IoT

MDPI

Review

Systematic Analysis on the Use of AI Techniques in Industrial IoT DDoS Attack Detection, Mitigation, and Prevention

Mikiyas Alemayehu [1], Mohamed Chahine Ghanem [1,2,*], Hamza Kheddar [3], Dipo Dunsin [4] and Marcio J. Lacerda [5]

[1] School of Computer Science and Mathematics, Keele University, Newcastle-Under-Lyme ST5 5AA, UK; m.alemayehu@keele.ac.uk
[2] Cybersecurity Institute, University of Liverpool, Ashton Street, Liverpool L69 3BX, UK
[3] LSEA Laboratory, Electrical Engineering Department, University of Medea, Medea 26000, Algeria; kheddar.hamza@univ-medea.dz
[4] Department of Computing, the Institute of Inner City Learning London, University of Wales Trinity Saint David, London E14 4HA, UK; d.dunsin@uwtsd.ac.uk
[5] Cyber Security Research Centre, London Metropolitan University, London N7 8DB, UK; m.lacerda@londonmet.ac.uk
* Correspondence: m.ghanem@keele.ac.uk

Abstract

Distributed Denial of Service (DDoS) attacks pose significant threats to Industrial Internet of Things (IIoT) environments, exacerbated by the resource constraints of IoT devices and the disruptive impact of such attacks. Conventional detection and prevention methods fall short of ensuring the availability and operational continuity required in industrial deployments. This article systematically analyses artificial intelligence (AI) techniques for detecting, preventing, and mitigating DDoS attacks in IIoT systems. We examine diverse AI-driven solutions, including machine learning (ML) and deep learning (DL) models, alongside hybrid approaches that enhance real-time threat identification, adaptive defence mechanisms, and decentralised trust management, addressing the evolving sophistication of DDoS attacks. This study highlights AI's potential to strengthen IIoT security and resilience, particularly in critical national infrastructure (CNI), where uninterrupted operations are paramount. However, challenges such as computational overhead, model interpretability, and dataset scarcity in industrial settings remain critical barriers. Additionally, the dynamic IIoT topology and heterogeneous device ecosystems necessitate context-aware AI solutions. This analysis underscores the need for lightweight, explainable AI frameworks and collaborative defence strategies tailored to the IIoT's unique constraints. It emphasises the integration of AI with emerging technologies like edge computing and federated learning to advance proactive, scalable DDoS defence mechanisms in industrial ecosystems.

Keywords: artificial intelligence; IoT; IIoT; critical national infrastructure; resilience; DDoS; machine learning; deep learning; cyber security

Academic Editors: Xianzhong Ding, Kang Yang and Saurabh Garg

Received: 2 May 2026
Revised: 23 June 2026
Accepted: 26 June 2026
Published: 30 June 2026

1. Introduction

This paper systematically analyses artificial intelligence (AI)-based Distributed Denial of Service (DDoS) attack detection techniques in the context of the Industrial Internet of Things (IIoT), while also highlighting some conventional and blockchain (BC)-based approaches. The Introduction covers the context and motivation, problem statement, research objectives, and structure of this paper.

1.1. Context and Motivation

The Internet of Things (IoT) refers to the interconnection of a large number of devices over the Internet that perform tasks including sensing, actuating, and communicating [1]. Some research indicates that approximately 38.6 billion IoT devices will be connected to the Internet by 2025, a figure that could reach 50 billion by 2030 [2]. However, predictions vary; for example, [3] states that there will be over 75 billion IoT devices generating revenue of over 10 trillion dollars in 2025. The rapid growth of the IoT is increasingly evident. The IoT connects various smart devices to the Internet, forming large networks. As a result, more data and user privacy are exchanged [4]. The IoT enables heterogeneous connections of smart devices worldwide, leading to a ubiquitous terminal for the interconnection of emerging technologies in areas including healthcare, home automation, smart cities, and the automotive field [5]. Following the increase in implementation and data transmission, the security of the IoT has become a pressing concern [4,6]. The large-scale interconnection makes IoT environments vulnerable to cyber threats and attractive to malicious actors [5].

The Industrial IoT refers to the application of IoT in the manufacturing and industrial sectors [1]. Industrial computer networks are designed to enable machine-to-machine (M2M) communications, where devices control and monitor other devices with minimal human intervention. These devices are built with limited computational resources such as memory, central processing units (CPUs), and in some wireless sensor network instances, battery-based nodes [7,8]. They are connected to the Internet and used in various industrial sectors, including oil, gas, military, agribusiness, and biological applications [9]. The development of Internet technology, transformation in industrial manufacturing systems, and advances in communications technology have driven the IIoT toward deeper and larger interconnection. The IIoT plays a significant role in industrial reform, acting as a bridge that connects the new Internet industry to traditional industrial systems, enabling upgrades. The IIoT is a combination of digital devices (such as actuators and sensors) and physical devices [10]. Confidentiality, integrity, and availability are common security goals in both the IoT and IIoT. Other implicit properties, such as resource constraints in agricultural and medical applications, are also common. Therefore, a general understanding of the IoT, including its properties, characteristics, and vulnerabilities, is important in order to better understand and leverage the IIoT [1]. The resource-constrained IIoT environment is vulnerable to various DDoS attacks. To address these, approaches including conventional techniques, as well as BC-based, ML-based, and DL-based methods, have been implemented, as illustrated in Figure 1.

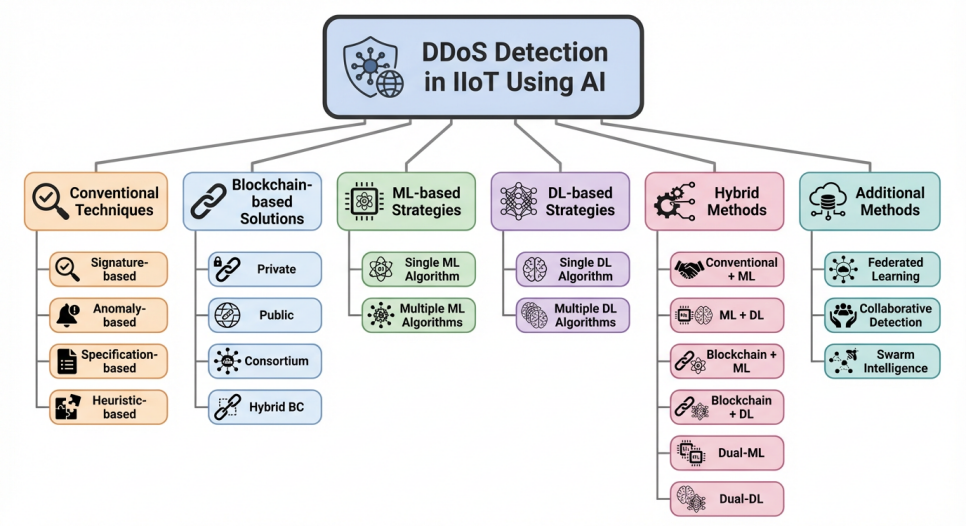

Figure 1. DDoS attack detection techniques in the IIoT.

1.2. Problem Statement

The Industry 5.0 revolution describes the smart factory ecosystem, which depends on fog computing, cloud computing, drones, BC, 5G/6G communications, and AI. Optimised operation and cost reduction are enabled by connecting the Internet to machines using the IIoT, gathering data at the edge and in the cloud using AI. However, deploying IIoT systems in open fields has made Industry 5.0 vulnerable to various cyber-attacks, including DDoS attacks [11]. The IIoT manages data generated in industrial production areas and supports intelligent industrial production, playing a significant role in ensuring production continuity and management. However, the large volume of data in this environment creates a high risk of cyber-attacks, threatening production and management. The rapid development of the IIoT has made industrial network structures more complex, leading to demanding expectations for defence mechanisms [10].

IIoT devices are vulnerable because they lack built-in security features that defend against threats. Low computational power and confined environments are the main reasons for these vulnerabilities, making traditional intrusion detection systems (IDSs)such as anomaly-based and signature-based techniques inefficient. Weak passwords and the absence of password usage on data are among the critical security flaws in IIoT environments. Most IIoT systems have weak default passwords or none at all. These vulnerabilities enable threat actors to exploit IIoT devices and conduct damaging assaults that can endanger user privacy [12]. The differences between the IoT and IIoT call for stricter security approaches in the IIoT. Although benefits outweigh threats, IIoT environments remain vulnerable due to computational and storage limitations. These limitations leave the IIoT vulnerable to cyber-attacks including phishing, malware, authentication attacks, DNS spoofing, SQL injection, reverse engineering, and web application attacks. Among these, the threat to availability posed by DDoS attackswhich work by exhausting system loopholes, is particularly concerning. DDoS attacks make a system or resource unavailable to legitimate users indefinitely [1].

To mitigate DDoS attacks in IIoT environments, alternative methods to traditional approaches include BC-based techniques. For instance, Ref. [13] highlights infrastructure security and data protection in IIoT systems, combining a BC-based data model for transparency with data security measures including authentication mechanisms and privacy protection protocols. The proposed method addresses data security through multiple layers of protection, focusing on practical implementation in industrial settings. Environmental factors are also considered. However, this approach is challenged by resource constraints and the low processing power of IIoT systems.

1.3. Research Objectives and Contributions

This paper aims to address the challenges of securing IIoT environments against DDoS attacks by leveraging AI and ML techniques. The objectives and contributions are as follows:

1. To analyse current state-of-the-art AI approaches for detecting and preventing DDoS attacks in IIoT environments. This includes evaluating the approaches, performance, and effectiveness of existing AI-based models in identifying and mitigating DDoS attacks in IIoT systems.
2. To identify gaps in existing solutions and challenges in practical deployment. By conducting a critical literature review of conventional, BC-based, ML-based, DL-based, and hybrid techniques, this research uncovers unaddressed limitations, issues, and bottlenecks in applying AI and ML approaches to real-world IIoT environments.
3. To propose future research directions and innovations for advancing security in IIoT systems. This research outlines actionable insights and recommends approaches to

bridge research gaps and advance the reliability of AI- and ML-based DDoS detection and mitigation techniques in IIoT environments.

1.4. Structure of the Paper

This systematic review is structured to provide a comprehensive understanding of DDoS attacks in IIoT systems. Section 2 describes the review methodology, including the review framework, search strategy, inclusion and exclusion criteria, and data extraction and analysis. Section 3 provides an overview of the IIoT, the nature of DDoS attacks in IIoT systems, and a summary of AI techniques for DDoS detection and mitigation, while also highlighting conventional and BC-based techniques. Section 4 presents results and analysis by exploring key findings, themes, and categories, organising the results into major themes, and providing quantitative insights and case studies. Section 5 reviews related survey and SLR papers. Section 6 reports key findings. Section 7 delves into critical evaluation, exploring challenges, emerging trends, and research gaps, and offers multi-stage recommendations for practitioners and researchers, along with policy suggestions to guide future developments. Section 8 concludes the systematic analysis with a summary, prospects for future work, and final remarks. Figure 2 illustrates the structure of the paper.

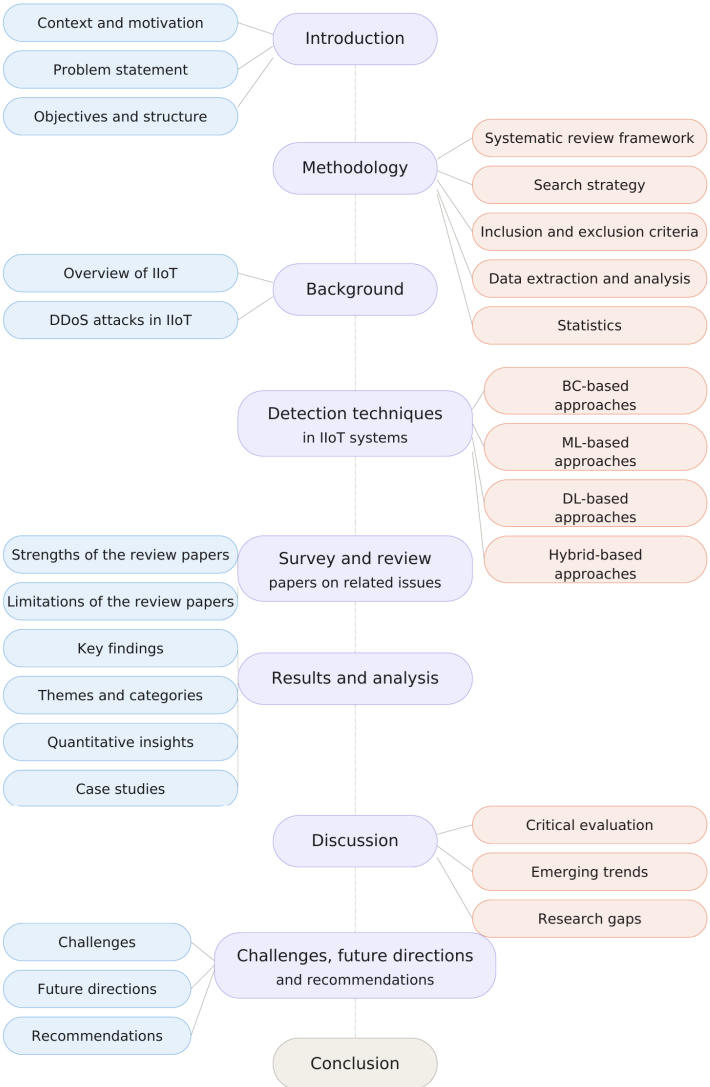

Figure 2. Structure of the systematic literature review, illustrating the sequential flow across methodology, background, comprehensive detection techniques, related survey analysis, key results, critical discussion, and conclusions, with each section building upon the findings of the previous one.

2. Materials and Methods

This section presents the systematic approach undertaken to conduct a systematic literature analysis on the use of AI and ML techniques for detecting and mitigating DDoS attacks in IIoT environments, while underlining the limitations of conventional techniques. The review adheres to a structured approach to guarantee comprehensiveness, following established guidelines for systematic literature reviews.

2.1. Research Questions and Objectives

The review process aims to address the following research questions:

RQ1: What are the limitations of conventional and BC-based DDoS detection techniques?
RQ2: What AI techniques have been used for detecting and mitigating DDoS attacks in IIoT environments?
RQ3: What are the key strengths, gaps, limitations, and challenges in mitigating DDoS attacks in IIoT systems?
RQ4: What research strategy could address the identified limitations to enhance the security of IIoT environments?

The corresponding objectives are outlined below:

1. To identify and analyse the shortcomings of traditional and BC-based DDoS detection methods, highlighting areas that require improvement.
2. To explore the role of AI-driven approaches in DDoS detection and mitigation within the IIoT, assessing their effectiveness and applicability.
3. To systematically examine existing methodologies, pinpoint their advantages and limitations, and identify unresolved challenges in securing the IIoT against DDoS threats.
4. To propose a comprehensive research direction that effectively addresses the identified gaps while ensuring a more resilient IIoT security framework.

2.2. Search Strategy

The systematic literature review (SLR) was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. PRISMA outlines a four-phase process; identification, screening, eligibility, and inclusion designed to ensure that only the most relevant and high-quality studies are considered. This structured approach promotes transparency, streamlines the review process, and enhances the reliability of the findings. An extensive search was conducted across major academic databases including IEEE Xplore, Scopus, Web of Science, and SpringerLink to locate comprehensive studies. These databases were selected based on their broad coverage of peer-reviewed literature in computer science, technology, and engineering. The research time frame was limited to publications between 2018 and 2025, reflecting recent advances in the field.

Keywords and Boolean operators were used as search strategies to maximise relevance. The selected keywords included AI, IoT, IIoT, Industrial IoT, Security, DDoS, ML, anomaly detection, and IDS. Boolean operators such as OR, AND, and NOT were used to structure keyword combinations and enhance the search relevance. In addition, parameters such as limiting to papers written in English and focusing more on the IIoT than the generic IoT were applied.

2.3. Study Selection and Screening Process

By applying rigorous inclusion and exclusion criteria, as explained in Table 1, we ensured that the studies were directly relevant to the objectives of the systematic analysis.

Table 1. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Peer-reviewed journal articles, conference proceedings, technical reports, and research articles published between 2018 and 2025.	Published before 2018.
Address the use of AI and ML techniques for the detection and mitigation of DDoS attacks in IIoT environments.	Do not discuss DDoS detection, DDoS mitigation, IIoT, IDS, or AI techniques.
Provide empirical results that demonstrate DDoS attack detection and mitigation in IIoT environments.	Lack empirical data and are solely theoretical without validation.
Discuss performance evaluation, including accuracy, precision, recall, F1-score, confusion matrix, execution time, and CPU usage.	No specific exclusion criteria applied for performance metrics.

2.4. Data Extraction and Analysis

Relevant studies were reviewed carefully to extract only relevant data systematically. Data extraction captured relevant aspects of each study.

AI Techniques: The specific AI-based approaches used for DDoS attack detection and mitigation were documented. These included traditional ML techniques such as *k*-nearest neighbours (KNN), support vector machine (SVM), and decision trees (DTs); DL techniques such as recurrent neural networks (RNNs), convolutional neural networks (CNNs), and long short-term memory (LSTM); and hybrid approaches that combine multiple methods. Limitations of conventional and BC-based techniques were also highlighted [14]. These techniques enable dynamic updates and continuous model refinement, as shown in Figure 3.

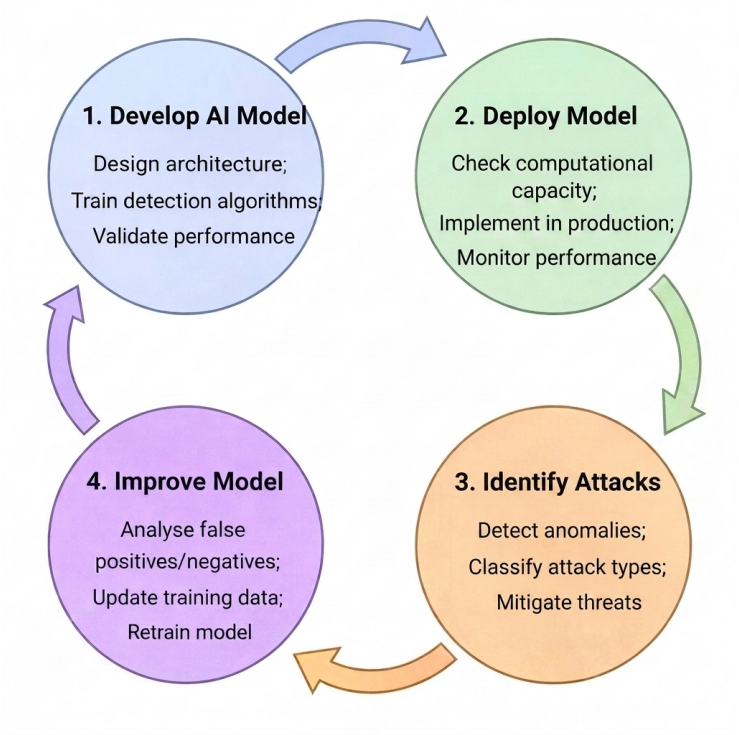

Figure 3. Life cycle of AI-based DDoS detection. A cyclical process for developing, deploying, and improving AI-bases IDS models.

Performance Metrics: Performance evaluation is emphasised by employing standard metrics including the confusion matrix, precision, recall, and the area under the receiver

operating characteristic curve. Particular emphasis is placed on comparing these metrics to assess model effectiveness comprehensively.

Performance metrics used to evaluate the models include accuracy, precision, recall, and F1-score. These metrics are detailed in Table 2.

Table 2. Performance metrics and their descriptions.

Metric	Mathematical Description	Description
Accuracy	$\frac{TP+TN}{TP+FP+FN+TN}$	Measures the proportion of correctly identified flows (both malicious and benign) out of all flows.
Precision	$\frac{TP}{TP+FP}$	Measures the proportion of correctly identified malicious flows out of all predicted malicious flows.
Recall	$\frac{TP}{TP+FN}$	Measures the proportion of correctly predicted malicious flows out of all actual malicious flows.
F1-score	$2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$	The harmonic mean of precision and recall, providing a balanced evaluation.

