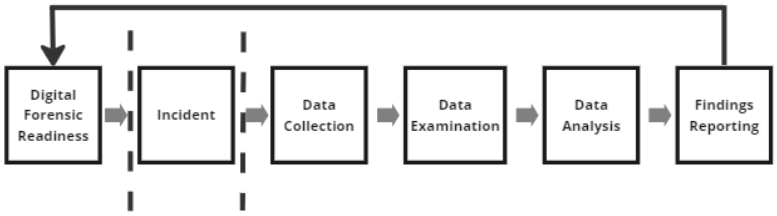

Fig.2: The Digital Forensic Investigation Lifecycle (Mouhtaropoulos et al., 2014)

Makura et al.,(2021) proposed a DFR framework based on ISO/IEC27043 standard. This framework was presented in a cloud environment for security monitoring. However, the requirement of digital readiness in IoT needs to be significantly covered. These include the planning pre-incident analysis of data representing the PDE process, planning the incident detection process, and defining the system architecture process, which was not considered in the Study. To implement DFR in an organisation, designers must include a variety of operational and operational planning strategies such as risk assessment, employee training, implementation tools, and measurement tools(Ab Rahman et al., 2016). However, the complexities of IoT create questions and obstacles in IoT forensic investigations, especially in acquiring and analysing digital evidence from IoT devices(Atlam et al., 2020).

1.2.2. Application and Use of IoT in an Organisation and Home Applications

As the current research on IoT infrastructures confirms, using IoT includes personal, work, health, education, etc. The related work in this section examines the application and use of IoT in organisation and home applications based on security procedures and design from a DFR perspective. Kim et al., (2020) explain that the devices are more complex in an intelligent home scenario forensic investigation and pose challenges for extracting meaningful data for analyses. 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.

Surangee et al (2011) commented that IoT devices have become widespread in intelligent living, manufacturing, automation and healthcare sectors.

Chi et al., (2019) Proposed a framework for IoT data acquisition and analysis. This framework drew data from user devices and the cloud to show the data acquisition process, but it does not cover forensic readiness in organisations or use international standards. Many authors provide frameworks for acquiring data from IoT when exploring literature. For example, Ngobeni et al., (2010) introduced the DFR wireless models while Oriwoh and Sant, (2013) Recommend the Forensic Edge Management System (FEMS). Meffert et al., (2017) Provided a general framework named Forensic State Acquisition from IoT (FSAIoT) to practically demonstrate that relevant data from IoT devices can be extracted using three different modes: controller to the device, controller to cloud and controller to controller. Kebande et al. (2018) Propose adding DFR to the IoT's smart environment using the standard procedure specified in the international standard ISO/IEC 27043.

1.2.3. Digital Forensic Investigation

Zawoad and Hasan,(2015) proposed a forensic-aware IoT (FAIoT) to support forensic investigations in IoT environments; however, this is a technology solution and does not provide adequate inputs for digital forensic readiness in IoT and also is not in accordance with the standard set by the ISO/IEC 27043 code. A forensic investigation framework based on a public digital ledger was also presented by Hossain et al (2018). The presented framework collected data from various sources, such as users' devices, cloud networks, and IoT, and then securely stored it as a blockchain network. Further, Do Valle et al., (2020)Explain that in criminal investigation scenarios, the use of lambda architecture that involves frameworks such as HDFS (Hadoop Distributed File System), Kafka, Spark, and Docker were used to analyse big data volumes to identify digital traces from large datasets that involve IoT device data

Kebandeet al. (2016) proposed a DFI framework based on the international standard ISO/IEC 27043, comprising three modules: proactive, IoT forensics, and reactive. Though the model is promising, it lacks in covering processes at an organisational level, which is a significant part of the DFR process. Another model was presented by Hossain et al., (2018), which was based on a Forensic investigation framework (FIF) for IoT using a public digital ledger. The proposed framework can collect data from various sources, such as cloud and user devices, and then store it in a secure blockchain for public access. The model can ensure confidentiality, anonymity, integrity, and non-duplication of data.

1.2.4. Forensic IoT Process

The Forensic IoT procedure outlined in the International Standard is deliberately abstract to apply to various digital investigations and forms of digital evidence. ISO/IEC 27043:2015 is a standard that primarily focuses on incident investigation principles and processes rather than offering comprehensive guidelines for the forensic IoT process (ISO, 2015). However, it provides a general framework for digital investigations and can be adapted for designing and developing high-level processes to break them down into parts (ISO/IEC 27041). The investigative procedures are precisely laid out and described so that they may be followed. This procedure has four distinct phases broken down further into categories, as shown in Figure 3. In this approach, readiness processes help organisations define IoT scenarios and strategies, recognise potential sources of digital evidence, and establish data collection, preservation, and analysis procedures. The initialisation phase is critical for promptly responding to IoT incidents, followed by acquisitive processes where investigators securely identify, collect, transport, and store IoT data.

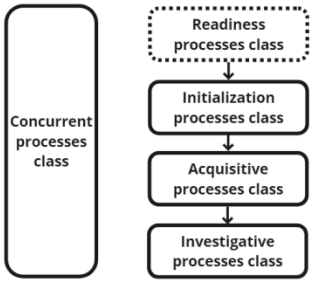

Fig .3: Digital forensic investigation process classes (ISO, 2015)

According to Kebande and Venter, (2018) the practices that guarantee an organisation can make the most of Digital Forensic evidence in the event of an occurrence 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 contains instructions for gathering possible digital evidence. The digital incident investigation, analysis, interpretation, and presentation are all forensic investigation process class subclasses. The process of wrapping up an investigation is a part of this as well. All process groups that happen simultaneously with a digital inquiry fall under the umbrella of "concurrent process classes." According to the authors, there would be more advantages to requiring the readiness process class as part of the digital investigative procedure.

1.2.5 Readiness process groups in ISO/IEC 27043

Sadineni et al., (2021) propose a readiness model, Ready-IoT, to monitor and log 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 to show its potential in detecting attacks performed on the network. Also, digital forensic readiness with standard approaches, essential in organisations, is not covered. ISO/IEC 27043 specifies four distinct process groups that comprise the preparedness process, as shown in Figure 4.

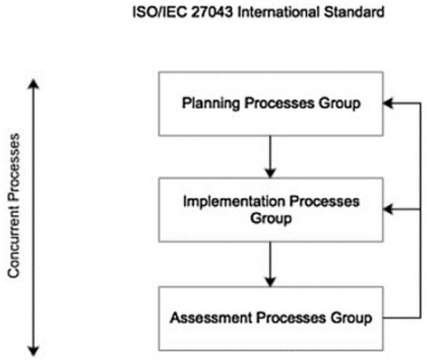

Fig .4: Readiness process groups (ISO, 2015)

ISO/IEC 27043 defines the planning process group as the actions determining 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 by considering legal and business-specific criteria in the planning process group(ISO, 2015)Implementation Process Group puts the procedures outlined in the strategy phase into action. Systems and procedures are set up, and the system architecture process is implemented to make Digital Forensic evidence collection possible(ISO, 2015).

Assessment Process Group actions 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 Digital Forensic principle (ISO, 2015).Concurrent processes are operations that co-occur as digital investigative operations. These steps have no set sequence but apply to various steps throughout the digital investigative process. One method to keep the chain of custody intact while digital evidence is passed between parties is to apply the "preserving chain of custody" technique to most steps in the digital investigative process (ISO, 2015).

1.2.6 Summary

The brief literature indicates research activity to show conceptual models and theoretical solutions of forensic IoT with little emphasis on practical DFR scenarios in organisations. However, it was noted that readiness processes in IoT frameworks and security mechanisms are needed to support forensic processes in organisations. The literature emphasises the importance of using standardised processes while conducting readiness processes. Therefore, this research will develop the DFR model using ISO/ IEC 27043 standards.