Note: TP (true positive); malicious traffic correctly identified as malicious, TN (true negative); benign traffic correctly identified as benign, FP (false positive); benign traffic incorrectly identified as malicious, and FN (false negative); malicious traffic incorrectly identified as benign.

In addition, efficiency is measured by CPU processing time.

Computational Effectiveness: Due to resource constraints in IIoT systems, approaches are examined based on computational efficiency, including memory requirements, suitability for edge IIoT or fog computing deployment, and training and inference time. The extracted data are synthesised to highlight recurring trends and gaps. A thematic approach groups findings into categories such as deployment techniques, research gaps, and challenges. This is then used to identify the current state of the study and inform recommendations for future work [15].

2.5. Statistics

We distributed the papers by category. Conventional approaches account for 16 papers (19.51%), BC-based techniques for 7 papers (8.54%), ML-based approaches for 13 papers (15.85%), DL-based approaches hold the highest share with 33 papers (40.24%), and hybrid approaches hold 13 papers (15.85%), as indicated in the pie chart in Figure 4. Our review is limited to papers between 2018 and 2025 due to relevance. This indicates that the detection and mitigation of DDoS attacks in IIoT environments has gained attention primarily within this period.

Our research indicates many publications between 2023 and 2025, with 2023 and 2024 taking the lead. This trend holds for AI-based techniques as well as conventional and BC-based approaches, as presented in Table 3.

Table 3. Number of papers published per category over the years.

Category	Papers by Year	Total
Conventional	2018 (1), 2019 (2), 2020 (3), 2022 (3), 2023 (4), 2024 (1), 2025 (2)	16
BC-based	2020 (1), 2021 (1), 2022 (1), 2023 (1), 2024 (1), 2025 (2)	7
ML-based	2020 (1), 2023 (6), 2024 (3), 2025 (3)	13
DL-based	2020 (2), 2021 (4), 2022 (4), 2023 (6), 2024 (15), 2025 (2)	33
Hybrid-based	2020 (2), 2021 (2), 2022 (3), 2023 (2), 2024 (1), 2025 (3)	13
Total Overall		82

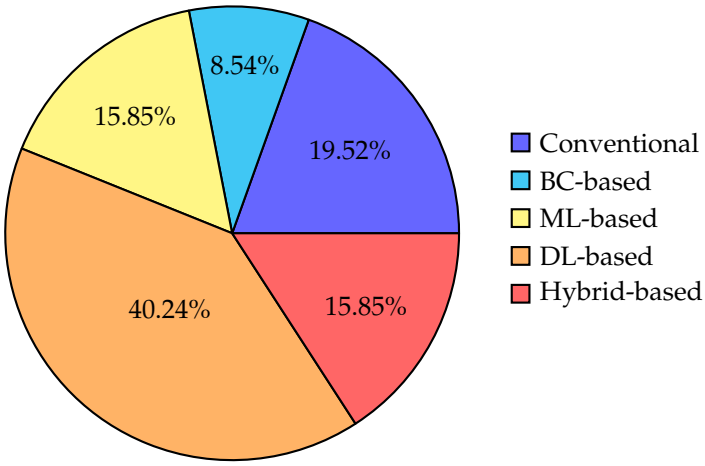

Figure 4. Distribution of research papers by category.

Considering the progress and decline in publications, conventional approaches are gaining less attention, while ML and DL are increasingly attracting interest. The addition of 2025 papers further reinforces the growing momentum of ML and hybrid approaches. This trend is visualised in the bar chart in Figure 5.

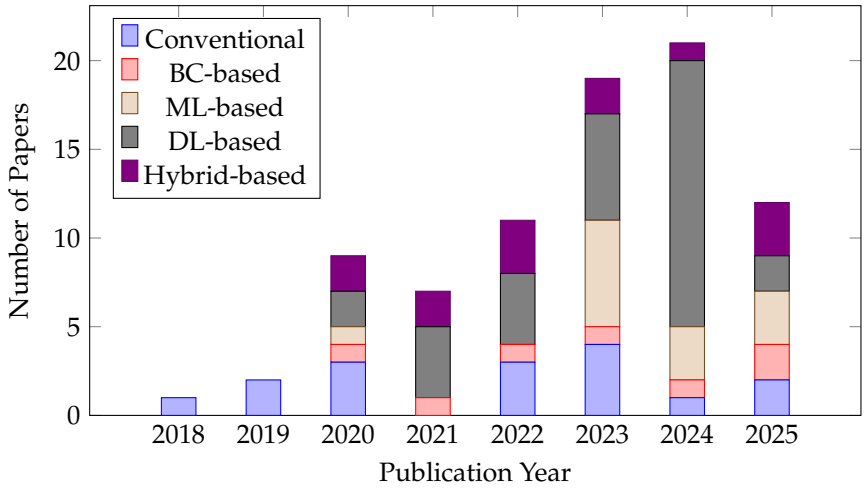

Figure 5. Research progress across years for different techniques (2018–2025).

3. Background

3.1. Overview of IIoT

The industrial sector enabled the revolution of the IIoT, which is now used in various sectors including smart grids, smart healthcare, smart logistics, smart transportation, smart manufacturing, smart traffic monitoring, and UAV network monitoring. The IIoT enables production efficiency and data optimisation for both security and production [16]. The IIoT is an enormous ecosystem that provides reliable communication and control systems, as well as actuator and sensor connections at the industrial level. Enterprise networks are globally enabled by heterogeneous communication that connects the IIoT architecture. Real-time capability and intelligence are provided to machines by IIoT systems to gather and analyse data, enhancing decision-making processes. This allows autonomous operation with minimal human intervention [17].

Smart grids are now equipped with industrial control systems (ICSs) incorporating communication technology using systems like supervisory control and data acquisition (SCADA) [18]. Due to the ubiquitous, intelligent automation and connectivity advantages

brought to industrial productivity by the IIoT, it is considered to be an emerging paradigm. The level of industrial manufacturing and the quality of monitoring capabilities of numerous devices are achieved by applying intelligent equipment in the IIoT. To improve the quality of service in IIoT networks, edge computing has become a solution that meets requirements. The shift from cloud to edge computing enables real-time communication and congestion avoidance with small amounts of data exchange. Despite the benefits of edge computing, IIoT management complexity and the difficulty of security scenarios have dramatically increased. Many IIoT devices have limitations in computational power and are vulnerable to attacks due to the locations where they are distributed [19]. Figure 6 highlights the diversity of IIoT ecosystems, including smart manufacturing, smart logistics, smart healthcare, and smart grids.

Resource limitations exist in edge clouds within IIoT environments. Delay-sensitive applications must also be considered, particularly regarding downtime during mitigation. An SDN-based IIoT system consists of a remote cloud, multiple devices, and several edge clouds. The device plane comprises devices that handle communication and data collection within edge clouds, including cameras, sensors, etc., as illustrated in Figure 6. Access points and their corresponding edge clouds form the data plane, which processes data collected from devices. The SDN controller, part of the control plane, maintains the global topology and manages network communications [20]. Utilising baseline network flow monitoring capabilities and predefined flow policies, the SDN control plane continuously captures network status to detect malicious traffic. When malicious traffic is identified at an edge cloud, the SDN controller updates it accordingly [17].

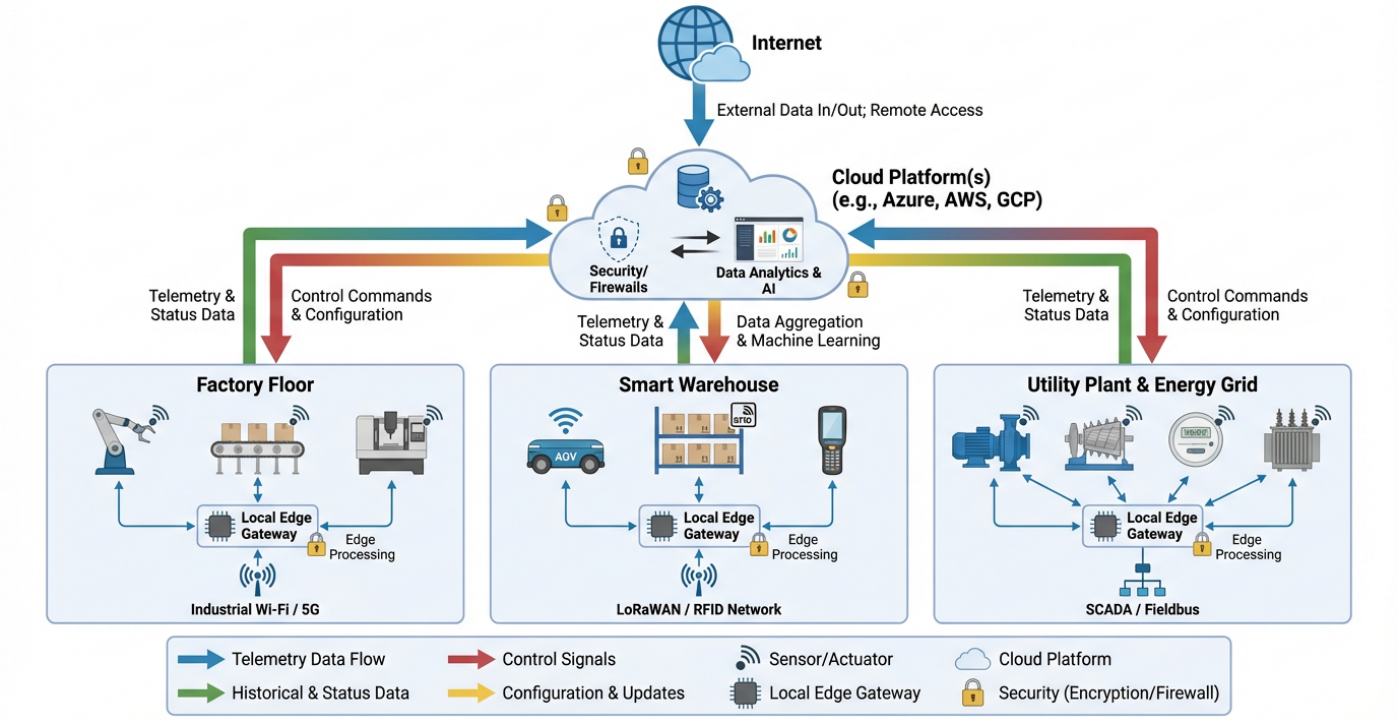

Figure 6. IIoT ecosystem.

3.2. DDoS Attacks in the IIoT

Unprecedented production control and monitoring systems have been made possible by IIoT systems [21]. Multiple systems are placed in the command centre, making it easy to process industrial data by leveraging integrated management [22]. The primary reason for analysing smart manufacturing data is to improve efficiency and security in production

environments [23]. However, this open and complex environment faces network security concerns [22].

In [24], the vulnerability of production lines with IIoT implementation when subjected to DDoS attacks is analysed. The paper highlights how integrating the IIoT into production systems increases vulnerability. The research uses an experimental analysis approach by testing direct DDoS flood attacks and DDoS reflective attacks. The vulnerability of IIoT-enriched production lines is tested in a real-world environment. Problematic IoT device detection is also conducted. The paper highlights that the default settings of IIoT-based production lines are not secure against DDoS attacks and are computationally limited. The production line assessment is based on communication resilience, sensor behaviour under attack scenarios, and production process disruptions. The results indicate that DDoS attacks successfully disrupted the production process and made IIoT communications dysfunctional. The research also demonstrates that DDoS attacks are devastating in production environments, applicable to broad Industry 4.0 implementations.

The authors of [25] developed a DDoS simulation model for determining DDoS attack vectors on a programmable logic controller in an IIoT environment. The research primarily aimed to determine the time required to launch a successful DDoS attack in an IIoT environment and to calculate the maximum response time. A queuing system-based simulation model (network simulation) was implemented in Python 3 for modelling sequential processes of DDoS attacks. The model can predict DDoS execution time using probability-based calculations and uses exponential distribution for modelling process duration. The model does not address specific DDoS types but focuses on attack impact, showing a probability value of 0.7 to 0.9999, with mean attack times ranging from 79.97 to 88.01 s.

The authors of [26] explored the time distribution laws for conducting DDoS attacks in IIoT networks through a natural experimental approach consisting of a conceptual model for studying DDoS attack implementation time, practical DDoS attacks using Bash scripting and UDP request generation, and statistical analysis of time distributions. UDP flood requests target PLCs. Direct switch connection and workstation-based attacks are used for implementation. The approach measures the time of successful attack simulation. Initial connection loss is detected within 7 to 8 s after attack initiation, and complete communication termination occurs between 70 and 80 s. The practical experimental setup uses real-world industrial components and tests multiple attack scenarios but is limited to UDP flood attacks.

In [27], the critical issues of security and digital forensics within the IIoT ecosystem are discussed. The paper highlights cybersecurity vulnerabilities resulting from increased connectivity and the need for robust forensic mechanisms. ML approaches, such as supervised learning, are highlighted due to the emergent configuration of IIoT systems, which require advanced analytics to ensure security and integrity. DDoS attacks are highlighted as disruptive in industrial environments, compromising network integrity. ML techniques are deemed promising for enhanced threat detection. The paper suggests that success can be measured by effective incident response times, accuracy of threat detection, and continuity maintenance during attacks.

DDoS attacks are among the critical security threats in IIoT environments. These attacks can be classified into three broad categories: flood attacks, reflective attacks, and amplification attacks. Table 4 defines these and other types, along with their impacts. Regardless of the type, exhausting resources is fundamental to DDoS attacks, which is precisely why IIoT systems are vulnerable due to their resource limitations [22].

Geographic Distribution of DDoS Attacks

According to NETSCOUT's DDoS Threat Intelligence Report for the second half of 2025, which monitored more than 8 million DDoS attacks across 203 countries and territories, the EMEA region experienced the highest attack volume globally, with 3,331,570 events, followed by APAC with 1,904,602, North America with 1,272,625, and Latin America with 1,014,148 [28]. At the campaign level, the hacktivist group Keymous conducted 249 DDoS attacks across 60 organisations in 21 industries and 15 countries between February and September 2025, with geographic concentration in Morocco, Saudi Arabia, Sudan, India, and France. Geopolitical factors are a significant driver of these patterns: hacktivist groups including NoName057(16) and Keymous persistently targeted government, transportation, and financial services infrastructure, with attack volumes spiking in direct response to elections, military operations, and geopolitical tensions. For IIoT-specific deployments, countries with high concentrations of critical infrastructure, energy grids, and industrial manufacturing face elevated exposure, as critical infrastructure including DNS and NTP services experienced sustained attack pressure throughout the period [28]. Regional attack percentage is illustrated in Figure 7.

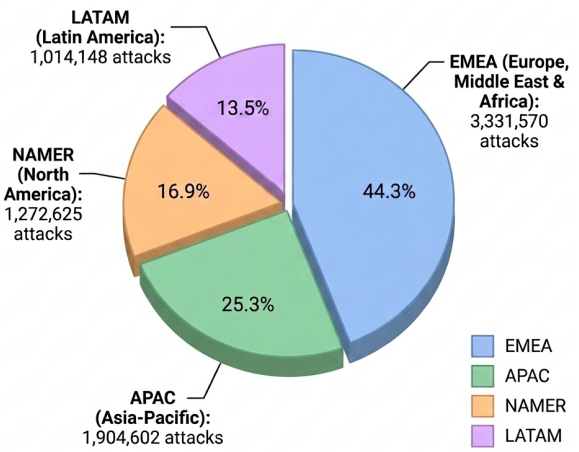

Figure 7. Regional distribution of DDoS attacks in 2H 2025, based on NETSCOUT ATLAS global threat intelligence covering 203 countries and territories [28].

Table 4. Hierarchical taxonomy of DDoS attacks in IIoT environments classified by attack layer, attack class, mechanism, and operational impact.

OSI Layer	Attack Class	Attack Type	Mechanism	IIoT Impact
Network (L3)	Volume-based	ICMP Flood, Spoofed-Packet Flood	Saturates bandwidth through high-volume traffic	Disrupts sensor-to-gateway communication; high severity
Transport (L4)	Protocol Exploitation	TCP SYN Flood, UDP Flood, Ping of Death, Smurf	Exploits stateful protocol handshakes to exhaust connection tables	Disables PLC and SCADA communication channels; critical severity
Transport (L4)	Amplification/Reflection	NTP Amplification, DNS Reflection	Exploits third-party servers to magnify traffic directed at the target	Overwhelms IIoT gateways with limited bandwidth; high severity
Application (L7)	Application Layer	HTTP GET/POST Flood, Modbus Flood, Slow HTTP	Mimics legitimate requests to exhaust application resources	Targets industrial web interfaces and control APIs; hard to detect; critical severity
Multi-layer	Low-rate/Stealthy	Slow-rate DDoS, Pulsing Attacks	Sends traffic below detection thresholds to gradually degrade service	Particularly dangerous in IIoT due to difficulty of detection against periodic traffic; high severity
Multi-layer	Zero-Day	Unknown protocol or application flaws	Exploits undisclosed vulnerabilities before patches are available	Circumvents all signature-based defences; critical severity in CNI

DDoS attacks can also be classified based on impact (high, medium, low) and attack target (IoT devices, IIoT devices, general industrial infrastructure).

3.3. IIoT Traffic Characteristics and Protocol-Aware Detection

A critical but frequently overlooked dimension of DDoS detection in the IIoT is the fundamental difference between IIoT network traffic and the generic IT or consumer IoT traffic on which most AI-based detection models are trained. Understanding these distinctions is essential because detection models that perform well on generic traffic benchmarks may fail silently when deployed in real industrial environments where traffic exhibits entirely different statistical properties.

Distinctive Characteristics of IIoT Traffic: IIoT network traffic is characterised by strong temporal regularity and periodic communication patterns that reflect the deterministic nature of industrial control processes. Sensors, actuators, PLCs, and SCADA systems communicate on fixed schedules, producing traffic with highly predictable inter-arrival times, packet sizes, and flow durations [29]. This periodicity is fundamentally different from the bursty, user-driven traffic patterns found in IT and consumer IoT environments, and it has direct implications for anomaly detection: statistical features such as entropy, variance, and packet rate, which are effective discriminators in IT contexts, may be uninformative or misleading when applied to the deterministic traffic of an industrial control loop [1]. Low-rate and stealthy DDoS attacks are particularly dangerous in IIoT environments precisely because they are designed to blend into this periodic traffic. By sending attack traffic at rates below detection thresholds and mimicking the timing patterns of legitimate industrial communications, adversaries can gradually degrade service availability without triggering conventional anomaly detectors. Among the reviewed approaches, only a small subset specifically addresses low-rate DDoS in IIoT contexts [3,30,31], and these represent an important but underdeveloped research direction. Furthermore, IIoT networks are highly sensitive to timing disruptions: even small increases in latency caused by attack traffic or mitigation responses can violate the real-time constraints of industrial control systems, causing process instability or safety system activation [24,29].

Protocol-Aware Detection for Industrial Communication Stacks: The majority of AI-based DDoS detection approaches reviewed in this paper operate exclusively at the network layer, relying on features such as packet size, flow rate, byte counts, and IP header statistics. While these features are useful for detecting volumetric and protocol-exploitation attacks, they are fundamentally blind to application-layer attacks that exploit the semantics of industrial communication protocols. IIoT environments rely on a distinct set of application-layer protocols that carry operational significance beyond what network-layer statistics can capture [32]. Modbus/TCP, one of the most widely deployed industrial protocols, structures communication as function-code-based requests between a master and slave devices. Abnormal function code usage, illegal register access attempts, or flooding of Modbus request queues represent application-layer DDoS vectors that are entirely invisible to classifiers operating only on IP flow statistics. The rule-based detection mechanism of [33], which analyses Modbus/TCP transactions using function-code-level inspection, is one of the few reviewed approaches that addresses this gap, but it is limited to known attack signatures and cannot adapt to novel Modbus abuse patterns. OPC-UA (Open Platform Communications Unified Architecture) is increasingly adopted in modern IIoT deployments as a platform-independent communication standard. Its session-based architecture, certificate-based security model, and complex service invocation patterns introduce attack surfaces that differ substantially from those of Modbus, including session hijacking, service flooding, and certificate exhaustion attacks that require protocol-semantic awareness to detect [32]. Similarly, Profinet, widely used in manufacturing automation, operates with

strict real-time guarantees and cycle-time requirements that make it particularly vulnerable to timing-based DDoS attacks that disrupt communication schedules without necessarily generating high traffic volumes [29]. The absence of protocol-aware detection in the reviewed literature represents a significant blind spot. Future AI-based IIoT DDoS detection systems should incorporate industrial protocol parsers as feature extraction components, enabling detection of illegal control-command sequences, abnormal function-code distributions, and protocol-state violations that are the hallmarks of application-layer IIoT attacks. This requires close collaboration between cybersecurity researchers and industrial automation engineers to develop protocol-level feature sets that accurately capture malicious behaviour without generating excessive false positives from legitimate but unusual operational commands.

4. Comprehensive DDoS Attack Detection Techniques in IIoT Systems

The evolution of DDoS detection techniques in IIoT environments reflects a progressive response to the limitations of each preceding generation of solutions. Conventional approaches, while fast and computationally inexpensive, proved insufficient against the growing sophistication and volume of attacks. Blockchain-based solutions addressed trust and transparency deficiencies but introduced resource overheads incompatible with constrained IIoT devices. ML techniques emerged to provide adaptive, data-driven detection but required large labelled datasets and struggled with evolving threats. Deep learning methods advanced detection accuracy further through automated feature extraction, yet at the cost of increased computational complexity. Hybrid approaches sought to reconcile these trade-offs by combining the strengths of multiple paradigms. The following subsections analyse each category in turn, highlighting not only individual contributions but also the broader limitations that motivated the transition to the next generation of solutions. As illustrated in Figure 8, DDoS attack mechanisms have undergone significant transformation over two decades, progressively shifting from simple bandwidth-exhausting volumetric floods toward increasingly sophisticated and targeted threats. The emergence of IoT botnets, most notably Mirai in 2016, marked a turning point by weaponising resource-constrained connected devices at scale. More recently, attacks have evolved to directly target IIoT-specific protocols such as Modbus and OPC-UA, exploit vulnerabilities in PLCs and SCADA systems, and employ low-rate stealthy techniques deliberately designed to evade conventional detection thresholds. This evolutionary trajectory underscores why static, rule-based defence mechanisms have become progressively inadequate, and why adaptive AI-based detection approaches are essential for securing modern IIoT environments against an ever-advancing threat landscape.

Cyber-attacks such as DDoS have become critical in IIoT environments [29]. DDoS attacks in the IoT and IIoT are widely discussed due to their disadvantageous impact and wide attack surface [34]. To address these challenges, researchers have proposed various solutions, including conventional techniques, BC technology, ML, DL, and hybrid approaches that combine two or more techniques, as shown in Figure 9.

The following sections cover the approaches, along with their strengths, weaknesses, datasets used for evaluation, and evaluation metrics. Additionally, Table 5 highlights their effectiveness by categorising the reviewed approaches based on zero-day attack efficiency, speed, accuracy, computational expense, dataset requirements, and scalability.

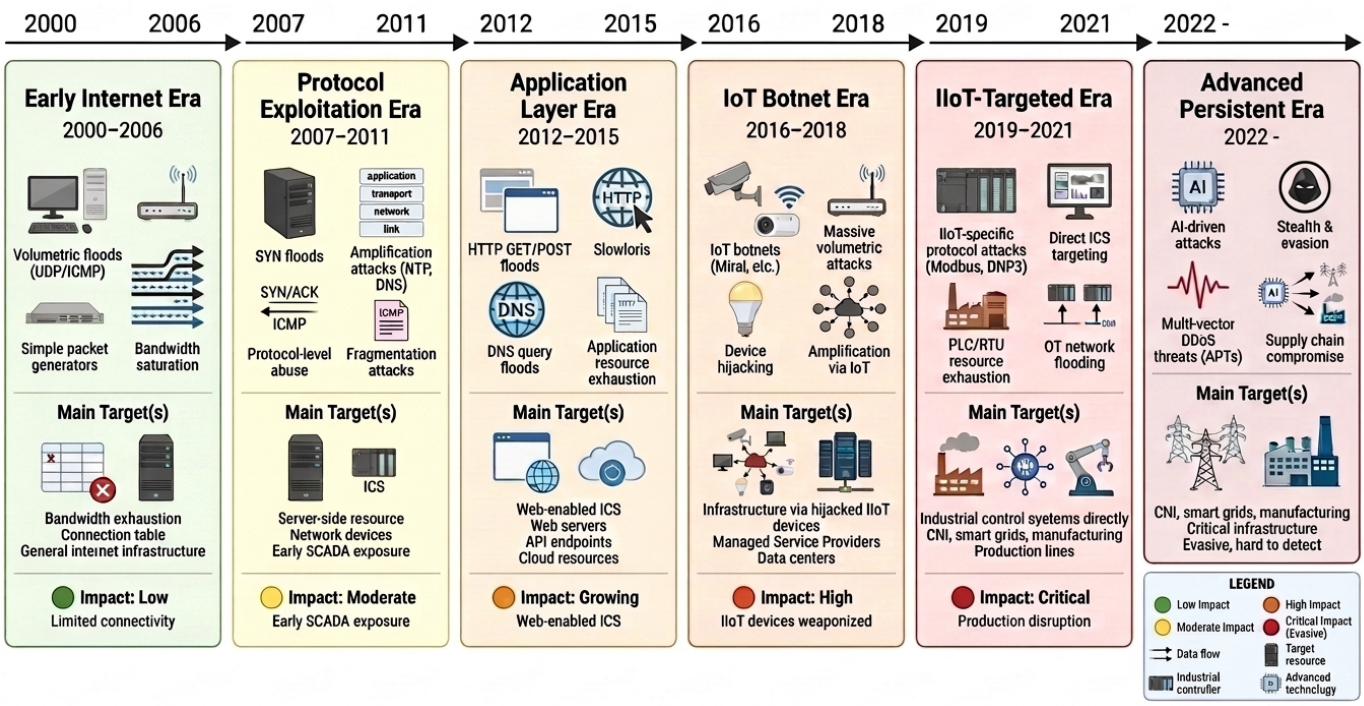

Figure 8. Evolution of DDoS Attack Mechanisms and Their Intensifying Impact on IIoT Environments Since 2000).

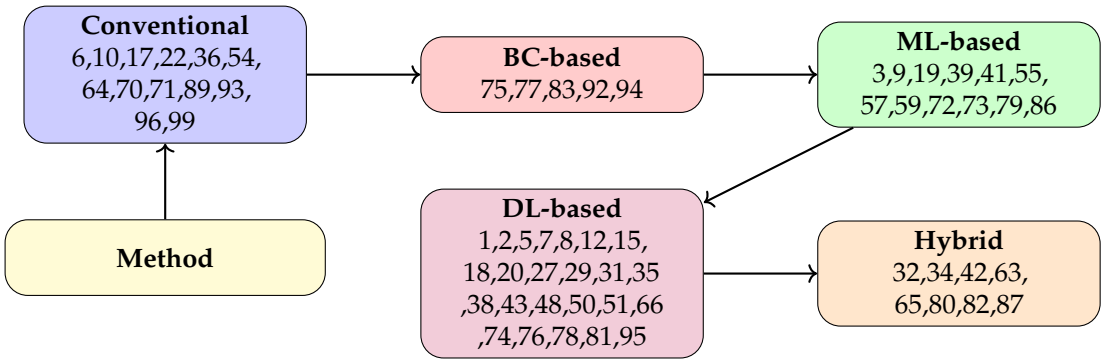

Figure 9. Categories of papers by method.

Table 5. Comparison of different security approaches in the IIoT.

Approach	Zero-Day Eff.	Speed	Accuracy	Computational Cost	Dataset Size Req.	Scalability
Conventional	Moderate	Fast	Medium	Low to Medium	Small to Medium	Limited
BC-based	Low to Mod.	Moderate	High	Medium	Medium	High
ML-based	High	Fast	High	Medium	Large	Mod. to High
DL-based	Very High	Moderate	Very High	High	Very Large	High
Hybrid	High	Fast	Very High	Med. to High	Large	High

To systematically contextualize these varied solutions, we first establish a structured taxonomy of DDoS detection approaches in IIoT environments. Table 6 categorizes existing methods into conventional, BC-based, ML-based, DL-based, and hybrid paradigms across five analytical dimensions, including detection paradigm, learning type, deployment tier, IIoT suitability, and zero-day capability. Within this taxonomy, the conventional category, characterized by rule-based or anomaly-based detection and non-learning paradigms serves as the foundational baseline against which more advanced techniques are compared.

Table 6. Structured taxonomy of DDoS detection approaches in IIoT environments across five analytical dimensions.

Category	Detection Paradigm	Learning Type	Deployment Tier	IIoT Suitability	Zero-Day Capability	Example Refs
Conventional	Rule-based/Anomaly	Non-learning	Edge/Fog	Moderate (low overhead)	Low	[33,35,36]
BC-based	Trust/Consensus	Non-learning	Fog/Cloud	Limited (high overhead)	Low	[37–39]
ML-based	Classification/Clustering	Supervised/Unsupervised	Edge/Fog/Cloud	High (lightweight models available)	Moderate	[3,40–42]
DL-based	Deep Feature Extraction	Supervised/RL/FL	Fog/Cloud	Moderate (high compute cost)	High	[17,43–45]
Hybrid	Multi-paradigm Fusion	Combined	Edge/Fog/Cloud	High (balanced trade-off)	High	[46–49]

4.1. Conventional Approaches for DDoS Attack Detection

DDoS attacks are a long-standing cyber threat that poses significant challenges. Conventional techniques, including anomaly detection, signature-based detection, edge-based solutions, and other IDS-integrated solutions, have been leveraged. The following section highlights some of these solutions.

The work in [35] addresses DDoS attacks in SDN-based IIoT environments by introducing anti-honeypot attack identification and proposing countermeasures. The authors implement a game theory-based approach called the Pseudo-Honeypot Game strategy. The paper underlines how DDoS attacks overwhelm SDN controllers in IIoT environments, and how SDN manages and protects IIoT devices. This is the first study to examine honeypot deployment for DDoS attacks in SDN environments. The approach is evaluated based on energy consumption and detection rate. However, the anti-honeypot attack significantly reduces the detection rate compared to the single honeypot game model, indicating that the defence mechanism is vulnerable.

The authors of [36] propose a multi-level DDoS mitigation framework using the SDN approach. The proposed framework operates across three levels: edge computing, fog computing, and cloud computing. It combines edge computing's quick response, fog computing's state awareness, and cloud computing's processing power. This technique is evaluated based on time consumption and enables multi-level security protection. However, handling and processing large amounts of data remains unaddressed.

The authors of [16] discuss security challenges in SDN-enabled IIoT/cyber–physical system networks. The paper focuses on secure communication and session key establishment between users and heterogeneous CPS devices. The main concern is protecting the IIoT ecosystem from various security threats due to wireless and insecure communication channels. The authors propose a three-way authentication scheme called SUSIC, which uses biometric authentication, passwords, and identity factors for security. The approach supports mutual authenticity and anonymity as well as disabling traceability features. The system is evaluated using a real-or-random model for formal security analysis. However, the use of sensitive cryptographic primitives may increase computational overhead, and the authentication burden on the control plane might overburden the controller node.

The work in [50] explores the detection of risks and vulnerabilities in IIoT-enabled CPSs, addressing the identification and filtering of critical attack paths. The study aims to identify and eliminate high-risk communication paths critical to IIoT systems. The article uses graph theory and classical algorithms, including a directed acyclic graph structure for threat and risk representation, a depth-first search algorithm, the Floyd–Warshall algorithm for attack path identification, and attack tree-based modelling. The approach serves as a generic vulnerability and risk assessment method that can improve latency compared

to conventional approaches. CVSS scores and the National Vulnerability Database are employed for vulnerability assessment. However, path reduction is limited to hop length consideration, and manual computation is needed for results. Performance is evaluated through running time analysis, path detection, and filtering efficiency, with validation using a healthcare scenario. The approach shows improved performance for certain node numbers compared to other approaches.

The scheme proposed in [33] addresses the detection of abnormal traffic in Modbus/TCP transactions in IIoT environments to protect against disruption and cyber-attacks. The paper primarily focuses on detecting anomalies caused by packet manipulation, including fabrication and modification of Modbus commands. Different types of DoS attacks are addressed, along with other cyber threats. A rule-based detection mechanism employing three detection tables for analysing Modbus/TCP transactions is used. The system is implemented as an industrial cyber prevention gate, operating as an industrial firewall. The approach analyses small volumes of traffic for prompt response and can detect various attack types through coordinated detection blocks, operating as a standalone network security system integrated into the firewall. However, the system still needs further validation in actual control system environments.

The authors of [51] focus on security challenges in Industry 4.0 environments, highlighting concerns arising from the combination of information technology and operational technology infrastructures in IIoT systems. The primary issue is ensuring end-to-end security while dealing with lightweight encryption requirements for IIoT networks. The paper implements the defence-in-depth approach, creating multiple security layers to protect against various attack vectors. Redundancy mechanisms are proposed to minimise DDoS attacks. Both passive (access control, traffic analysis, intrusion detection) and active (traffic filtering, vulnerability scanning, hardening) security mechanisms are integrated, along with network segmentation. However, the middleboxes in this approach require full access to relayed data, and messages require continuous decryption and re-encryption at gateways, creating security vulnerabilities. The paper provides a framework without quantitative data.

The paper [52] addresses false data injection attacks in IIoT environments, focusing on data dissemination in dense IIoT systems. Both external attackers who capture nodes for propagating false data and internal attackers who circumvent access control are addressed. DDoS attacks are listed among the attacks analysed. The paper proposes CONFIT (CONsensus-Based Data FIlteriNg for IIoT), which uses a consensus-based clustering mechanism for efficiency while ensuring the authenticity and availability of collected data. The approach can only be tested with full knowledge of the architecture. NS3-simulator is used for evaluation, comparing CONFIT against Dynamic Data-Aware Firefly-Based Clustering. In the test scenario, devices acted as attackers, but full system information was provided for testing.

The authors of [31] discuss the problem of large-scale DDoS attacks in IoT environments that emerge from multiple low-rate DDoS attacks originating from geographically distributed IoT devices. This attack is difficult to detect due to the IoT environment's distributed nature. The authors propose a fog computing-based approach utilising fog nodes closer to edge IoT devices. The paper states that experimental results show faster detection rates of low-rate DDoS attacks at fog nodes. However, except for Pearson correlation and false positive rate, detailed outcomes and specific metrics are not provided.

Yang et al., in [53], explore security vulnerabilities in SCADA energy management systems and DDoS attack mitigation in IIoT environments. The authors propose token-based authentication, including a token-based authentication service for generating tokens for legitimate devices; a trusted encrypted validator module for encryption, decoding,

and device verification; and a transport-layer security 1.3 protocol for secure connections. The approach uses two-way identity authentication with tokens, protects sensitive materials through private tokens, and defends against multiple attack types, including man-in-the-middle, replay, and impersonation attacks. However, the approach requires higher processing overhead (e.g., the system takes 186 ms, 1.7 times longer than without encryption verification). The approach measures CPU resource usage and access time.

The authors of [54] discuss challenges of data security in edge-intelligent IIoT, addressing major security issues including reliable storage, convenient data usage, efficient search, and secure deletion. The authors implement a three-layer architecture incorporating cloud, fog, and device layers, using fog computing as edge intelligence. The framework processes data at fog nodes before uploading data to the cloud periodically. DoS attacks are discussed as one of the vulnerabilities. The approach provides low latency, location awareness, and decentralised computation capability, enabling transient storage at fog nodes. However, fog nodes are not fully trusted.

Zhou et al., in [55], discuss challenges of DDoS attacks in large-scale IIoT systems. The authors implement a fog-based security framework introducing a regional aggregator concept for DDoS attack mitigation. The framework consists of four layers, with fog computing as the central security mechanism. The conceptual framework reduces latency to sub-milliseconds by eliminating cloud-sensor back-and-forth delays and enables faster device authorisation and data processing due to fog nodes. However, the framework faces challenges in authentication, trust, location awareness, and energy consumption.

The proposed framework in [56] explores challenges of real-time response requirements and limited device computation capabilities in IIoT systems. The authors implement a fog computing-based approach using a three-level architecture: field level, local level, and cloud level. DDoS attacks in bio-environments are discussed, focusing on components including sensors, controllers, and actuators. The approach provides fast detection through cloud coordination but takes longer to identify attack patterns at the local fog level. The approach is evaluated based on detection time and detection rate against TCP SYN and Modbus flood DDoS attacks.

The work in [57] addresses DDoS attack mitigation in IIoT environments using a hybrid combination of minimax game formulation, zero-sum game modelling, and SDN-based architecture. DDoS attacks are addressed in the context of delay attacks targeting latency in DetNet systems. The approach provides dynamic resource allocation through SDN and real-time attack patterns. However, it is limited to latency-based attack scenarios. Performance is measured through model execution time with different PLC counts, achieving a 54% reduction in attack impact compared to traditional strategies.

Mounika et al., in [58], propose a real-time DDoS detection and mitigation framework for SDN environments by integrating Mininet, the POX controller, and the Snort Intrusion Detection System. The framework seamlessly combines signature-based and anomaly-based detection with dynamic mitigation: Snort monitors traffic and pushes real-time alerts to the POX controller, which automatically modifies OpenFlow switch flow tables to isolate malicious traffic in a honeypot while preserving services for legitimate users. The experimental results demonstrate that the system triggers alerts within 1–2 s and restores the victim host to a safe state with 100% redirection accuracy against SYN flood, ICMP, and UDP attack scenarios. However, achieving accurate real-time synchronisation between Snort and POX required extensive iterative tuning to reduce false positives and negatives. Furthermore, while the system is modular and cost-effective, its current implementation remains a prototype evaluated on a small-scale virtualised topology of three hosts, leaving performance and scalability in large-scale, high-throughput industrial IIoT environments as an open question.

Finally, Srivastava and Sinha, in [59], propose a statistical method for detecting unknown variants of high-volume DoS/DDoS attacks by leveraging data mining techniques. The framework employs the Frequent-Pattern Growth (FP-Growth) algorithm to extract unique attack signatures from real-time traffic, offering higher memory efficiency and faster processing than traditional Apriori-based methods. Jaccard similarity scoring then compares incoming data packets against a high-volume attack knowledge base, achieving accuracies of 91.66% and 94.87% on the RTNITP24 and CICIDS2017 datasets, respectively. This approach is particularly relevant to IIoT environments, where high-volume floods targeting PLCs and SCADA systems represent a critical availability threat. However, the model cannot detect entirely unknown zero-day patterns that share no characteristics with known high-volume attacks, as it assumes a degree of correlation between established signatures and their variants. Furthermore, the approach is strictly restricted to high-volume attacks, rendering it ineffective against low-rate DDoS threats that evade detection by mimicking legitimate IIoT traffic patterns. Future research is required to reduce the time complexity of the signature extraction process and expand the detection scope to broader attack domains. Table 7 summarises conventional techniques, highlighting their approaches, achievements, limitations, and datasets used for evaluation.

Table 7. Conventional approaches for detecting DDoS attacks in the IIoT.