.

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	✓	×	×

Table .1: Digital Forensic Readiness Frameworks/models comparisons.

To meet this research, the IoT forensic readiness model's objectives must be met, and the gaps must be overcome where none of the frameworks/models fully support the three elements highlighted in Table 1. Specifically, a) Readiness Process; b) ISO Standardised - ISO/IEC27043 standard; and c) Forensic Processes Targeting Organisations.

The research proposes a model for DFR in IoT-enabled organisations, targeting the three elements and critical components of the IoT-FR framework (organisational, Readiness, and IoT Security Layer Processes). The following section discusses the strategies and procedures employed to conduct the quantitative investigation of the Digital Forensic Readiness Model (DFRM). Specifically, it outlines the detailed action plan for gathering, analysing, and interpreting data to address the research objectives effectively.

1.3. Research Design

Research methodology is a practical method of collecting, interpreting, and analysing data(Williams, 2007). There are three main research methods: quantitative, qualitative, and mixed.(Williams, 2007; Creswell, 2009). The research applies the pragmatism paradigm and quantitative methodology for this study. Quantitative research in a Digital Forensic Readiness Model (DFRM) uses experiments, numerical data, and statistical analyses to assess and measure digital forensic readiness's effectiveness, implementation, and impact within an organisation. This method is valuable in developing a digital forensics model because it allows for a deeper understanding of the complexities of digital forensics in real-time scenarios. Since the IoT-FR is at a conceptual stage, research activities show conceptual frameworks and theoretical solutions of forensic IoT with little emphasis on practical DFR scenarios in organisations. 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 the ISO/IEC 27043 standard.

1.3.1 Proposed Model

The proposed model is based on the frameworks presented in Table 1 and targets the IoT-FR framework's three critical organisational elements: readiness, IoT Security Layer, and Processes. The model, which integrates the various processes, has been developed and is represented in Figure 5. The model involves the organisational and IoT system architecture readiness processes to develop security procedures and policies. The IoT architecture management includes policies and procedures for monitoring data flow during application runs, incident detection, monitoring for data breaches, and comprehensive risk detection and mitigation to include in the organisation's overall cyber security model.

The model presented below emphasises that organisations must ensure IoT architecture processes are based on ISO/IEC 27043 standards. The IoT architecture presented includes the system architecture, information systems/infrastructure in the organisation, network perimeter and endpoints, software, and data. The details related to the architecture provide the information sources in the organisation's I.S. The data component in IoT architecture is essential to enable readiness processes according to international standards. The DFRM is based on readiness, initialisation, acquisition, and investigation. Each of these significant processes will include steps to follow for the organisation, as illustrated in the model diagram.

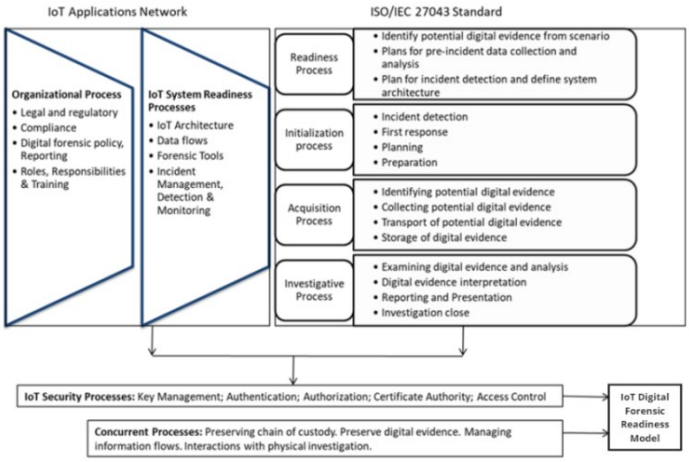

Fig .5 Proposed Research IoT Digital Forensic Readiness Model

.

As per the standard process, the readiness process is treated as a functional requirement in any organisation, including three processes. These processes are defined below:

- The planning process is a comprehensive undertaking that initiates processes to define IoT scenarios, identify sources of evidence, plan digital evidence-gathering methods, analyse evidence, and establish pre-incident detection processes.
- The implementation process follows the planning activities, implementing pre-incident gathering processes, storage techniques, analysis of collected data, and pre-incident detection processes within IoT environments.
- The assessment process is a critical step that evaluates the implementation process to ensure validity and presents the results, instilling confidence in the model's reliability.

In digital forensics within IoT environments, preparing for potential incidents beforehand is critical for effective response and mitigation strategies. Multiple techniques are deployed to achieve DFR in IoT-based environments, focusing on gathering past information. One such technique involves IoT sensor monitoring, utilising systems like ZigBee combined with light, humidity, and temperature sensors. Additionally, monitoring IoT devices based on network packets that send or receive packets enables the capture of data packets for interpretation, shedding light on device interactions and potential occurrences within the IoT ecosystem, including microcontrollers, Wi-Fi modules, and routers.

Assessing and monitoring protocols and services for IoT networks is crucial to increasing pre-incident detection. This approach allows investigators to collect a wide range of data to identify information about sources for conducting a digital forensic investigation. The IDS system plays an important role as it can detect and identify various modes of intrusion and send timely notifications to administrators.

Incident detection capabilities can be enhanced by incorporating false alarm detection mechanisms, allowing organisations to improve their readiness to respond to incidents or mitigate potential threats.

The readiness processes include the following parameters for preparing a forensic investigation:

- Forensic logging: It collects digital artefacts for analysis, while log parsing involves extracting specific events from collected logs.
- Log preservation: It ensures information integrity through hash value creation, while its storage in a forensic database enables verification and analysis.
- Log analysis: It detects security incidents within collected data, and log characterisation categorises logs to expedite investigations.
- Readiness report: It helps to achieve a critical outcome by implementing readiness processes. Also, procedural flows enable the interaction among readiness guidelines, techniques, processes, and reporting stages, collectively aimed at preparing IoT-based environments for forensic investigations.

The initialisation process involves initiating an investigation whenever PDE is identified, starting with post-event response mechanisms and proceeding to incident detection, planning, and preparing for digital investigations. Following this, the greedy process focuses on acquiring PDE from IoT-based environments, including identification techniques, evidence-collection methods, and procedures for preservation and storage under appropriate conditions. Then, the investigative process aims to determine the loss of detected incidents by examining and analysing collected PDE. This process interprets IoT environment activities resulting from incidents and presents them as hypotheses in legal proceedings.

1.4. Experiment

The experiment involves creating a realistic organisation scenario in a confined environment with various digital evidence, 50 user devices (desktops, laptops, and two network devices) and potential attackers or malicious actors in real-world digital forensic investigations. The user devices are a mixture of Windows 10, Windows 11 and Linux machines. The open-source standard digital forensic tools WAZUH and SPLUNK were used to gather digital forensic data (identification, detection, and storage) and analyse it (detection and monitoring). All system, network, and application logs will be stored in another database storage (forensic data store). 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.

1.4.1. Detection of Unauthorized Process at WAZUH and Forensic Analysis

The WAZUH command has the ability to run commands on an endpoint and monitor the output of the commands. The experiment uses WAZUH ClientUbuntru 192.168.0.9 and WAZUH server 192.168.0.8 to detect the NetCat process and malicious processes, respectively. The NetCat is applied to execute nc.exe to run a malicious process. Post this, the WAZUH is configured for the Ubuntu endpoints, and the WAZUH server is configured to trigger an alarm every timeNetCat launches a program. The alerts can be visualised via the WAZUH dashboard, as shown in the following figure.