Ref	Year	Approach	Product/System	Achievement	Limitations	Dataset/Testbed
[35]	2020	Game theory-based PHS	SDN-enabled defence system for IIoT	Lower energy consumption, effective DDoS defence	Reduced detection rate due to AHA	12 servers, 10 honeypots (4 regular, 6 pseudo)
[36]	2018	Multi-level SDN-based framework with edge/fog/cloud computing	DDoS mitigation framework for IIoT security	Fast response time, multi-level protection	Challenges with large data processing	Mininet VM with OpenFlow switches
[9]	2021	D-ConCReCT: Distributed congestion control by duty-cycle restriction	DoS attack detection and mitigation system for IIoT	Effective in 500-node networks; faster detection than centralised approach	Variable DDoS mitigation effectiveness; needs traffic segmentation optimisation	Simulated data
[16]	2023	Cryptographic three-factor authentication scheme	User access control mechanism for SDN-enabled IIoT/CPS	Supports mutual authenticity and anonymity	Additional authentication burden on controller nodes	Smart devices and controller nodes
[50]	2023	Graph-based (DAG, DFS, Floyd–Warshall)	Graph-based vulnerability and risk assessment framework	Fast attack path detection and improved running time	Manual computation needed; limited to hop length	Transportation sector case study with CVEs
[33]	2024	Rule-based detection	Industrial cyber prevention gate	Detection with small traffic volume	Needs further stability testing in real-world scenarios	IndusCAP-Gate (Industrial Cyber Attack Prevention-Gate)
[51]	2020	Defence-in-depth with redundancy	End-to-end security framework for Industry 4.0	Multi-layer security, network segmentation	Middleboxes require full data access; continuous decryption/re-encryption	No quantitative data
[52]	2022	CONFIT consensus-based clustering	Data dissemination control system for dense IIoT	Rapid identification and isolation of malicious networks	Requires full network knowledge for testing	Gas pressure sensor data from UCI ML repository
[31]	2023	Fog computing-based DDoS detection	Large-scale DDoS detection system for IoT	Early detection and fast response	Experimental demonstration only	Not mentioned
[57]	2024	Minimax game-theoretic with SDN	DDoS mitigation for IIoT DetNet networks	Dynamic resource allocation; 54% reduction in attack impact	Limited to latency attacks	Synthetic data using stochastic probability distribution
[53]	2022	Token-based authentication with TLS encryption	SCADA energy management system security	Prevents DDoS, MitM, and replay attacks	Processing time 1.7× longer than without encryption	Synthetic data from Smart Green Energy Science City, Taiwan
[54]	2019	Cloud-fog-mist-device framework with three-layer security	Edge intelligent IIoT data security system	Decentralised computation; location awareness	Heavy reliance on fog nodes	IIoT device data for fog node storage
[56]	2019	Three-level fog architecture for IIoT security	DDoS mitigation system for IIoT environments	Fast detection through cloud server coordination	Longer detection at local fog level	Metro railway control system testbed

Table 7. *Cont.*

Ref	Year	Approach	Product/System	Achievement	Limitations	Dataset/Testbed
[58]	2025	SDN-based framework using Mininet, POX, and Snort IDS	Real-time DDoS detection and honeypot-based mitigation	100% redirection accuracy; low latency (1–2 s); automatic flow rule updates	Complex real-time synchronisation; prototype tested on small-scale virtual topology only	Mininet simulation with SYN flood, ICMP, and UDP attacks
[59]	2025	FP-Growth signature extraction and Jaccard similarity	Detection of unknown DoS/DDoS variants in IIoT	Efficient signature extraction; up to 94.87% accuracy on real-time data	Assumes correlation with known patterns; limited to high-volume attacks; ineffective for low-rate DDoS	RTNITP24 and CICIDS2017

Across the conventional approaches reviewed, a clear pattern emerges: while techniques such as SDN-based mitigation, fog computing architectures, and game-theoretic models offer fast response times and low computational overhead, they share a fundamental weakness: their reliance on predefined rules, static thresholds, and manually configured policies renders them ill-equipped to handle the dynamic, evolving nature of modern DDoS attacks in IIoT environments. The best-performing conventional approaches, such as the multi-level SDN framework of [36] and the fog-based architecture of [56], demonstrate that layered, distributed designs outperform single-point solutions. However, none of the reviewed conventional works address zero-day attacks, and the majority are validated only in simulated or synthetic environments. The critical verdict is that conventional techniques remain useful as a first line of defence for known, well-characterised attack patterns, but they cannot stand alone in modern IIoT deployments where attack sophistication consistently outpaces rule updates.

Despite the progress achieved by conventional techniques, their centralised architectures and rule-based logic proved vulnerable to dynamic and distributed attack vectors. This motivated the adoption of blockchain-based approaches, which offer decentralised trust management and tamper-resistant audit trails, as discussed in the following subsection.

4.2. BC-Based Approaches for DDoS Attack Detection

BC-based approaches for DDoS attack detection have gained significant attention due to their decentralised, transparent, and tamper-resistant characteristics. These approaches leverage mathematical modelling to describe attacker and defender behaviour, optimise detection mechanisms, and analyse framework performance. Generally, attacker–defender interaction can be formulated using game theory, where the attacker's utility U_a is the difference between potential gain G_a and cost C_a:

$$U_a = G_a - C_a \tag{1}$$

Similarly, the defender (BC node or network operator) maximises utility U_d considering reward from successful detection R_d and operational cost C_d:

$$U_d = R_d - C_d \tag{2}$$

Total detection time includes anomaly detection time T_{detect}, block generation time T_{block}, and propagation delay $T_{propagate}$:

$$T_{total} = T_{detect} + T_{block} + T_{propagate} \tag{3}$$

Reputation scores $S_i(t)$ of node i at time t are updated based on historical behaviour and recent malicious activity $A_i(t)$:

$$S_i(t+1) = \alpha S_i(t) + \beta A_i(t) \tag{4}$$

Finally, BC-enabled systems can use ML classifiers to identify anomalous traffic patterns stored in the immutable ledger. The probability of traffic instance X being classified as an attack y can be estimated via Bayesian inference:

$$P(y|X) = \frac{P(X|y)P(y)}{P(X)} \tag{5}$$

Due to limitationsin conventional DDoS detection solutions and IDSs in general, BC technology has become an alternative solution to ensure availability, security, and reliability. However, BC-based solutions face resource constraints and scalability issues in IIoT environments. The authors of [37] highlight security, privacy, control, compliance, computability, and reliability challenges in cloud computing with smart IIoT environments. The work primarily focuses on tackling security risks and difficulties associated with exchanging confidential information in cloud infrastructure for IIoT environments. The authors implement an approach named DistB-SDCloud, combining BC technology into an SDN-enabled IIoT system within a cloud environment. SDN is said to be vulnerable to DDoS attacks, hence the integration with BC. The distributed structure improves the reliability and speed of physical and logical data. However, the architecture needs effective implementation in diverse scenarios. The approach is evaluated based on latency, CPU utilisation, and bandwidth usage.

Rathee et al., in [38], focus on protecting data transmission, reducing production costs, and ensuring transparent communication between industrial services. The authors implement a hybrid BC-based framework for the IIoT. BC technology tracks industrial activities and worker locations, controls automated data collection and analysis, and ensures protection and secrecy of control systems. The approach is evaluated based on authentication delay, message resistance, and DoS/DDoS attack resilience. It ensures transparency between entities and validates through BC creation and miner validation. However, this approach faces cost overhead due to system complexity and storage issues.

In [39], the proposed method addresses efficiency and security concerns in cross-domain IIoT authentication. The authors focus on heavy computational overhead and vulnerability to DDoS attacks in BC-based authentication systems. Off-chain and on-chain mechanisms are implemented using BC technology. The protocol uses a single-domain server for authenticating both local and foreign domain devices. The key generation phase uses only four messages, reducing communication overhead. The approach achieves fast operation and a high transaction rate in a permissioned structure. However, the system still requires BC infrastructure and domain server involvement. The approach is evaluated based on computation-related criteria, communication-related criteria, and BC storage cost measurement.

The authors of [60] address data privacy and security risks like eavesdropping and hijacking attacks in communication channels. A BC-based certificateless signature is implemented using the Schnorr mechanism. DDoS is one of the security vulnerabilities addressed. The approach provides protection against device capture attacks through the elliptic curve discrete logarithm problem assumption and implements secure signature verification using timestamps to prevent replay attacks. The approach is evaluated based on communication costs, signature overall costs, and security feature comparison with other protocols. However, optimisation to make it lightweight is still needed.

The work in [61] discusses securing communication, server security, data sharing, and access control mechanisms in IIoT systems by implementing a permissioned BC. This allows only selected and authorised participants to join the network and implements identity management capabilities. Additionally, this approach controls transaction execution based on participant identity. The authors address DDoS as one of the critical security vulnerabilities in IIoT environments. However, the paper primarily presents a conceptual and theoretical framework.

Rajesh et al. [62] introduce a collaborative DDoS defence system that leverages the Ethereum blockchain to share threat intelligence and incentivise organisational participation. The framework combines rate limiting and time-window traffic analysis for detection, while employing an incentive mechanism based on NFTs and cryptocurrencies to encourage businesses to actively report and store malicious IP addresses on an immutable ledger. This collaborative approach achieves a significant mitigation improvement, blocking up to 5,000 malicious IPs within 100 ms in a cloud-based environment, directly addressing the collective action problem that limits the effectiveness of isolated DDoS defence systems. However, the framework faces notable limitations. The initial data insertion process introduces potential latency, particularly when using Redis as a backup system for the blockchain, which can reduce real-world writing speed. Furthermore, the system's effectiveness relies heavily on the quality and volume of shared intelligence from partner organisations, and the study identifies further research needs in cross-chain interoperability and scalability in larger, more complex vertical IIoT deployments.

Moudoud et al. [63] propose SecureShare, a novel cross-domain DDoS mitigation framework integrating digital twins, SDN, NFV, and blockchain for smart consumer networks. The framework's key contribution is a decentralised resource-sharing scheme that uses fuzzy quantified propositions and linguistic quantifiers to rank resource providers fairly based on satisfaction and preferences, addressing the challenge of equitable burden-sharing across autonomous systems during large-scale DDoS events. A reputation scheme and blockchain-based mutual authentication with access tokens foster trust and ensure secure, tamper-proof collaboration between different network domains. Extensive testing on Ethereum's Sepolia network and Microsoft Azure Digital Twins demonstrates the framework's efficiency in handling large-scale attacks while maintaining low execution delay. However, scalability remains a critical concern as the number of on-chain operations increases, which the authors identify as a priority for future optimisation using hybrid on-chain and off-chain solutions. Additionally, the system's overall performance depends heavily on the accuracy of the digital twin virtual replicas and the timely synchronisation of model updates across multiple potentially untrustworthy SDN domains. Table 8 summarises BC-based techniques.

Table 8. BC-based approaches for detecting DDoS attacks in the IIoT.

Ref	Year	Approach	Product/System	Achievement	Limitations	Dataset/Testbed
[37]	2023	BC-based SDN with cloud	DistB-SDCloud architecture for IIoT security	Low latency	Needs validation in diverse implementation scenarios	Testbed with MiniNet and OpenFlow
[38]	2021	BC-based framework for IIoT security	IIoT security management and tracking system	DDoS attack resistance, automated data validation	Computational complexity, costly	Testbed (500 m × 500 m IIoT environments)
[39]	2023	Hybrid off-chain and on-chain BC authentication	Authentication protocol for multi-domain IIoT systems	Reduced overhead	Requires BC implementation and domain server	OpenSSL cryptographic implementation tests

Table 8. *Cont.*

Ref	Year	Approach	Product/System	Achievement	Limitations	Dataset/Testbed
[60]	2022	BC-based certificateless signature using Schnorr mechanism	Security protocol for IIoT devices	Protection against device capture and replay attacks	Lightweight optimisation still needed	MIRACLE library
[61]	2020	Permissioned BC	IIoT security framework	Enhanced DDoS detection	DDoS attack success rate not quantified	Practical Byzantine Fault Tolerance (PBFT) consensus algorithm
[62]	2025	Blockchain-powered collaborative defence with NFT/crypto incentives	Decentralised threat intelligence sharing for DDoS	Incentivised collaboration; immutable IP storage; blocks 5000 IPs within 100 ms	Latency in blockchain data insertion; dependence on partner sharing quality; lacks cross-chain interoperability	Ethereum blockchain and API-based collaboration testbed
[63]	2025	SecureShare: Digital twin, SDN, NFV, and blockchain hybrid	Cross-domain DDoS mitigation for smart consumer networks	Fair resource-sharing via fuzzy logic; reputation-based decentralised trust; tested on Sepolia and Azure Digital Twins	Scalability with frequent on-chain operations; synchronisation dependency on digital twin accuracy	Sepolia (Ethereum) testnet and Microsoft Azure Digital Twins

The five BC-based approaches reviewed reveal a consistent tension between security assurance and practical deployability in the IIoT. While BC offers genuine advantages in decentralised trust management and tamper-resistant audit trails, none of the reviewed works fully resolves the fundamental incompatibility between BC's computational demands and the resource constraints of IIoT edge devices. The most practically grounded work, [39], addresses this through off-chain and on-chain hybrid mechanisms that reduce communication overhead, representing the most promising direction. In contrast, [61] remains entirely conceptual, offering no empirical validation. Critically, BC-based approaches treat DDoS as one vulnerability among many, rather than as the primary threat, meaning that none of the reviewed BC works provides dedicated DDoS detection performance metrics. This represents a significant gap: BC's value for IIoT security lies in trust and authentication rather than in real-time traffic-based DDoS detection, and future work should be explicit about this distinction rather than presenting BC as a general-purpose DDoS solution.

While blockchain-based solutions strengthened trust and transparency in IIoT networks, their high computational overhead and latency introduced new barriers in resource-constrained environments. This gap prompted the adoption of ML techniques, which offered data-driven adaptability without the infrastructure demands of blockchain, as examined next.

4.3. ML-Based Approaches for DDoS Attack Detection

ML-based approaches for DDoS attack detection have become a dominant research direction due to their ability to model complex and non-linear patterns in network traffic. These models rely on extracting discriminative features from traffic data and constructing classifiers that differentiate between normal and malicious behaviours. Formally, let $X = \{x_1, x_2, \ldots, x_n\}$ represent a set of network traffic instances, where each x_i is a feature vector consisting of traffic attributes such as packet rate, flow duration, or byte size.

A supervised ML classifier learns a mapping function $f : X \to Y$, where $Y = \{0, 1\}$ denotes class labels (0 for normal, 1 for DDoS attack). The classifier is trained on a labelled dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$ to minimise a loss function L, commonly cross-entropy loss:

$$L = -\sum_{i=1}^{N} [y_i \log f(x_i) + (1 - y_i) \log(1 - f(x_i))] \quad (6)$$

Feature selection or extraction is key to improving accuracy and reducing complexity. Statistical measures such as mean μ, standard deviation σ, entropy $H(X)$, or correlation coefficients ρ are often computed:

$$H(X) = -\sum_{x \in X} P(x) \log P(x) \tag{7}$$

Once trained, the classifier outputs a prediction $\hat{y}$ for an unseen instance x: $\hat{y} = \arg\max_{y \in Y} P(y|x)$. Anomaly-based models (e.g., clustering or autoencoders) estimate deviation from normal patterns using distance or reconstruction error, e.g., Euclidean distance $d(x, \mu)$ to a centroid μ:

$$d(x, \mu) = \sqrt{\sum_{j=1}^{m} (x_j - \mu_j)^2} \tag{8}$$

An instance is flagged as anomalous if $d(x, \mu) > \delta$.

To address limitations in both conventional and BC-based approaches, ML techniques have emerged as promising solutions. Various ML algorithms have been implemented to identify, classify, and mitigate DDoS attacks in IIoT environments.

The work in [3] discusses the detection of IoT-based DDoS attacks, focusing on stealthy low-rate attacks and early detection. The authors implement a hybrid approach using a lightweight unsupervised classifier (HBOS-based) deployed at IoT edge gateways and reinforcement learning (SAC-based) with collaboration mechanisms. Both flood-based volumetric attacks and stealthy low-rate DDoS attacks are addressed. The approach provides early detection and resource utilisation. The model is tested on a real-world testbed using evaluation metrics including FPR, area under the curve, and confusion metrics, achieving 99.2% accuracy in the first cycle. The N-BaIoT dataset and a custom testbed are used.

The authors of [40] discuss DDoS attack detection in IIoT environments using random forest and naive Bayes. DDoS is addressed as an attack type that slows data transmission and causes network flooding. The Edge-IIoTset dataset is used for evaluation. Random forest outperforms naive Bayes across all test scenarios, achieving 100% and 78.56% accuracy, respectively. However, the high performance is influenced by the relatively small dataset size.

The work proposed in [64] highlights IoT/IIoT network security by implementing an ensemble learning-based IDS using random forest for classification, Pearson correlation coefficients for feature selection, and isolation forest for outlier detection. The model handles IIoT security concerns, including DDoS attacks, effectively manages imbalanced datasets, and provides effective feature selection. Evaluation using confusion metrics shows accuracy as high as 99.98%. Nonetheless, broader validation with real-world testbeds is needed.

The authors of [65] address cyber-attack detection in IIoT environments, highlighting minimum detection and high error rates. They propose an RL-based approach named SPC-DRRL with three key components: log-likelihood sliding principal component for feature extraction, dynamic reward reinforcement learning for classification, and an incident repository for continuous learning. DDoS attack types are explored along with other attacks. Evaluation metrics include detection time, accuracy, overhead, and error rate. The approach reduces computational usage by about 17–41% compared to similar approaches, and the incident repository enables continuous learning. However, implementation and maintenance are costly, and communication between systems is complex due to technology and protocol exclusivity.

In [66], the need for a comprehensive security testbed is addressed to generate diverse intrusion datasets. ML techniques including SVM, random forest, and decision tree are used.

Seventeen types of DDoS attacks (TCP SYN flood, UDP flood, MitM ransomware, wildcard abuse) are included. The testbed incorporates various sensors in the IIoT perception layer, along with realistic network topologies and communication protocols. High accuracy is recorded for all three algorithms, but emerging threats considering the heterogeneity of IIoT environments need to be addressed.

Similarly, in [41], the focus is on detecting DDoS attacks in Edge-IIoT networks using two ensemble learning techniques: XGBoost and hard voting ensemble (combining SVM, decision tree, and naive Bayes). Four types of DDoS attacks (TCP SYN flood, UDP flood, HTTP flood, ICMP flood) are discussed. The Edge-IIoT dataset (63 features) is used. XGBoost achieves 99.88% accuracy, outperforming hard voting by 11%, but zero-day attacks are not addressed.

The authors of [42] address cyber threat detection in IIoT systems, including DoS, data probing, malicious operation, spying, malicious control, scan, and wrong setup. DDoS is also analysed. The authors implement a lightweight Random Neural Network-based approach for attack prediction, designed for resource-constrained IIoT environments. It can be deployed on a single-board computer and integrated with different network topologies. The approach provides a fast prediction time of 120 ms on Raspberry Pi, low power consumption (2.54 W normally, 2.84 W during processing), and 99.20% accuracy. However, complexity reduction, scalability, and further optimisation for edge implementations are needed.

The authors of [67] address security challenges in edge devices in IIoT systems, focusing on protecting them from internal and external attacks. Decision tree, random forest, and gradient-boosting algorithms are implemented, with decision tree selected as the final algorithm. The paper explores the three main layers of IIoT network topology: edge, fog, and cloud. IIoT edge devices are critical for networking but face security vulnerabilities. DoS and DDoS attacks are mentioned among other threats. The approach achieves 99.69% accuracy, but trained ML models cannot be directly implemented on low-performance edge devices.

The work in [68] discusses the security gap in the Industrial Internet of Service, analysing how DDoS vulnerabilities could affect the IIoS. Six ML algorithms (naive Bayes, SMO, J48, Decision Table, AdaBoost, Simple Logistic) are analysed using the CIC-IDS2017 dataset. Decision Table and J48 achieve 98.9% accuracy with computational efficiency of 4.53 s. However, the analysis is limited to offline evaluation.