Fig .6 Visualisation of data alert in the WAZUH dashboard

The forensic evidence is to be collected manually using Linux logs (Auditd logs), a powerful tool providing detailed logging system activities. By running the command using Auditd logs, evidence of the execution of the nc.exe malicious process is collected (figure 7).

Fig 7 Evidence of execution of nc.exe malicious process.

1.4.2 Reporting File Integrity Monitoring (FIM) Process.

In this experiment, digital forensics was conducted through the file auditing feature in the Windows WAZUH client machine and the following steps were undertaken to conduct the experiment:

- Enable the File Auditing feature.
- Configure the folder to add File Auditing.
- Configure Windows WAZUH Client side.
- Configure Windows WAZUH Server side.
- The attacker will delete the files from this classified folder.
- WAZUH Client will take the log and update the WAZUH server.
- WAZUH server will clearly identify with Forensic Evidence.
- On the client side, windows logs can also be used as forensic evidence. We use the Windows Event Viewer tool with Event ID 4660.
- These audit logs are saved and exported.
- To investigate this case further, the SPLUNK tool is used, and forensic evidence is collected.

Administrator permission is required to experiment since file auditing features are turned off by default in Windows. The Windows log and security are selected to execute the event viewer because the experiment only concerns network events. The evidence gathered by using SPLUNK is as follows.

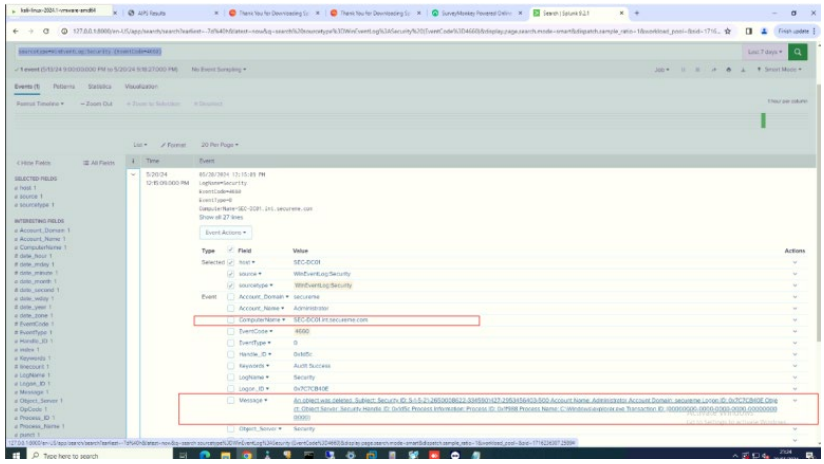

Fig.8 Evidence collected using SPLUNK

1.5. Implications

The implications highlight the benefits of the proposed model and the importance of collecting and preserving evidence in a manner suitable for courtroom presentation. Specifically:

- **Reduced costs:** Cost Savings associated with digital forensic investigations are a crucial advantage of DFR implementation.
- **Improved efficiency:** Prototypes that have implemented DFR make seamless technology use possible. In contrast to investigating every cloud instance, the DFI can, for example, concentrate only on a particular cloud instance where security incidents were found. This focused approach expedites the forensic process by reducing the resources required for the investigation and improving effectiveness and efficiency.
- **Collection of Admissible Evidence:** Digital evidence from forensic investigations must be allowed in court. DFR ensures that the right policies and guidelines are followed when collecting, preserving, and presenting digital evidence in a way that complies with legal specifications. Thus, digital forensic investigations can be used as evidence in a court of law.
- **Providing Competitive Advantage:** In addition to assisting companies in adhering to industry rules, DFR increases the confidence of the stakeholders by showing responsibility and readiness for cybersecurity-related risks. Hence, the company's competitive advantage and reputation may both benefit.

1.6 Limitations

DFR serves an excellent purpose for organisations in addressing security issues, but these organisations can face a few challenges and issues during an investigation. Specifically:

- A DFR plan serves as a framework for the steps to be taken when digital evidence is required for investigation. Its primary objective is maximising accessible evidence while minimising time and costs. An organisation's lack of such a plan can hamper investigations.
- It is crucial to match DFR practices with legal rules and privacy laws to ensure digital evidence can be appropriately used in court.
- Implementation of the DFR is challenging due to the lack of skilled personnel.
- An organisation's cost of adopting DFR in terms of finances, technology, and skills is predominantly high, making it challenging for organisations to adopt the technology.

- The absence of guidelines or standardisation of the DFR model makes it challenging for the evidence collected through DFR to be acceptable in legal dealings.
- The question of data custody and an organisation's digital compliance makes it difficult to produce evidence in a court of law.
- Court injunctions make presenting evidence gathered through DFR challenging, which can lead to questions about the program's implementation.
- The uncertainty associated with the required data tenure that needs to be maintained creates challenges for DFR implementation. Early disposal or retention of extensive data may lead to difficulty collecting digital evidence.
- Respondents' insufficient readiness in case of an emergency leads to data loss. The DFR system needs to be handled by respondents who can act swiftly in case of an attack.
- Disabling DFR systems can allow employees to tamper with an organisation's effectiveness, so it is crucial to protect the system from internal threats.

1.7. Discussion of Findings

The literature reveals that cybercrime has a significant financial impact on organisations and the economy. DFR implementation is crucial to addressing this issue as it provides an organisation with a tool to conduct investigations and improve response time for an incident, eventually reducing the cost burden. To do so, careful assessment and work planning are required to understand the organisation's needs. Refinement of DFR models and time-to-time performance evaluation can further aid in keeping the model on track.

The research has presented a method for systematically collecting and interpreting DFR data in numeric form from IoT-enabled organisations. The proposed model's concept is based on using a pragmatic approach that practically addresses the uniqueness of digital challenges. Furthermore, applying an iterative process aids in developing a DFR model that is both effective and adaptable to real-time situations.

The design model used open-source digital forensic tools to gather and analyse the data collected for forensic investigation. The IoT DFRM model developed can integrate various procedures, including compliance with ISO/IEC 27043 standards, IoT system architecture, and organisational procedures. The model also emphasises detecting incidents, mitigating risks, and monitoring data flow.

The proposed DFR model targets organisational complexities, readiness processes, and compliance with ISO standards. ISO/IEC 27043:2015 emerges as a crucial standard for incident investigation concepts and procedures, offering a general framework adaptable to IoT environments. Incorporating DFR processes within the digital investigative procedure is necessary to fully exploit digital proof and minimise business disruptions during forensic investigations.

By adhering to standards and implementing robust planning, implementation, and assessment stages, organisations can enhance their capability to respond effectively to cyber incidents. The identified techniques for achieving DFR in IoT-based environments reveal the significance of gathering past information through IoT sensor monitoring and network protocol analysis. Incorporating mechanisms like IDS and false alarm detection further strengthens incident detection capabilities. The structured approach outlined for initialisation, acquisitive, and investigative processes provides a framework for identifying, acquiring, and analysing Potential Digital Evidence, essential for formulating effective incident response strategies in IoT environments. Proactive measures and standardised processes enhance organisations' readiness for cyber threats in IoT ecosystems.

1.8. Conclusion

To protect private data, vital infrastructure, and the confidence of stakeholders, this analysis highlights the significance of preventative cyber security procedures, IT security risk assessments, and the development of sound cybersecurity policies. As the number of possible attack vectors increases with the number of connected devices, it is crucial to have a thorough grasp of the dangers unique to IoT ecosystems. This research also shows that due to the changing and varied nature of IoT environments, conventional security approaches may not be enough, calling for alternative ways of risk evaluation. 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.

1.9. Recommendation for Further Research

Digital Forensics in the Internet of Things (IoT) is a rapidly evolving technique that requires continuous innovation to tackle emerging challenges. It is recommended that future research should prioritise techniques that would develop faster and more reliable methods to discover evidence and further streamline the process. Further, it is recommended that research should focus on optimising hardware for enhanced efficiency in digital forensic investigation. It is also recommended that priority should be given to developing practical models that would provide robust frameworks for advancing digital forensic practices.