The authors of [69] discuss security concerns in SCADA network systems connected to public networks, underlining DDoS attacks in energy management systems. Multiple ML algorithms (OneR, naive Bayes, SVM, KNN, random forest, AdaBoost) are utilised, with a token authentication module as a defence approach. The proposed model can distinguish between natural, malevolent, and non-malicious disruptions and is tested on three-class and binary datasets. However, it cannot handle complex applications without causing delays.

The authors of [70] present a cloud-based security framework using federated learning-based ANN with information fusion for detecting DDoS attacks (RP poisoning, SSL-based attacks, DNS flood). The framework operates in a three-layer architecture (device, edge, cloud) and implements a cloud-based global security auditor for vulnerability investigation. Evaluation using classification metrics and CPU utilisation shows high accuracy, but the evaluation is limited to specific hardware configurations (Windows 10, 4.0 GHz i7, 64 GB RAM), and baseline security protocols at local levels are assumed.

Estupiñán Cuesta et al., in [71], evaluate the efficacy of XGBoost and random forest models for detecting application-layer DDoS attacks, specifically HTTP floods, in SDN environments. A key strength of this study is the detailed comparison of two flow-generation

tools, CICFlowMeter and NTLFlowLyzer, used to build customised datasets of 424,922 and 731,589 flows, respectively. While XGBoost proved more resource-efficient, with faster training times, random forest demonstrated superior reliability, with a near-zero false negative rate using the NTL-Dataset, achieving 99.99% accuracy. However, the study is limited to HTTP flood attacks (GoldenEye, Slowloris, HULK) in a strictly controlled environment, without addressing volumetric UDP/ICMP floods, OpenFlow-specific attacks, adversarial robustness, or zero-day scenarios. The absence of benchmarking against widely used public datasets such as CICDDoS2019 further limits the comparability of findings across broader research contexts.

Mallela et al., in [72], address the rising threat of DDoS attacks in IoT systems by proposing an optimised detection framework combining hybrid feature selection with ensemble learning. The framework integrates chi-squared and Recursive Feature Elimination (RFE) to identify the most impactful features from the CICIoT2023 dataset, reducing the feature set to just 10 key attributes while achieving a peak detection accuracy of 99.95% using XGBoost across 12 DDoS attack classes. This significant dimensionality reduction directly addresses the computational constraints of resource-limited IIoT deployments. However, the experimental results show no further performance gains beyond ten features, suggesting that the model may have reached its optimisation ceiling for the specific attack classes in the dataset. Furthermore, the framework has yet to be validated in dynamic SDN-based IoT environments, which remains an important direction for future work.

Finally, Hirsi et al., in [73], introduce HSF, a hybrid machine learning framework for dual-plane DDoS detection and mitigation in software-defined networks. The framework synergistically integrates random forest for feature importance ranking and dimensionality reduction with support vector machines for high-precision classification, monitoring both the control plane (protocol, packet rate) and the data plane (byte count, delay). HSF achieves 99.2% accuracy, an exceptionally low false positive rate of 0.019%, and minimal latency of 7–12 ms per packet, making it well suited for real-time industrial applications. However, its scalability in ultra-large SDN deployments remains an open challenge, as increased traffic volumes could elevate computational burden. Additionally, the framework does not explicitly address adversarial threats such as model poisoning attacks, which the authors identify as a critical direction for future research.

Table 9 summarises ML-based techniques.

Table 9. ML-based approaches for detecting DDoS attacks in IIoT.

Ref	Year	Approach	Product/System	Achievement	Limitations	Testbed/Dataset
[3]	2023	ML combining supervised learning and RL	DDoS attack detection for IoT	Early detection of stealthy DDoS; resource utilisation	Limited testbed scale and device types	N-BaIoT
[40]	2024	Random forest and naive Bayes	DDoS detection for IIoT	Random forest achieved 100% accuracy across tests	Small dataset size limiting tree generation	Edge-IIoTset
[64]	2023	Random forest, PCC, isolation forest ensemble	IDS	Handles imbalanced data	Limited dataset validation	Bot-IoT, NF-UNSW-NB15-v2
[65]	2023	RL with sliding principal component	Attack detection (incl. DDoS) for IIoT	Reduced memory usage	High maintenance cost, scalability limitations, complex protocols	TON_IoT
[74]	2022	ML-based threat detection (DT, RF, GB)	Lightweight IDS for IIoT edge	High accuracy, multiple security implementations	Cannot be directly implemented on edge nodes	MQTTset

Table 9. *Cont.*

Ref	Year	Approach	Product/System	Achievement	Limitations	Testbed/Dataset
[66]	2023	ML-based security testbed (SVM, DT, RF)	Security testbed generating ForgeIIOT dataset	High accuracy	Needs to address emerging IIoT threats	ForgeIIOT
[41]	2023	XGBoost and hard voting ensemble (SVM, DT, NB)	DDoS detection for Edge-IIoT	High detection across various attacks using XGBoost	Zero-day attacks not addressed	Edge-IIoT
[42]	2020	Lightweight Random Neural Network	IIoT cyber-attack detection	Lightweight for resource-constrained IIoT	Complexity and scalability issues	DS2OS
[67]	2023	ML (DT, RF, GB)	Lightweight IDS for IIoT edge	High accuracy	Cannot be directly implemented on edge nodes	MQTTset
[68]	2023	Six ML algorithms	DDoS detection using Weka	Faster computation	Offline analysis only	CIC-IDS2017
[70]	2024	Federated learning-based ANN with information fusion	Cloud-based security framework for IIoT	Cloud-based global security auditor	Evaluation limited to specific hardware configuration	ToN-IoT and CICDDOS
[69]	2023	Six ML algorithms (OneR, NB, SVM, KNN, RF, AdaBoost)	SCADA energy management security with token verification	Distinguishes natural, malevolent, and non-malicious disruptions	High memory needs, system delays	Testbed (1221 natural, 3711 attack, 294 no-event samples)
[71]	2025	XGBoost and random forest with customised SDN datasets	Application-layer DDoS detection in SDN	99.99% accuracy; compares CICFlowMeter vs. NTLFlowLyzer tools	Limited to HTTP floods; no volumetric or zero-day tests; lacks public dataset benchmarks	Custom SDN datasets
[72]	2025	Hybrid feature selection (chi-squared + RFE) and XGBoost	Optimised DDoS detection for IoT networks	99.95% accuracy with only 10 features; high computational efficiency	Performance plateaued at 10 features; not validated in SDN-based IoT settings	CICIoT2023
[73]	2025	HSF: Hybrid SVM-RF for dual-plane monitoring	Real-time dual-plane DDoS detection in SDN	99.2% accuracy; very low FPR (0.019%); low latency (7–12 ms)	Scalability in massive SDN deployments needs optimisation; vulnerable to adversarial poisoning	Custom SDN-DDoS dataset and NSL-KDD

The ML-based approaches reviewed demonstrate that ensemble and tree-based methods, particularly random forest and XGBoost, consistently deliver the strongest combination of accuracy and computational efficiency for IIoT DDoS detection. Random forest achieved 100% accuracy in [40] and 99.98% in [64], while XGBoost outperformed a hard-voting ensemble by 11% in [41], confirming that boosting and bagging strategies are the leading ML paradigms for this problem. Lightweight approaches such as the Random Neural Network of [42], deployable on a Raspberry Pi with 120 ms inference time, represent the most practically viable direction for resource-constrained IIoT edge nodes. However, two critical weaknesses pervade this category: first, the near-universal reliance on public benchmark datasets such as Edge-IIoTset and CIC-IDS2017 raises serious generalisation concerns, as strong performance on a single controlled dataset does not guarantee robustness in heterogeneous real-world IIoT deployments; second, zero-day attack detection remains largely unaddressed, with only reinforcement learning-based approaches such as [65] offering any degree of adaptation to unseen threats. The field would benefit from a deliberate shift toward lightweight, online-learning ML models evaluated on multi-site, protocol-diverse IIoT testbeds.

Although ML approaches demonstrated promising detection accuracy, their reliance on manual feature engineering and limited capacity to model complex temporal and spatial

patterns in network traffic created an opening for deep learning solutions, which are explored in the following subsection.

4.4. DL-Based Approaches for DDoS Attack Detection

The rapid growth of the IIoT necessitates robust security mechanisms [75]. DL-based solutions have emerged as advanced and robust techniques that leverage neural networks to effectively identify, classify, and mitigate DDoS attacks.

DL-based approaches automatically extract hierarchical and non-linear features from raw network traffic data without manual feature engineering. Let $X = \{x_1, x_2, \ldots, x_n\}$ denote traffic samples, each a raw input vector. A deep neural network models a mapping $f(X;\theta)$ parameterised by weights θ, learned by minimising a loss function L over a labelled dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$. For classification, cross-entropy loss is commonly used:

$$L = -\sum_{i=1}^{N}\sum_{k=1}^{K} y_{ik} \log f_k(x_i;\theta) \tag{9}$$

where K is the number of output classes, y_{ik} is the ground truth, and $f_k(x_i;\theta)$ is the predicted probability for class k. Models are trained using backpropagation with gradient descent:

$$\theta^{(t+1)} = \theta^{(t)} - \eta \nabla_\theta L \tag{10}$$

where η is the learning rate.

For example, the authors of [43] emphasise that IoT environments are more vulnerable to DDoS attacks due to computational and storage limitations. LSTM and CNN techniques are implemented to protect benign traffic while providing immediate detection during DDoS attacks. The system is evaluated on a mixed dataset, achieving 98.9% detection accuracy and 99.9% classification accuracy. However, it depends on an edge server and requires continuous updates of filtration rules for both the flow filter and flow handler.

The authors of [17] address DDoS attacks targeting SDN controllers in IIoT networks, focusing on SYN, DNS, and UDP floods while maintaining data privacy. They implement a low-complexity CNN-MLP model with residual connections, a federated learning framework for decentralised training, and Pearson correlation coefficient feature selection. The approach achieves 98.37% accuracy but focuses only on three attack types, and testing used only one industrial agent while five were used for training, insufficient validation.

The work in [76] discusses privacy concerns in DDoS attack classification for SDN-enabled IIoT networks, where sharing sensitive industrial traffic with third parties poses risks. The authors use federated learning with a CNN-MLP model, residual connectivity, PCC filter-based feature selection, and federated averaging for parameter aggregation. The approach preserves privacy through local training and efficient feature selection, achieving 98.37% accuracy. However, transferring weighted parameters between edge servers and aggregation servers could create network overhead.

In [10], data integrity and reliability in the IIoT are addressed. The paper highlights extreme class imbalance, redundant features, and insufficient detection accuracy of traditional methods. A DL approach integrates hierarchical clustering for under-sampling, an optimal feature selection algorithm based on greedy search, and a DNN with parallel global and local sub-networks. DDoS attacks are among those tested. The approach reduces information loss in majority samples and eliminates redundant features, evaluated via F1-score and standard deviations, but not in real-world scenarios.

The work in [22] highlights limitations of conventional IDSs for modern threat detection in the IIoT. The authors use a deep reinforcement learning approach employing the PPO2 algorithm with LightGBM feature selection, ReLU activation, and a multi-layer per-

ceptron. DDoS is one of the threats targeted. The scheme enables fast model convergence, automatic information mining, and self-updating capability, achieving a 99% detection rate. However, a distributed architecture is needed to keep up with high-speed, large-capacity, multi-dimensional data processing.

The authors of [4] highlight security issues in green IIoT environments, focusing on IDSs in resource-constrained settings. They implement a DRL approach using the deep deterministic policy gradient algorithm, with traffic flow prediction via statistical feature extraction and intrusion detection using critical thresholds. Reflection-based DDoS attacks are discussed. The model is lightweight and suitable for resource-constrained environments but struggles with network traffic that has significant fluctuations.

The scheme in [12] tackles unwanted intrusion detection in wireless networks while guaranteeing data privacy through a decentralised approach. The authors combine federated learning with CNN and RNN classifiers, training models locally at device endpoints and aggregating centrally. Various DDoS attack types (UDP, ICMP, HTTP, TCP) are examined. The approach preserves privacy by keeping data locally and reduces bandwidth usage by sharing only model parameters. Accuracies of 92.49% (federated learning) and 93.92% (centralised ML) are achieved using the Edge-IIoTset dataset, but the lack of a federated learning-specific dataset may limit real-world representation.

The authors of [44] explore scalability issues of centralised IDSs in the IIoT, including traffic overhead and latency. They propose Deep-IFS, a DL approach that employs local gated recurrent units for local representation and multi-head attention for global learning in distributed fog computing. Tested against DDoS, DoS, scanning, malware, and other threats using the TON-IoT, EDGE IoT, and X-IIoTID datasets, accuracies of 98.2% and 99.75% are recorded. However, the method requires distributed fog computing infrastructure and has restricted bandwidth at the device layer.

Alashhab et al. [30] explore low-rate DDoS attack detection using LSTM for SDN-enabled IoT. LSTM is effective for capturing sequence-based data and temporal patterns. The approach achieves 98.8% detection accuracy but may struggle with some slow-rate attacks that mimic benign traffic, and dependence on specific datasets may limit real-world representativeness.

The authors of [77] explore DDoS attacks in 5G and beyond (B5G) networks using two merged DNN algorithms with PCC feature selection. The model detects ten types of DDoS attacks and benign traffic, achieving 99.66% accuracy. However, computational effort and latency need reduction.

The authors of [78] address anomaly detection in the IIoT using a distributed RL and GAN framework to improve attack detection with imbalanced data. DoS, scanning, malicious control, malicious operation, spying, data probing, and incorrect setup are addressed. The DRL-GAN minimises false alarms using the DS2OS dataset but requires strong network infrastructure and may have increased computational complexity due to full-feature datasets.

The work in [79] highlights IIoT security vulnerabilities, focusing on detecting DDoS, MitM, and start–stop attacks in critical infrastructure and SCADA. A neural network-based expert system uses network packet mirroring for non-intrusive monitoring, achieving 99.7% accuracy, but focuses only on network attacks rather than a comprehensive approach.

The authors of [45] address vulnerability to sophisticated multivariate botnet attacks in the IIoT, using LSTM and DNN algorithms. The model is effective, scalable, and flexible, detecting zero-day attacks, but does not clearly define the dataset used and lacks consideration of IIoT heterogeneity.

Likewise, the authors of [80] discuss security challenges in the IIoT within smart cities, using DRL, RNN, and CNN. DDoS attacks are discussed in the context of botnet attacks caused by password vulnerabilities. The work serves only as a reference model.

The authors of [81] discuss detection and classification of botnet attacks in the IIoT using AttackNet, which combines CNN and GRU. The model is effective without label information in the target domain and provides advanced feature extraction, achieving 99.75% accuracy, but is costly due to large data volume and computational complexity.

The authors of [82] discuss DDoS attack classification in the IIoS using four DL algorithms (GRU, CNN, LSTM, DNN) on the CIC-DDoS2019 dataset, achieving 99% accuracy for each. However, further enhancement is needed for low-rate DDoS attack detection.

The authors of [83] highlight challenges in 6G networks posed by IT-OT convergence, implementing a DL-assisted software-defined security architecture to protect against DDoS and other threats. Various DL algorithms are analysed, but the DL approach may be complex for resource-constrained IIoT environments.

The paper [84] explores securing data transmission and detecting anomalies in the IIoT using a multi-cascaded CNN with grasshopper optimisation and dynamic honeypot encryption. The model provides privacy-preserved data transmission and secure cloud storage, evaluated via average delay and confusion metrics.

The authors of [85] discuss detection of advanced persistent threats in critical IIoT infrastructure using a BERT model for APT attack sequence detection and unsupervised learning for anomaly detection. DoS, flood, smurf, and routing protocol attacks are addressed. The method achieves 99% detection accuracy but may misjudge attack intentions due to limitations in word vector representation.

The authors of [86] highlight the need for comprehensive, realistic cybersecurity datasets for the IoT and IIoT. The Edge-IIoTset dataset includes over ten IoT devices in a seven-layer testbed with 61 high-correlation features. Traditional ML (DT, NB, SVM, KNN, logistic regression) and DL (DNN, GRU) are implemented. Common DDoS attacks (TCP SYN, UDP, HTTP, ICMP floods) are addressed. Decision tree achieves 99.54% accuracy for binary classification and 99.49% for multi-classification. The dataset is publicly available and valuable for industrial environments.

Ain et al. [87] propose a hybrid deep learning model for DDoS detection in IoT networks, integrating convolutional neural networks for spatial feature extraction, long short-term memory for temporal pattern recognition, and autoencoders for dimensionality reduction. The framework's key strength lies in its holistic multi-architectural design: autoencoders learn normal traffic structures to identify anomalies, while the CNN-LSTM layers capture complex spatial and temporal dependencies that single-model approaches cannot address simultaneously. Evaluated on the CICIOT2023 dataset, the hybrid framework achieves a validation accuracy of 96.60%, demonstrating strong performance in classifying dominant attack types including ICMP and UDP floods. However, the model struggles with rare attack classes such as HTTP floods and SlowLoris, where significantly lower F1-scores were observed due to high class imbalance in the training data. Additionally, while designed for resource-constrained IoT environments, the system exhibits sensitivity to specific traffic patterns and noise, evidenced by occasional spikes in loss values during training. Training time optimisation and more sophisticated rebalancing strategies remain critical areas for future work to ensure stable and reliable real-world deployment.

Finally, Akhi et al. [88] address the need for efficient, lightweight security solutions in resource-constrained edge devices by deploying a Temporal Convolutional Network (TCN) model on a Raspberry Pi 4. The TCN model is converted into TensorFlow Lite format and undergoes INT8 quantisation, reducing the model size significantly from

248.5 KB to 89.1 KB without compromising detection performance. This optimisation directly addresses the memory and computational constraints of IIoT edge deployments, achieving 99.95% accuracy, an ultra-low average inference latency of 0.19 ms, and stable power consumption of approximately 4.22–4.64 W on the target hardware. However, the study focuses exclusively on the Raspberry Pi 4 platform, which limits the direct generalisability of performance and power results to other edge hardware such as the ESP32 or Raspberry Pi Pico. Additionally, while the model demonstrates high precision on the UL-ECE-MQTT-DDoS-H-IoT2025 and UL-ECE-UDP-DDoS-H-IoT2025 datasets, it has yet to be evaluated in ultra-large-scale industrial topologies or against complex multi-class attack patterns, including adversarial poisoning or stealthy lateral propagation.

Table 10 summarises DL-based techniques.

Table 10. DL-based approaches for detecting DDoS attacks in the IIoT.

Ref	Year	Approach	Product/System	Achievement	Limitations	Dataset/Testbed
[43]	2020	LSTM and CNN	Edge-centric DDoS defence system	Immediate detection, resource efficiency	Edge server dependent, needs continuous filter updates	CICDDoS
[86]	2022	DL with DNN, GRU	Edge-IIoTset dataset	Comprehensive dataset for IoT/IIoT	Primarily centralised validation	Edge-IIoTset
[17]	2023	Federated learning with CNN-MLP	DDoS classification system	Privacy-preserving	Limited to three DDoS attack types	CICDDoS2019
[76]	2022	Deep federated learning with CNN-MLP and PCC	DDoS classification for SDN-IIoT	Privacy-preserving, low-complexity	Overhead due to parameter transfer	CICDDoS2019
[10]	2024	DL with hierarchical clustering and feature selection	IIoT IDS	Improved accuracy, reduced information loss	Only tested on public datasets	NSL-KDD, CICIDS2017
[22]	2022	DRL with LightGBM	IIoT IDS	Fast convergence, automatic information mining	Centralised architecture limitations	Natural gas pipeline data (U.S. Energy Dept)
[4]	2021	DDPG-based learning	IDS for Green IoT	Lightweight, suitable for resource-constrained devices	Struggles with significant traffic fluctuations	CICDDoS2019
[89]	2023	FL with GRU and CFO-based radio fingerprinting	Hawk distributed anomaly detection for LoRa IIoT	Privacy-preserving, low computational complexity	Limited to specific hardware-based attacks	Real-world data from 60 LoRa devices
[12]	2023	FL with CNN and RNN	IIoT IDS	Privacy-preserving, decentralised learning	No FL-specific dataset	Edge-IIoTset
[44]	2021	Local GRU and multi-head self-attention	DL-based IDS	Overcomes RNN and attention limitations	Requires distributed fog infrastructure	UNSW-NB15
[30]	2024	RNN and LSTM	Low-rate DDoS attack detection	Detects low-rate attacks in SDN-IoT	May miss stealthy attacks; dataset dependence	Not clear
[90]	2024	CSAE, ABILTSM, softmax with private BC	IIoT security framework	Improved detection of DDoS and other threats	Potential BC vulnerabilities	ToN-IoT, Edge-IIoT
[77]	2021	Two DNNs with PCC	DDoS detection in 5G/B5G	Detects 10 DDoS attack types	Computational overhead and latency	CICDDoS2019
[78]	2020	Distributed RL and GAN	Anomaly detection for IIoT	Minimal false alarms, improved accuracy	High computational overhead for training	DS2OS
[45]	2023	LSTM and DNN	Botnet detection in IIoT	High accuracy, zero-day detection	Lacks heterogeneity consideration	Not specified
[91]	2023	LSTM with BC and garlic routing	Secure data sharing for IIoT beyond 5G	Improves compromise rate and scalability	Needs real-time attack evaluation	X-IIoTID

Table 10. *Cont.*

Ref	Year	Approach	Product/System	Achievement	Limitations	Dataset/Testbed
[79]	2024	NN-based expert system	IIoT attack detection for PLCs	Real-time detection, low latency, high accuracy	Limited dataset and environment	Custom testbed with PLCs
[92]	2024	GRU-assisted federated deep recurrent RL	IDS for IIoT	High accuracy, handles non-IID data	Energy consumption higher than similar approaches	TON_IoT, Edge_IIoT, X-IIoTID
[81]	2024	CNN and GRU (AttackNet)	IIoT botnet detection	Advanced feature extraction	Costly due to data volume and complexity	N_BaIoT
[82]	2023	GRU, CNN, LSTM, DNN	DDoS classification for IIoS	Real-time optimisation	Weak against low-rate DDoS attacks	CIC-DDoS2019
[83]	2022	DL-assisted software-defined security for 6G	Security architecture for OT-IT integration	Automated security orchestration	Scalability issues	Multiple (IoT Sentinel, AWID3, etc.)
[84]	2023	RMC-CNN with multi-scale grasshopper	Anomaly detection for IIoT	Secured data transmission, improved throughput	Needs resource-constrained optimisation	Testbed (power, loop, land sensor data)
[7]	2024	DQN, DDQN, D3QN, REINFORCE, A2C, PPO	NIDS for ICS/OT	Real-time adaptation	Requires adaptation for prerecorded dataset	Combined SNL-IA State OT dataset
[85]	2021	BERT-based DL for APT detection	APT detection for IIoT infrastructure	High detection accuracy	Word vector limitations may cause misjudgment	Private power grid data
[87]	2025	Hybrid CNN, LSTM, and autoencoder	DDoS detection in IoT networks	Multi-architectural synergy; captures spatial and temporal dependencies;	Poor performance on rare attack types; sensitive to data noise and class imbalance	CICIOT2023
[88]	2025	Lightweight TCN optimised with TFLite and INT8 quantisation	DDoS detection for resource-constrained edge devices	99.95% accuracy; ultra-low latency (0.19 ms); minimal model size (89.1 KB)	Evaluation limited to Raspberry Pi 4; lacks testing on multi-class and adversarial threats	UL-ECE-MQTT/UDP-DDoS-H-IoT2025 on Raspberry Pi 4

The DL-based category is the largest and most technically diverse reviewed in this work, yet it also exhibits the most pronounced gap between reported accuracy and practical deployability. Architectures such as AttackNet [81], Deep-IFS [44], and the BERT-based APT detector of [85] demonstrate that sophisticated DL models can achieve detection accuracies above 99%, but these results are almost exclusively obtained on public datasets under controlled conditions. Among sequential models, LSTM-based approaches [30,43] excel at capturing temporal attack patterns but introduce inference latency incompatible with hard real-time IIoT constraints. Federated learning variants [12,17,76] represent the most strategically important direction within this category, as they address both privacy preservation and distributed deployment, two requirements unique to IIoT environments that general IT-focused DL models ignore. Deep reinforcement learning approaches [4,22,92] offer the most promising path toward adaptive, continuously learning detection systems, but they remain computationally expensive and have not been validated under longitudinal concept drift. The overarching conclusion for this category is that accuracy is no longer the limiting factor; the field must shift its evaluation criteria toward inference latency, energy consumption, and robustness under distribution shift if DL-based IIoT DDoS detection is to move from laboratory demonstration to operational deployment.

Despite the high detection accuracy achieved by deep learning models, their computational demands and dependency on large labelled datasets highlight the need for more balanced solutions. Hybrid approaches, which strategically combine multiple paradigms, have emerged to address these trade-offs, as described below.

4.5. Hybrid-Based Approaches for DDoS Detection

The limitations of conventional approaches, resource consumption challenges, integrity advantages of BC-based solutions, and scalability and adaptability advantages of ML/DL have made hybrid DDoS attack solutions a reality in IIoT environments [74].

The authors of [46] combine a genetic algorithm with DL techniques to reduce processing time by half through feature reduction. High adaptability and improved detection/classification are achieved, but quality may be affected by dataset dependability. The model is tested against DoS, malware, backdoor, and other threats, achieving 96% accuracy on the UNSW-NB dataset. However, computational resource intensity in larger networks remains unaddressed.

In [93], the critical lack of benchmark IoT and IIoT datasets is highlighted. The solution includes seven supervised learning algorithms (logistic regression, LDA, KNN, CART, random forest, naive Bayes, SVM) and LSTM for threat identification. DDoS attacks are explored along with eight other cyber threat types. CART outperforms the others, with 77% accuracy. Privacy issues are not well explored, and the exploration is limited to specific sensors and attacks.

The authors of [47] highlight security challenges in M2M communication in the IIoT, including DDoS, sniffing, and data tampering. They implement an LSTM-based model, BC technology, onion routing, and edge intelligence with 5G integration. The approach uses virtual finger tokens and TTL fields in onion routing to enhance security, reducing computational overhead via edge intelligence. Evaluation uses confusion metrics and false negative rate, but high infrastructure requirements may arise.

The authors of [94] highlight security challenges in edge-enabled IIoT related to bot attacks, stating that bots could turn the IIoT into an Industrial Botnet of Things. A hybrid approach integrating ML and DL with cloud computing analyses connection requests from external sources to internal industrial networks, detecting malicious requests including zero-day threats. The model is flexible but needs comparison with real-world botnet detection and clarity on which ML/DL algorithms are used.

The paper [48] focuses on sensor access control systems and protection against various cyber-attacks, including DDoS. The authors implement BC for sensor access information gathering and ML for attack detection, with a five-layer architecture (sensing, protocol/network, transport, application, advanced services). The ANN algorithm outperforms other ML algorithms, with 99.97% accuracy. However, the layered architecture could increase system complexity, and effectiveness depends on the quality of ML classification and BC implementation.

The authors of [49] discuss security challenges in digital twins in IIoT systems, focusing on early botnet detection to avoid incorrect and expensive virtual model conceptualisation. They implement a BC-enabled twin framework, a DL-based botnet detection model for traffic inspection, and smart contracts for authentication. The DL model inspects half-open connections and unique IP addresses. The framework ensures secure data synchronisation between digital twin and packet auditor, inspects encrypted/unencrypted packets, and controls botnet spread through digital twin certification revocation. Accuracy of 99.97% is recorded, but further optimisation with IP-tracing methods is needed.

Moving on, [95] explores data authentication, attack prevention, and privacy preservation in IIoT-driven CPSs. The hybrid approach, named AILBSM, combines BC technology and AI. The framework uses a lightweight consensus proof-of-work for privacy preservation, an authentic intrinsic analysis model for feature encoding, and a convivial optimised sprinter nature network algorithm for attack classification. The model is evaluated against DDoS, DoS, and other cyber-attacks but is not suitable for large-scale applications due to overfitting and overlapping.

The authors of [96] discuss botnet attack detection in the IIoT, focusing on Mirai and BALLSHITE attacks. DDoS is addressed as simple but successful. The authors implement a two-step feature selection method using unsupervised learning with hybrid filter-wrapper-based selection and an optimised NN classifier with a metaheuristic algorithm. K-means clustering integrated with FGOA-KNN feature selection and Improved Harris Hawk Optimisation-Neural Network minimise unnecessary features and optimise NN parameters. However, optimisation algorithms could further enhance detection.

Villegas-Ch et al., in [97], propose a hybrid solution integrating blockchain and deep learning to enhance security, scalability, and energy efficiency in heterogeneous IoT ecosystems. The framework ensures decentralised device authentication and data traceability through a lightweight blockchain consensus protocol, while simultaneously providing real-time intrusion detection via deep learning models optimised for edge servers. Evaluated on the UNSW-NB15 dataset, the system demonstrates high performance in identifying multi-vector threats including spoofing and DoS attacks, achieving an authentication latency of just 15 ms and maintaining operational continuity in networks with up to 1000 devices, with energy consumption monitored at 150 W for large-scale deployments. However, managing the synergies between blockchain and AI in highly dynamic scenarios introduces significant architectural complexity that may require further optimisation for massive-scale deployments. Additionally, the system faces challenges in adapting to zero-day attacks without continuous retraining and federated updates to the local AI models at the edge.

Jyothsna and Jyothsna, in [98], propose a multi-layered framework for DDoS mitigation in SDN-IoT environments integrating Temporal Graph Neural Networks (TGNNs), Quantum-Inspired Approximate Optimisation (QAOA), and Federated Adversarial Learning. The TGNN captures evolving topological and temporal flow relationships, while QAOA-based feature selection reduces training and inference times by 40% and 35%, respectively, ensuring that only the most discriminative features are used. The system achieves 97.2% detection accuracy and a low latency of 35.13 ms, with a 22% improvement in stealthy attack detection compared to traditional rule-based and centralised models. However, the integration of quantum-inspired modules and federated learning layers may impose significant computational demands that challenge the most resource-constrained IoT edge devices. Furthermore, the effectiveness of the actor–critic reinforcement learning filter against sophisticated adversarial attacks depends heavily on the robustness of the federated training process, which may require extensive fine-tuning to maintain optimal performance in dynamic network conditions.

Table 11 summarises hybrid-based techniques.

Table 11. Hybrid approaches for detecting DDoS attacks in the IIoT.

Ref	Year	Approach	Product/System	Achievement	Limitations	Testbed/Dataset
[46]	2024	Genetic algorithm and DL	IIoT cyber-attack detection model	Improved processing time and classification	Dataset dependency, scalability, computational overhead	UNSW-NB
[93]	2020	Supervised learning and DL	IoT/IIoT IDS	Heterogeneous network traffic incorporation	Limited to specific sensors and attacks	ToN-IoT
[47]	2023	LSTM with BC	IDS for data security in IIoT	Reduced computational overhead	High infrastructure requirement	X-IIoTID
[94]	2022	VHN, cloud computing, and DL/ML	Secure network model for edge-enabled IIoT	Known/unknown bot detection	Clarity of algorithms and real-world comparison needed	TrickBot, PersiraiBot, MoziBot, LuaBot, MiraiBot, 0-day variant

Table 11. *Cont.*

Ref	Year	Approach	Product/System	Achievement	Limitations	Testbed/Dataset
[48]	2022	BC and ML	IIoT sensor access control system	Multiple proactive defence layers	Computational complexity from layered structure	TON-IoT
[49]	2022	BC-enabled digital twin with DL	Botnet detection for IIoT	Early detection, secure data sync, packet inspection	Needs better IP tracing for command and control servers	Bot-IoT
[95]	2023	AILBSM (BC, COSNN, LCPoW)	Security framework for IIoT-based ICS	Two-level privacy preservation	Overfitting issues	NSL-KDD, BoT-IoT, CICIDS2017, UNSW-NB15, DS2OS
[96]	2023	FGOA-kNN feature selection, IHHO-optimised NN	IIoT botnet detection	Efficient minimisation of unnecessary features	Classification algorithms need enhancement	N-BaIoT
[97]	2025	Hybrid blockchain and deep learning architecture	Scalable security for heterogeneous IoT (5G, LoRa, Wi-Fi)	95.2% precision for spoofing; 15 ms latency; energy-efficient for 1000+ devices	Complexity in dynamic scenarios; requires optimisation for massive scale	UNSW-NB15
[98]	2025	Hybrid TGNN, QAOA, and Federated Adversarial Learning	Real-time DDoS mitigation for SDN-IoT	97.2% accuracy; 22% improvement in stealthy attack detection; 35.13 ms latency	High architectural complexity; potentially heavy for ultra-constrained devices	Mendeley-DDoS, SDN-IoT-CustomSet, IoT-EdgeTrafficSet

Hybrid approaches represent the most architecturally mature category reviewed, demonstrating that combining complementary paradigms produces measurable improvements over single-method solutions. The BC-enabled digital twin framework of [49] and the AILBSM framework of [95] illustrate that integrating trust mechanisms with detection intelligence addresses threats that neither component could handle alone. The genetic algorithm and DL combination of [46] demonstrates that intelligent feature reduction can halve processing time without sacrificing detection quality, directly addressing the resource constraint problem. However, hybrid approaches introduce their own challenges: increased architectural complexity, higher integration overhead, and in several cases [47,94], insufficient clarity about which component contributes most to detection performance. The most critical observation across this category is that hybrid approaches achieve their best results when each component addresses a distinct, clearly defined limitation: BC for trust, ML for lightweight classification, DL for complex pattern recognition, and edge intelligence for latency reduction. Future hybrid designs should be guided by this principle of purposeful composition rather than combining techniques opportunistically. Overall, hybrid approaches currently offer the best balance of accuracy, adaptability, and security depth for IIoT DDoS detection, and they are the recommended direction for practitioners deploying security solutions in production IIoT environments.

Figure 10 compares the accuracy of selected approaches from each category. Note that accuracy alone does not determine superiority; the deployment environment, computational consumption, and evaluation method (testbed vs. public dataset) also matter.

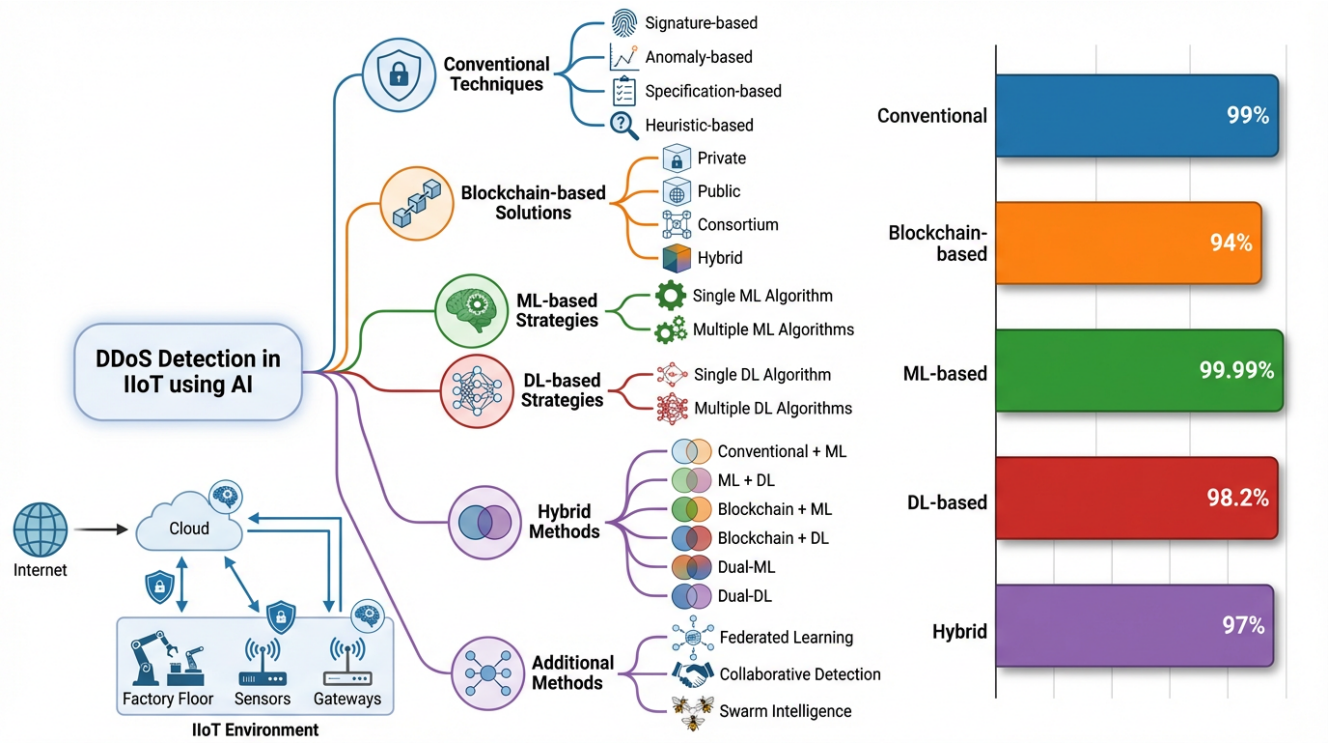

Figure 10. Accuracy comparison across selected DDoS detection approaches (exemplary).

5. Survey and Review Papers on Related Issues

This section reviews existing survey and systematic literature review (SLR) papers closely related to DDoS detection and mitigation in IIoT environments. The primary goal is to contextualise the present work within the broader research landscape, identify limitations and gaps in prior reviews, and demonstrate how this analysis extends and complements the existing body of knowledge. Each reviewed paper is assessed in terms of its focus, strengths, and limitations, with findings summarised in Table 12.

As part of our SLR, we reviewed articles on related topics to identify gaps, limitations, and strengths of previous works. The strengths and limitations of these papers are highlighted in Table 12.

The review paper [18] addressed limitations of conventional supervised and unsupervised ML techniques in IDSs, focusing on the inability to autonomously adapt to emerging threats without human intervention. After an extensive literature review, the authors proposed RL and DRL approaches. DDoS attacks are discussed as one threat in communication networks and IIoT environments, but the paper is more lenient towards communication networks than IoT/IIoT. Meanwhile, [99] presents a comprehensive survey of hybrid IDS approaches that integrate BC with federated learning for enhancing security in edge-enabled IIoT. The paper highlights challenges of centralised ML techniques resulting in computational overhead. Various research papers are evaluated based on their metrics, exploring additional AI techniques including ML and DL. Despite this, vulnerabilities of federated learning in servers, sensor nodes, and potential data breaches are overlooked.

The paper [100] provides an extensive survey on security challenges in IIoT environments, covering security requirements, potential attacks, and mitigation strategies using AI in edge systems. ML techniques are reviewed primarily, with DDoS discussed among other key threats. About 243 articles are reviewed, focusing solely on the IIoT. Although extensive, in-depth security threats are not explored, and the background on AI and BC is not satisfactory.

The systematic review in [101] analyses the use of ML- and DL-based IDSs in IoT environments. The paper is well structured, with clear breakdowns of IoT architecture, attacks, IDS architecture, and detection methods. It is comprehensive in coverage but does not provide practical demonstration or quantitative comparison of reviewed techniques.

The survey in [102] explores challenges of analysing large data generated by smart devices in industrial networks, highlighting the need for intelligent approaches. DL is highlighted as promising in the IIoT, discussing security in three phases: device, cloud, and connection security. The paper offers theoretical foundations and practical applications but only covers DL approaches, without including other AI-based or hybrid solutions.

Moving forward, the work in [32] focuses on complex security issues arising from IT and OT integration across industrial sectors. DDoS attacks are highlighted as major threats in the IIoT, particularly in manufacturing, grid systems, and healthcare. The paper analyses security challenges across different sectors and discusses countermeasures, including time-sensitive data, authentication, and access control. It is limited in practical guidelines, and most security techniques discussed are primarily for IoT environments and may not sufficiently satisfy IIoT requirements.