The scope for future work related to the given research topic is vast. Frameworks that fulfil the essential requirement for implementing DFR-IoT in a smart environment can be proposed. Furthermore, deep investigations can be undertaken into existing practices to improve and refine the technology. This can be achieved by

verifying models using expert input and conducting technical analyses to improve digital forensics processes.

References

Ab Rahman, N. H. et al. (2016) Forensic-by-Design Framework for Cyber-Physical Cloud Systems. *IEEE Cloud Computing*. [Online] 3 (1), 50–59.

Abomhara, M. &Køien, G. M. (2015) Cyber security and the Internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*. [Online] 4 (1), 65–88.

Angrishi, K. (2017) *Turning Internet of Things(IoT) into the Internet of Vulnerabilities (IoV) : IoT Botnets*. [online]. Available from: http://arxiv.org/abs/1702.03681.

Atlam, H. F. et al. (2020) Internet of Things Forensics: A Review. Internet of Things (Netherlands) 11.

Cassell, C. et al. (2018) *The SAGE Handbook of Qualitative Business and Management Research Methods: History and Traditions*. [Online]. SAGE Publications Ltd.

Chi, H. et al. (2019) 'A Framework for IoT Data Acquisition and Forensics Analysis', in *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*. [Online]. 22 January 2019 Institute of Electrical and Electronics Engineers Inc. pp. 5142–5146.

Creswell, J. W. (2009) *Research Design Qualitative and Quantitative Approaches. Thousand Oaks. CA Sage.*

Ghelani, D. (2022) Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*. [Online] 3 (6), 12–19.

Hossain, M., Karim, Y., et al. (2018) 'FIF-IoT: A forensic investigation framework for IoT using a public digital ledger', in *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*. [Online]. 26 September 2018 Institute of Electrical and Electronics Engineers Inc. pp. 33–40.

Hossain, M., Hasan, R., et al. (2018) 'Probe-IoT: A public digital ledger based forensic investigation framework for IoT', in *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*. [Online]. 6 July 2018 Institute of Electrical and Electronics Engineers Inc. pp. 1–2.

Imperva (2022) *Cyber Security Threats What are Cyber Security Threats?* [online]. Available from: https://www.imperva.com/learn/application-security/cyber-security-threats/.

ISO (2015) *International Standard, Information Technology – Security Techniques – Incident Investigation Principles and Processes*. [online]. Available from: ISO.org (Accessed 15 March 2023).

Jang-Jaccard, J. & Nepal, S. (2014) 'A survey of emerging threats in cybersecurity', in *Journal of Computer and System Sciences*. [Online]. 2014 Academic Press Inc. pp. 973–993.

Karie, N. M. & Karume, S. M. (2017) *Digital Forensic Readiness in Organizations DIGITAL FORENSIC READINESS IN ORGANIZATIONS: ISSUES AND CHALLENGES*.

Kebande, V. R. et al. (2018) *Adding Digital Forensic Readiness as a Security Component to The IoT Domain*. 8 (1).

Kebande, V. R. et al. (2020) Holistic digital forensic readiness framework for IoT-enabled organisations. *Forensic Science International: Reports*. [Online] 2100117.

Kebande, V. R. & Ray, I. (2016) 'A generic digital forensic investigation framework for Internet of Things (IoT)', in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*. [Online]. 23 September 2016 Institute of Electrical and Electronics Engineers Inc. pp. 356–362.

Kim, S. et al. (2020) Smart Home Forensics—Data Analysis of IoT Devices. *Electronics 2020, Vol. 9, Page 1215*. [Online] 9 (8), 1215. [online]. Available from: https://www.mdpi.com/2079-9292/9/8/1215/htm (Accessed 2 December 2022).

Leedy, P. D. & Ormrod, J. Ellis. (2001) *Practical research : planning and design*.

Meffert, C. et al. (2017) 'Forensic state acquisition from the Internet of things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition', in *ACM International Conference Proceeding Series*. [Online]. 29 August 2017 Association for Computing Machinery. p.

Mouhtaropoulos, A. et al. (2014) Digital Forensic Readiness: Are We There Yet? JICLT Journal of International Commercial Law and Technology 9 (3). [online]. Available from: http://www.cesg.gov.uk/products_services/iatp/documents/data_handling_review.pdf.

Ngobeni, S. et al. (2010) *IFIP AICT 337 - A Forensic Readiness Model for Wireless Networks*.

Oriwoh, E. & Sant, P. (2013) 'The forensics edge management system: A concept and design', in *Proceedings - IEEE 10th International Conference on Ubiqui-*

tous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013. [Online]. 2013 pp. 544–550.

Rahi, S. (2017) Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. *International Journal of Economics & Management Sciences*. [Online] 06 (02).

Sgurev, V. et al. (2020) *2020 IEEE 10th International Conference on Intelligent Systems (IS) : proceedings*.

Singh, A. et al. (2019) 'Digital Forensic Readiness Framework for Ransomware Investigation', in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*. [Online]. 2019 Springer Verlag. pp. 91–105.

Soltani, S. & Seno, S. A. H. (2019) A formal model for event reconstruction in digital forensic investigation. *Digital Investigation*. [Online] 30148–160.

SPEAR Project (2021) *Forensic Readiness in Critical Infrastructures - SPEAR Project*. [online]. Available from: https://www.spear2020.eu/News/Details?id=123 (Accessed 13 May 2023).

Surange Geetanjali & Khatri Pallavi (2021) '*IoT Forensics: A Review on Current Trends, Approaches and Foreseen Challenges*', in 2021 p.

Do Valle, J. M. et al. (2020) 'Big Data Platform for Analysing Crime Evidences', in *Proceedings - 2020 IEEE 6th International Conference on Big Data Computing Service and Applications, BigDataService 2020*. [Online]. 1 August 2020 Institute of Electrical and Electronics Engineers Inc. pp. 113–119.

Williams, C. (2007) Research Methods. Journal of Business & Economic Research-March 5.

Zainudin, N. M. et al. (2022) Digital Forensic Readiness for Cyber Security Practitioners: An Integrated Model. Journal of Positive School Psychology 2022 (3). [online]. Available from: http://journalppw.com.

Zawoad, S. et al. (2015) 'OCF: An Open Cloud Forensics Model for Reliable Digital Forensics', in *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*. [Online]. 19 August 2015 Institute of Electrical and Electronics Engineers Inc. pp. 437–444.

Žukauskas, P. et al. (2018) 'Philosophy and Paradigm of Scientific Research', in *Management Culture and Corporate Social Responsibility*. [Online]. InTech. p.

Appendix A: List Of Abbreviations

DF	Digital Forensic
DFI	Digital Forensic Investigation
DFR	Digital Forensic Readiness
IDS	Intrusion Detection System
I.T.	Information Technology
I.S	Information Systems
IoT	Internet of Things
DFRF	Digital Forensic Readiness Framework
DFRM	Digital Forensic Readiness Model
DFIF-IoT	Digital Forensic Investigation Framework for IoT
FSAIoT	Forensic State Acquisition from IoT
PDE	Potential Digital Evidence
DFI	Digital Forensic Investigator
FAIoT	Forensic Awareness Internet of Things
FIF	Forensic Investigation Framework
FEMS	Forensic Edge Management System
IoT-FR	Internet of Things Forensic Readiness
DDoS	Distributed Denial of Service
FIF-IoT	Forensic Investigation Framework for Internet of Things
HDFS	Hadoop Distributed File System
ISO	International Organisation for Standardization
IEC	International Electrotechnical Commission
DFF	Digital Forensic Framework