The authors of [103] used the PRISMA framework to analyse recent works related to ML-based IDS techniques for the IIoT. The paper highlights the need for efficient security approaches to combat threats using IDSs, addressing DDoS as difficult to identify (Mirai botnet as an example). The approach is structured and comprehensive but does not propose future directions or new technical solutions.

The review in [104] discusses detection and mitigation of DDoS attacks in smart grid environments using RL techniques, primarily analysing the use of DRL for cyber threat detection. DDoS attacks are addressed in the context of SDN-enabled smart grid applications. The paper identifies current trends and future research prospects but is limited in exploring practical implementation challenges of DRL approaches.

The authors of [105] reviewed several AI-based IDS solutions to detect botnet attacks in IIoT environments, conducting an extensive literature review and analysing 25 ML algorithms. DDoS is addressed as a prominent threat. The paper presents a comprehensive description of multiple AI models and tests on seven different IoT devices, indicating physical limitations in power, budget, and size. However, sufficient future directions are not suggested.

The authors of [106] analysed the role of ML and DL in securing 5G-driven IIoT systems through encryption, authentication, and access control. The paper analyses multiple approaches including ML, DL, BC, fog architecture, and integrated hybrid systems, providing wide comprehensive coverage from basic structure to product life cycle and a practical perspective considering both research and market realisation. The authors highlight that ML/DL algorithms could become security vulnerabilities themselves. However, limitations and future directions in using ML/DL for securing 5G-driven IIoT are not indicated.

The authors of [107] conducted a case study to address security concerns arising from the shift of traditionally offline infrastructure to online IIoT systems, focusing on DDoS attacks when ICSs become networked. The smart energy supply chain was used to analyse security concerns. The case study proposes decentralised data processing instead of aggregating IoT data into larger datasets. Future recommendations include alternative architectures for the IIoT, focus on offline-to-online transition, and emphasis on temporal aspects of security management. The study is primarily conceptual, highlighting regulatory and policy issues without quantitative metrics.

The authors of [108] discuss security threats in WSN within IoT and IIoT systems, focusing on intrusion detection mechanisms against sinkhole attacks. Various ML-based solutions are highlighted. After reviewing 60 papers, the authors propose a hybrid ap-

proach combining network modelling, mathematical analysis of routing metrics, and game theory, using the Bellman–Ford algorithm, ERNT, and isotonicity/monotonicity properties. The approach enables dynamic and static trust assessment but faces challenges with selective forwarding attacks in scale-free networks and does not evaluate BC-based or DL-based approaches.

Wainwright et al., in [109], provide a systematic review of SDN-based DDoS detection and mitigation strategies specifically for resource-constrained Small to Medium-sized Enterprises (SMEs). The study classifies current research into two distinct boundaries: lightweight ML and heuristic-based models designed for edge-based screening on devices such as Raspberry Pi, and high-accuracy hybrid deep learning models requiring cloud-assisted resource allocation. The authors contribute a conceptual closed-loop architecture where edge detection triggers mitigation rule updates at the SDN controller, addressing the need for automatic low-latency responses without expert human intervention. However, the review identifies critical limitations in the existing body of work: most solutions rely on simulated environments and stationary public datasets such as CICIDS2017 and Bot-IoT, which do not reflect the bursty traffic patterns, VPN encapsulation, or heterogeneous traffic typical of live SME or industrial networks. Additionally, there is a significant lack of integrated detection–mitigation frameworks, model explainability, and real-world benchmarks for CPU and memory consumption, leaving a gap between academic progress and deployment feasibility in actual industrial settings.

Abdulrahman and Singh, in [110], provide a comprehensive review of deep learning architectures for DDoS detection in communication networks and IoT environments. The study systematically categorises modern DL models including CNN, LSTM, and RNN, highlighting their ability to automatically learn intricate attack patterns and achieve detection rates exceeding 98%, significantly outperforming traditional rule-based and signature-based methods. The authors also contribute a detailed discussion on recent DDoS trends and provide a clear distinction between traditional and anomaly-based detection mechanisms. However, the review focuses predominantly on qualitative descriptions of DL capabilities without providing a quantitative meta-analysis. Furthermore, while critical gaps such as dataset imbalance and the need for explainable AI are identified, the paper does not provide an extensive evaluation of real-time determinism or computational overhead of these models in safety-critical IIoT environments, which remains a vital requirement for critical national infrastructure protection.

Vadlamudi and Viswa Bharathy, in [111], present a systematic review evaluating various ML and DL models for DDoS defence in IoT environments. A primary strength of this study is its comparative analysis of fifteen different methodologies, highlighting that ensemble models combining KNN with logistic regression and stochastic gradient descent achieve superior accuracies of up to 99.96% compared to standalone classifiers such as naïve Bayes. The authors also contribute a detailed discussion on the impact of data preprocessing and optimisation techniques on model stability across diverse benchmarks, including CIC-DDoS2019 and CIC-IoT2023. However, the review focuses primarily on detection accuracy metrics, with relatively little comparative assessment of real-time latency or operational overhead such as CPU and memory usage, which are critical for deployment on resource-constrained IoT edge devices. Additionally, the paper provides limited discussion on model robustness against emerging adversarial threats such as model poisoning or evasion attacks in dynamic heterogeneous IoT ecosystems.

Harshitha et al., in [112], present a systematic analysis of ML and DL techniques for DDoS detection in SDN environments, tracing the evolution of detection from traditional threshold-based methods to sophisticated intelligent systems such as CNNs that project traffic into 2D matrices to identify spatial attack patterns. The authors contribute a thorough

categorisation of benchmark datasets including CICIDS2017, CICDDoS2019, and NSL-KDD, and they compare the trade-offs between different algorithms, contrasting random forest's interpretability against SVM's high computational cost for large-scale applications. However, the review's literature search is limited to publications up to November 2022, which excludes recent advances in zero-day threat defence, federated learning, and protocol-aware detection that have emerged since. Additionally, while the paper discusses sophisticated attack patterns broadly, it lacks in-depth analysis of specific industrial protocols such as Modbus and DNP3, or the unique real-time determinism required for critical national infrastructure in IIoT environments.

Table 12 provides a summary of the reviewed SLR and review papers.

Table 12. Systematic literature review papers.

Ref	Year	Focus	Strength	Limitations
[18]	2024	Comprehensive RL/DRL IDS review	Comprehensive coverage of RL/DRL in IDSs	Focuses primarily on communication networks
[1]	2023	DDoS attacks and defence in IIoT	In-depth coverage of IIoT architecture layers	No experimental validation
[99]	2024	Hybrid (BC, FL, ML, DL) IDS analysis	Various BC- and FL-based IDSs explored	DDoS attacks not explicitly discussed
[100]	2023	IDS challenges in IIoT	Wide range of coverage	Lack of in-depth exploration, including AI use
[101]	2020	IDS security vulnerabilities in IoT	Well-structured, clear section breakdown	Limited quantitative comparison
[102]	2021	DL techniques for IIoT	Implementation framework	Only DL-focused
[32]	2023	IIoT security across IT/OT integration	Multi-domain security coverage	IoT-centric solutions for IIoT systems
[103]	2023	ML-based IDS analysis	Structured methodology	No technical solution proposal
[104]	2023	DDoS mitigation using RL	Comprehensive review of smart grid security with DRL	Lacks practical implementation challenges
[105]	2024	AI-based IDS for IoT	Comprehensive testing across multiple devices	Physical limitations of IoT (power, budget, size)
[106]	2021	5G-enabled IoT security using ML/DL	Comprehensive coverage across security taxonomy	No clear future directions
[107]	2018	Security vulnerabilities in IIoT transition	Comprehensive analysis using energy sector example	Conceptual analysis lacking practical validation
[108]	2024	WSN security in IoT/IIoT (sinkhole attacks)	Mixed methods (quantitative and qualitative)	Gap in direct attack identification
[109]	2025	SDN-based DDoS detection and mitigation for SMEs	Identifies lightweight vs. hybrid DL trends; proposes edge-based closed-loop framework	Reliance on simulated environments and curated datasets; lacks integrated detection–mitigation benchmarks and XAI
[110]	2025	Review of DL architectures for DDoS detection in IoT and communication networks	Systematic categorisation of CNN, LSTM, RNN; identifies DL superiority over traditional methods	Qualitative focus lacks quantitative meta-analysis; ignores IIoT real-time constraints
[111]	2025	Systematic review of AI-enabled DDoS defence in IoT	Comparative analysis of 15 ML/DL models; identifies high accuracy of ensemble methods (>99%)	Focuses on accuracy over latency and overhead; lacks discussion on adversarial robustness
[112]	2025	Systematic analysis of ML/DL for DDoS detection in SDN environments	Traces detection evolution from threshold-based to spatial-aware CNNs; categorises 10+ algorithms	Literature limited to 2018–2022; lacks focus on IIoT-specific protocols and real-time determinism

5.1. Strengths of the Review Papers

These review papers provide valuable insights into IIoT security challenges, offering broad perspectives on various AI-driven defence mechanisms. Many highlight key threats such as DDoS attacks and explore different detection and mitigation techniques, from traditional ML to BC-based solutions [18,100,101]. Some papers stand out by analysing multiple security layers, covering device, network, and cloud-level protections [32,102].

Others offer comprehensive literature reviews, summarising past research and identifying emerging trends [102,103]. A few introduce novel frameworks or methodologies (e.g., RL, FL), making them good starting points for further research [104,105]. Most importantly, these works help pinpoint critical research gaps, guiding future efforts to strengthen IIoT security [106–108].

5.2. Limitations of the Review Papers

The main issue with these review papers is that they often lack depth in analysis and clear future directions. Many focus on general security challenges without providing a structured comparison of different solutions [18,100]. Some highlight ML and DL techniques but miss hybrid approaches that combine multiple techniques [100,101]. While some papers conduct extensive literature reviews, they do not connect the dots or clearly show what is missing in current research [32,102]. Others are too narrowly focused on specific domains like smart grids, making it hard to apply their findings to the IIoT as a whole [104]. Many evaluate security methods primarily based on detection accuracy in simulated environments, neglecting practical deployment challenges [105,106]. Finally, inconsistent evaluation criteria across studies make it difficult to compare different approaches effectively [107,108].

6. Results and Analysis

This section presents and synthesises the key findings derived from the systematic analysis of the 82 reviewed papers. The results are structured into thematic categories encompassing AI-based detection models, hybrid approaches, and conventional and BC-based strategies. Quantitative insights are provided alongside case studies to offer a comprehensive evidence-based synthesis across all reviewed technique categories.

6.1. Key Findings

Our key findings include the effectiveness of AI techniques and challenges with implementation.

Effectiveness of AI techniques: Conventional DDoS defence systems have proven insufficient to ensure IIoT security [113]. In contrast, AI-based solutions have demonstrated promising results in autonomous detection of emerging threats in IIoT environments [114]. This is due to resource constraints in IIoT systems, including limitations in power, budget, and size, which pose significant challenges to security implementation [115].

Implementation Challenges: Many solutions demonstrated by researchers rely primarily on simulated environments rather than real-world testbeds, meaning that many proposed approaches may not be as effective as they appear when evaluated only in controlled environments. Although AI-based techniques show great potential, physical limitations of IIoT devices affect the deployment of AI-based security techniques [114]. Additionally, systems require continuous updates for the detection, classification, and mitigation of DDoS attacks.

6.2. Themes and Categories

Our themes and categories include AI-based detection models, hybrid approaches, BC-based methods, and conventional detection strategies.

AI-Based Detection Models: Multiple AI-based solutions are utilised, including traditional ML techniques (A2C, ANN, CART, CNN, D3QN, DNN, DQN, DRL, decision tree, federated learning, GAN, GRU, KNN, LDA, logistic regression, LSTM, MLP, naive Bayes, random forest, RNN, SVM, XGBoost) and DL techniques (DNN, ANN, GRU, LSTM, RNN, CNN, RMC-CNN, CNN-MLP, RBM, DBN, DBM, GAN, DQL, DRL, DQN, DDPG),

as well as hybrid approaches combining ML and DL. These techniques enable identification, classification, and mitigation of DDoS attacks in IIoT environments.

Hybrid Approaches: Solutions that combine ML/DL with BC technologies and other conventional techniques exist to detect and mitigate DDoS attacks. The integration of federated learning, which enables a high level of privacy by not sharing data for model training, is used with BC and conventional techniques to enhance detection and mitigation. Detection strategies include edge-based detection for real-time response, collaborative solutions between different AI techniques, and addressing both flood-based volumetric attacks and stealthy low-rate DDoS attacks.

6.3. Quantitative Insights

Quantitative insights include detection accuracy and performance considerations.

Detection Accuracy: DL-based algorithms such as LSTM and CNN systems achieved 98.8% detection accuracy and 99.9% classification accuracy [43]. AttackNet (CNN and GRU) demonstrated 99.75% detection accuracy [81]. CNN-MLP with federated learning achieved 98.37% accuracy. These results indicate promise in AI-based detection, classification, and mitigation.

Performance Considerations: Systems are evaluated using various metrics, including false positive rate, false negative rate, true positive rate, true negative rate, accuracy, precision, recall, F1, and area under the curve. Additionally, processing large volumes of data and computational complexity pose significant challenges due to resource constraints in IIoT systems.

6.4. Case Studies

Our case studies include real-world implementations and specific applications.

Real-World Implementations: Testing was conducted in various environments, including 500m×500m IIoT environments with multiple nodes, MiniNet and OpenFlow testbed implementations, and Bot-IoT dataset evaluation [38]. However, as mentioned, the majority of models were evaluated on simulation environments using publicly accessible datasets, indicating the necessity of creating real-world testbeds.

Specific Applications: Systems are designed for various frameworks, including SDN-based IIoT systems, edge gateway deployments, ICS environments, and BC-based certificateless signatures using the Schnorr mechanism. The analysis reveals that while AI-based DDoS detection systems show impressive accuracy rates, real-world implementation challenges such as resource limitations and scalability constraints persist [116].

7. Discussion

The implementation of AI-based security solutions for DDoS detection in IIoT environments shows promising results but also faces multiple challenges. These challenges stem from inherent limitations of IIoT devices, the complexity of attack detection, and the lack of standardised datasets, all of which hinder the full potential of AI-driven security mechanisms. Highlighting emerging trends and identifying research gaps enables stakeholders to have a clear understanding of robust, efficient, and scalable security frameworks for IIoT systems.

7.1. Critical Evaluation

We critically evaluated the strengths of the systematic analysis of current AI techniques and weaknesses in implementation and performance.

Strengths of Current AI Techniques: High detection accuracy, with multiple AI models achieving detection accuracy rates above 98%; advanced feature extraction capabilities in hybrid approaches; and effective autonomous detection of emerging DDoS threats. These

techniques also demonstrate adaptability and versatility in handling various DDoS attack types, particularly flood-based and stealthy DDoS attacks, enhancing threat detection [15].

Weaknesses: Most solutions rely on simulated environments rather than real-world applications, indicating implementation limitations. There is also high computational complexity in large-scale deployment, dependency on edge server infrastructure, and performance issues such as resource-intensiveness of complex AI models, limited validation in real industrial settings, and dynamic network topologies needing serious consideration [117,118].

7.2. Emerging Trends

Emerging techniques such as federated learning-based approaches, edge AI implementation, and BC integration are highlighted. These offer promising directions for improving DDoS detection and mitigation.

Federated learning (FL) has emerged as a promising direction for privacy-preserving and distributed DDoS detection in IIoT environments, enabling local model training without sharing raw industrial traffic data [12,17,76]. However, the practical deployment of FL in IIoT settings faces a range of serious engineering challenges that the existing literature has not yet fully resolved.

First, IIoT edge nodes are highly heterogeneous in terms of computational capacity, memory, and communication bandwidth. Devices ranging from high-performance industrial gateways to low-power wireless sensor nodes participate unevenly in the federated training process, leading to straggler effects where slower nodes delay global model aggregation or are excluded entirely, resulting in biased updates [29].

Second, IIoT networks are characterised by unstable and intermittent connectivity, particularly in remote industrial deployments using wireless or cellular links. Intermittent participation means that local models may be trained on temporally inconsistent data slices, introducing model drift across federated sites and reducing the coherence of the globally aggregated model [99].

Third, the data distributions across IIoT nodes are typically severely non-IID (non-independent and identically distributed). Different industrial sites, device types, and network topologies generate traffic with fundamentally different statistical characteristics. Standard federated averaging algorithms such as FedAvg perform poorly under non-IID conditions, and more sophisticated aggregation strategies remain computationally expensive for resource-constrained nodes [92].

Fourth, and critically from a security perspective, the federated learning process itself introduces new attack surfaces. Malicious or compromised edge nodes can perform local model poisoning attacks by injecting adversarial gradient updates that corrupt the global model without detection [70]. Similarly, the aggregation server represents a centralised point of failure that is susceptible to manipulation. These threats are particularly concerning in IIoT environments, where physical access to edge devices may be easier for adversaries to obtain.

Addressing these challenges requires advances in robust aggregation mechanisms tolerant of non-IID distributions and poisoning attempts, asynchronous FL protocols suited to intermittent connectivity, and lightweight FL implementations compatible with severely resource-constrained IIoT devices. Until these challenges are systematically resolved, the deployment of federated learning for IIoT DDoS defence remains largely conceptual rather than operationally mature.

Edge AI implementation facilitates real-time detection capabilities, enabling immediate threat detection at network edges, reducing latency in response times, and optimising resource use. Finally, BC integration enhances security by providing improved data trans-

parency and integrity, improving authentication techniques, and enabling multi-layer protection strategies, making it a powerful tool in defence against DDoS attacks.

7.3. Research Gaps

Several research gaps persist, particularly in federated learning-based techniques. For lightweight AI model development, there is a pressing need for more resource-efficient solutions, including computationally efficient models optimised for resource-limited devices while maintaining a balance between accuracy and resource usage [119]. There are also integration challenges in seamlessly incorporating AI-based models into existing security protocols. Standardisation of AI-based security protocols and ensuring interoperability between different security layers remain significant obstacles [120]. Furthermore, future research should focus on creating adaptive AI models that can handle emerging threats effectively, including the need to develop benchmark datasets for better evaluation and validation in real-world settings.

Static Training and Long-Term Model Degradation: A critical but underaddressed limitation across the reviewed literature is the near-universal reliance on static, offline training pipelines. The overwhelming majority of ML and DL models reviewed in this paper are trained once on a fixed dataset and evaluated in a closed-world assumption, where the test distribution mirrors the training distribution. This approach is fundamentally misaligned with the realities of long-term IIoT deployments, where concept drift, topology changes, device ageing, firmware updates, and workload variation continuously alter the statistical properties of network traffic [115].

In practice, a DDoS detection model trained on traffic from a manufacturing plant in 2022 may perform significantly worse when deployed in 2024, as network configurations evolve, new device types are introduced, and attack strategies adapt. Fast-evolving botnets such as Mirai and its derivatives, which continuously modify their command-and-control communication patterns and propagation mechanisms, further accelerate model staleness [45]. Similarly, zero-day attack variants that deviate from known traffic signatures can evade models that have not been updated to reflect current threat intelligence [85].

Among the reviewed approaches, only a small subset incorporates mechanisms for continuous learning or model adaptation. The SPC-DRRL approach [65] introduces an incident repository for continuous learning, and deep reinforcement learning-based methods [4,22] offer some degree of online adaptation through policy updates. However, these remain exceptions rather than the norm, and none of the reviewed works provides a systematic evaluation of detection performance under longitudinal concept drift conditions. Future research should prioritise the development of online learning frameworks, incremental model update strategies, and drift detection mechanisms specifically designed for the resource-constrained and dynamically evolving IIoT threat landscape.

This discussion highlights that AI approaches show promising results in detecting DDoS attacks in IIoT environments. However, significant challenges related to resource constraints and real-world implementation remain [14]. Emerging techniques such as federated learning and edge AI offer potential solutions, but further research is required to develop lightweight and efficient models that can be effectively integrated into existing IIoT security frameworks [121].

7.4. Challenges

Deploying AI techniques for securing IIoT environments against DDoS attacks is not straightforward. Several obstacles must be overcome to achieve effective and scalable security solutions. Key challenges include resource constraints, limitations in detection accuracy, and issues related to dataset standardisation.

Resource Constraints: One of the most pressing limitations is the constraint of computational and physical resources [14]. Unlike traditional IT systems, IIoT devices are often designed for efficiency, with minimal computational power, limited memory, and restricted storage capacity, making it challenging to deploy advanced AI models that require extensive processing capabilities.

Additionally, AI models for DDoS detection need continuous updates to remain effective against evolving cyber threats. Real-time model updates and threat analysis impose significant computational overhead that many IIoT devices are ill-equipped to handle. The challenge becomes even more pronounced for zero-day attacks, which demand rapid identification and mitigation, requiring models that can adapt dynamically to new attack patterns [122].

Power consumption is another crucial factor. Many IIoT devices operate in energy-sensitive environments, such as remote industrial locations or battery-powered systems. Implementing resource-intensive AI-driven security solutions may lead to excessive power drain, potentially reducing the lifespan and operational efficiency of these devices. Without energy-efficient AI models or alternative lightweight security approaches, deployment of AI-based DDoS detection mechanisms remains impractical for many IIoT applications.

Latency and power consumption represent two of the most critical yet underappreciated constraints on AI-based DDoS defence in IIoT environments. From a latency perspective, many IIoT deployments operate under strict real-time or near-real-time requirements, particularly in industrial control systems, SCADA environments, and manufacturing automation, where response delays of even a few hundred milliseconds can disrupt critical processes or cause cascading failures. Deep learning models such as LSTM and GRU, while achieving high detection accuracy, introduce non-trivial inference latency due to their sequential processing nature and large parameter counts. Similarly, ensemble and hybrid methods, although effective, impose compounded computational overhead that is difficult to reconcile with the tight timing requirements of delay-sensitive IIoT applications [115]. Lightweight models such as Random Neural Networks [42] and decision tree-based classifiers [67] offer faster inference but may sacrifice detection robustness against stealthy or complex attack variants.

From a power consumption perspective, a large proportion of IIoT devices are deployed in energy-sensitive environments, including remote industrial sites, battery-powered wireless sensor nodes, and solar-powered edge gateways. Running continuous AI inference pipelines on such devices introduces sustained computational loads that significantly accelerate energy depletion, reducing device lifespan and operational reliability [29]. This tension between the need for always-on security monitoring and the energy budget of constrained devices remains an open challenge. Federated learning-based approaches partially address this by distributing the computational burden across nodes [12], and edge AI implementations reduce round-trip latency by processing traffic locally [44]. Nevertheless, developing AI-based defence mechanisms that simultaneously satisfy sub-millisecond latency requirements and operate within the tight power envelopes of IIoT devices remains a largely unsolved problem, and one that warrants dedicated investigation in future research.

Detection Accuracy Challenges: Achieving high detection accuracy is another major challenge. The accuracy of AI models depends on the quality and diversity of training data. In IIoT environments, data quality issues such as extreme class imbalance, redundant features, and meaningless data can significantly degrade performance. Attack detection becomes particularly challenging when only a few instances of malicious traffic exist compared to a large volume of normal network activity.

Furthermore, IIoT networks are highly dynamic and heterogeneous, making it difficult to develop a single AI model that performs well across different deployment scenarios.

A model trained on data from one type of IIoT infrastructure may not generalise effectively to another due to variations in network protocols, device behaviour, and attack patterns. Noise in IIoT network data further complicates the learning process, leading to increased false positives or false negatives.

Another significant challenge is the lack of comprehensive, realistic datasets for model validation. Many AI-based security solutions are trained and tested in controlled environments rather than real-world IIoT settings. As a result, models may perform well in simulations but fail to detect real-time attacks when deployed in industrial environments. The absence of standardised benchmarks for evaluating AI models exacerbates this issue, making it difficult to compare different approaches and ensure consistent performance across various IIoT applications.

The Accuracy-Latency Trade-Off in IIoT Deployments: A fundamental engineering tension in AI-based DDoS detection for the IIoT is the trade-off among detection accuracy, model complexity, and inference latency. This trade-off is particularly acute in IIoT environments because industrial control systems, SCADA networks, and manufacturing automation pipelines impose hard real-time or near-real-time constraints that are incompatible with the inference overhead of complex deep learning models [29,115].

Deep learning architectures such as LSTM [30,43], GRU [44,81], and CNN-MLP hybrids [17,76] consistently report detection accuracies exceeding 98%, but their sequential processing requirements and large parameter counts introduce inference latencies that may be unacceptable in delay-sensitive contexts. For instance, LSTM models process input sequences step by step, making their latency proportional to the sequence length, which can become problematic when monitoring high-frequency industrial traffic streams. Transformer-based models, while powerful, carry even larger computational footprints and are generally unsuitable for direct edge deployment without significant compression.

Conversely, lightweight models such as the Random Neural Network [42], which achieves 99.20% accuracy with a prediction time of 120 ms on a Raspberry Pi, and decision tree classifiers [67], which operate with minimal memory overhead, offer faster inference but may lack the representational capacity to detect complex, multi-vector, or stealthy low-rate DDoS attacks. The inherent simplicity of these models can become a liability when facing sophisticated adversaries who deliberately craft traffic to evade threshold-based or shallow classifiers.

This trade-off is further compounded by the heterogeneity of IIoT deployments: a model that is computationally feasible on an industrial gateway with dedicated hardware may be entirely impractical on a battery-powered sensor node. The reviewed literature does not yet offer a systematic benchmarking of this accuracy–latency trade-off across different IIoT deployment tiers, representing a significant gap. Future research should develop tiered AI architectures that match model complexity to device capability, potentially combining lightweight edge-side detectors for fast first-pass screening with more complex fog- or cloud-side classifiers for detailed threat analysis [36,44].

False Positive Costs in Unsupervised IIoT Detection: The scarcity of labelled industrial DDoS datasets has driven interest in unsupervised and semi-supervised detection methods, which do not require fully annotated training data. However, these approaches face a particularly serious practical barrier in IIoT environments: the disproportionately high cost of false positives. In a standard IT security context, a false alarm may trigger an alert that a human analyst can review and dismiss with minimal disruption. In an IIoT environment, however, an automated mitigation response triggered by a false positive, such as blocking a traffic flow, isolating a device, or throttling a communication channel can directly interrupt industrial processes, halt production lines, disable safety monitoring systems, or cause cascading failures in tightly coupled operational technology networks [24,29].

Among the reviewed unsupervised and anomaly-based approaches, this concern is rarely quantified. The DRL-GAN framework of [78] reports minimised false alarms as an achievement, but it does not provide a production-context analysis of what a residual false positive rate would mean operationally. Similarly, isolation forest-based methods [64] and autoencoder-based anomaly detectors are known to produce elevated false positive rates when applied to IIoT traffic that exhibits natural burstiness or periodic communication anomalies unrelated to attacks. The practical usability of unsupervised methods in the IIoT therefore requires not only minimising false negatives but rigorously bounding false positive rates to levels compatible with operational continuity requirements. This necessitates the development of domain-specific threshold calibration methods, confidence-aware detection outputs, and graduated mitigation response strategies that can distinguish high-confidence detections warranting automated intervention from low-confidence anomalies requiring human review before action is taken.

Dataset Standardisation: A critical factor in the success of AI-based DDoS detection in the IIoT is the availability of high-quality datasets. However, the current landscape is plagued by a lack of sufficient real-world attack data, making it difficult to develop robust models that can effectively distinguish between normal and malicious network behaviour [123].

Most existing datasets are either outdated or fail to capture the complexity of modern IIoT threats. Additionally, many datasets used in research are artificially generated, meaning that their applicability to real-world industrial environments is limited. Without access to diverse, up-to-date attack data, AI models risk being trained on incomplete or irrelevant information, leading to poor generalisation when faced with novel attack strategies.

Another challenge is the absence of standardised evaluation benchmarks for assessing the performance of AI-based detection mechanisms. Without universally accepted benchmarks, comparing different AI models becomes difficult, hindering progress. Researchers and industry professionals require a common framework for dataset collection, labelling, and validation to ensure that AI-driven security solutions can be reliably tested and deployed in practical IIoT scenarios.

Efforts to standardise datasets must focus on collecting real-world attack data from diverse IIoT infrastructures, ensuring that AI models are trained on realistic and representative network traffic patterns. Additionally, establishing open-source repositories with well-documented datasets can facilitate collaborative research and the development of more effective and scalable AI-based DDoS detection and mitigation techniques.

DDoS Mitigation and Prevention: Observed Techniques and Effectiveness: The NETSCOUT DDoS Threat Intelligence Report for 2H 2025 provides concrete evidence of both the scale of DDoS threats and the effectiveness of mitigation approaches deployed against them [28]. Among the most effective techniques observed, anycast-based traffic distribution proved highly resilient: DNS root servers maintained high availability throughout the period despite at least 38 significant attacks, including a 21 Gbps flood, validating the effectiveness of distributed anycast architecture and capacity provisioning as a mitigation strategy [28]. Traffic predictability-based filtering also demonstrated strong practical utility, particularly against NTP-based attacks, where the highly consistent patterns of legitimate NTP traffic enabled precise filtering of anomalous traffic during more than 45,000 recorded NTP-component attack alerts [28]. At the attack complexity level, more than half of all observed attacks were multi-vector, with 42.06% using two to five vectors, confirming that single-vector mitigation approaches are insufficient for modern IIoT deployments [28]. The report also documents a decisive shift toward AI-enhanced DDoS-for-hire operations, where conversational AI interfaces now enable even unskilled adversaries to launch complex multi-vector campaigns, placing additional pressure on detection and mitigation

systems to adapt dynamically [28]. Within IIoT environments specifically, mitigation approaches reviewed in this paper span SDN-based dynamic traffic management [36,57], fog-computing-based distributed detection [31,56], federated learning for privacy-preserving collaborative defence [12,17], and blockchain-based trust frameworks [37,38], collectively reflecting the shift toward adaptive, intelligent defence mechanisms capable of responding to the evolving IIoT threat landscape.

The Generalisation Gap: A significant but underappreciated concern in the reviewed literature is the generalisation gap between performance on public benchmark datasets and robustness in real-world heterogeneous IIoT deployments. The majority of the reviewed studies evaluate their proposed models on one or two public datasets, most commonly CIC-DDoS2019, Edge-IIoTset, N-BaIoT, TON-IoT, or Bot-IoT. While these datasets have been valuable in enabling reproducible research, they were largely constructed in controlled laboratory environments using a limited set of device types and network configurations, and they may not capture the full complexity of real industrial deployments [86,93].

In practice, IIoT environments are characterised by deep heterogeneity: they encompass devices from multiple vendors running different firmware versions, communicating over a mix of protocols including Modbus, OPC-UA, Profinet, MQTT, and proprietary industrial standards, connected through hybrid wired and wireless topologies, and subject to site-specific traffic patterns that vary significantly across industries and geographic regions. A model that achieves 99% accuracy on the Edge-IIoTset dataset, which uses a seven-layer testbed with approximately ten IoT device types [86], may perform considerably worse when deployed in a real smart grid, automotive manufacturing facility, or oil and gas pipeline monitoring system, where traffic characteristics, protocol distributions, and attack patterns differ substantially from those represented in the benchmark.

Furthermore, cross-vendor deployments introduce interoperability challenges at the feature extraction level: packet header structures, timing characteristics, and flow-level statistics that serve as effective discriminating features in one deployment context may be absent, differently structured, or misleading in another. None of the reviewed studies provide cross-environment validation, multi-site evaluation, or explicit analysis of how their models degrade under distribution shift. Addressing this generalisation gap requires the creation of diverse, multi-site, protocol-aware IIoT datasets, as well as the adoption of domain adaptation and transfer learning techniques that allow models to generalise across heterogeneous industrial environments [124].

Lack of IIoT-Specific DDoS Sectoral Statistics: A further evidence gap that significantly limits the ability to prioritise defensive investments across industrial sectors is the absence of systematically reported, DDoS-specific attack statistics broken down by IIoT industry vertical. Existing threat intelligence reports tend to conflate DDoS with broader cyber threat categories or focus on general IT and Internet-facing infrastructure rather than IIoT-specific deployments. The closest available evidence comes from the NETSCOUT DDoS Threat Intelligence Report for 2H 2025, which identifies government agencies, financial services, telecommunications, transportation, and hospitality sectors as experiencing the highest concentration of DDoS attacks globally [28]. However, this report does not disaggregate DDoS impacts specifically within IIoT-connected industrial environments such as manufacturing, energy, oil and gas, or water treatment. This represents a meaningful gap: without IIoT-specific DDoS incidence data, it is difficult to calibrate sector-appropriate defence strategies or assess the relative exposure of different industrial verticals. Future research and industry reporting should work towards standardised, sector-disaggregated DDoS incident disclosure specifically for IIoT environments. Further information is provided in Table 13

Table 13. Summary of challenges in deploying AI for securing the IIoT against DDoS attacks.

Challenge	Brief Description	Status	Details
Resource Constraints	Computational and physical limitations of IIoT devices	Partially addressed	Resource-efficient AI models still in development; real-time updates and threat analysis remain challenging
Detection Accuracy Challenges	Difficulty achieving high accuracy due to data quality issues	Unaddressed	Class imbalance and noise lead to false positives/false negatives; heterogeneous network environments make model generalisation difficult
Dataset Standardisation	Lack of comprehensive, real-world datasets	Unaddressed	Existing datasets outdated or artificially generated; absence of standardised benchmarks hinders validation

Notable Datasets from Real Industrial Environments: While the majority of the reviewed studies rely on generic public datasets, several datasets collected from real or near-real industrial environments deserve explicit highlighting as more appropriate benchmarks for IIoT DDoS detection research. The WUSTL-IIoT-2018 dataset [125] was collected from a real SCADA testbed and captures genuine ICS network traffic under both normal and attack conditions, making it one of the few publicly available datasets with authentic industrial protocol behaviour. The gas pipeline and water storage tank datasets developed by Morris and Gao [126] were collected from laboratory-scale ICS environments and include multiple DoS and DDoS attack scenarios targeting industrial control processes directly. The CICAPT-IIoT dataset [127], released by the Canadian Institute for Cybersecurity in 2024, was generated using a hybrid testbed combining real and simulated IIoT components and covers more than 20 attack techniques across eight attack tactics. Most recently, a 245 GB dataset of real-world ICS network traffic in PCAP format was published by Zhejiang University [128], representing one of the largest and most realistic ICS traffic collections currently available to researchers. These datasets collectively offer significantly greater ecological validity than generic IoT benchmarks and should be prioritised in future IIoT DDoS detection research to reduce the generalisation gap discussed above.

7.5. Future Work

The findings of this systematic analysis point to several concrete and actionable directions for future research in AI-based DDoS detection and mitigation for IIoT environments. These are organised below by research priority.

Lightweight and Energy-Efficient AI Models: The most pressing research need identified across the reviewed literature is the development of AI models that can operate within the strict computational and energy budgets of IIoT edge devices. Current DL models, while achieving high accuracy, are too resource-intensive for direct edge deployment. Future research should investigate model compression techniques including pruning, quantisation, and knowledge distillation as pathways to producing edge-deployable detection models without sacrificing robustness. The Random Neural Network approach of [42], deployable on a Raspberry Pi, provides a useful baseline that future lightweight designs should aim to match or exceed in both accuracy and energy efficiency.

Online Learning and Concept Drift Adaptation:The near-universal reliance on static, offline training pipelines is a critical limitation that must be addressed. Future work should prioritise the development of online learning frameworks capable of continuously updating detection models as network traffic patterns evolve due to device ageing, topology changes,

and emerging attack families. Incremental learning strategies, drift detection mechanisms, and reinforcement learning-based adaptive policies [4,22] represent the most promising directions for building detection systems that remain effective over the full operational lifetime of an IIoT deployment.

Federated Learning for Privacy-Preserving Collaborative Defence: Federated learning is a strategically important direction for IIoT DDoS detection because it enables collaborative model training across distributed industrial sites without sharing sensitive operational data. However, as discussed in Section 7, current FL implementations face serious engineering challenges including non-IID data distributions, intermittent connectivity, and vulnerability to model poisoning attacks. Future research should develop robust aggregation mechanisms tolerant of these conditions, asynchronous FL protocols suited to unreliable industrial networks, and poisoning-resistant federated training schemes specifically validated in IIoT environments [92,99].

Protocol-Aware and IIoT-Specific Detection: The majority of the reviewed approaches rely on generic network-layer traffic statistics and are evaluated on IT-oriented datasets. Future research should develop detection models that incorporate industrial protocol semantics, including Modbus, OPC-UA, and Profinet, enabling detection of application-layer and protocol-abuse attacks that are invisible to network-layer classifiers. This requires the creation of IIoT-specific datasets capturing protocol-level traffic from real industrial deployments, which is itself an urgent research priority [1,29].

Real-World Testbeds and Standardised Benchmarks: The overwhelming reliance on public benchmark datasets such as CIC-DDoS2019, Edge-IIoTset, and N-BaIoT creates a generalisation gap that currently prevents confident claims about real-world effectiveness. Future work should prioritise the construction of multi-site, multi-protocol, multi-vendor IIoT testbeds that capture the heterogeneity of real industrial deployments. Establishing open-source, well-documented benchmark repositories specifically for IIoT DDoS detection would enable meaningful cross-study comparison and accelerate progress across the research community [66,86].

Explainable AI for IIoT Security: Industrial operators require not only accurate detection but also interpretable explanations of why a given traffic pattern was flagged as malicious, particularly in safety-critical environments where false positives can trigger costly production shutdowns. Future research should integrate explainability mechanisms such as SHAP values, attention visualisation, and rule extraction into IIoT DDoS detection models, making AI-based security decisions auditable and actionable for human operators [14].

Collaboration Between Academia and Industry: Bridging the gap between theoretical advances and operational deployment requires structured collaboration between research institutions and industrial stakeholders. Industry partners can provide access to real operational data, realistic testbed environments, and practical deployment constraints that academic research often lacks. Joint research programmes, shared dataset initiatives, and standardisation efforts coordinated through bodies such as IEC and NIST would significantly accelerate the translation of AI-based DDoS detection research into production-ready IIoT security solutions.

7.6. Recommendations

In this section, we recommend actions for practitioners, researchers, and policymakers to address challenges in IIoT security, especially in DDoS detection and mitigation.

For Practitioners: Best practices for deploying AI-based DDoS attack detection in the IIoT should be developed and disseminated. This includes implementing edge computing for low-latency detection and immediate response, as well as a layered security approach.

Adopting a defence-in-depth strategy, which incorporates multiple layers of security such as traffic analysis, access control, and vulnerability scanning, is essential [129]. Decentralised data processing should also be considered to avoid aggregating IIoT data into large datasets, and continuous monitoring and updating of threat models should be implemented based on evolving attack patterns [130].

For Researchers: Future work should focus on developing adaptive AI models capable of learning from emerging threats. Moreover, lightweight AI models suitable for resource-constrained IIoT environments should be developed. Hybrid AI approaches, which combine multiple techniques to improve security, should also be explored. Furthermore, researchers should focus on data management by creating comprehensive benchmarking datasets and developing standardised testing methodologies for real-world applications. Addressing scalability in large-scale deployments is another critical area that researchers need to explore.

Policy Recommendations: Policymakers should work towards creating standardised guidelines for AI-based DDoS detection and mitigation in IIoT systems. This includes developing a unified framework for IIoT implementations and creating standardised evaluation metrics for security solutions. Promoting collaboration between industry and academia, as well as encouraging cross-industry standardisation efforts, will facilitate faster knowledge sharing and improve the overall security of IIoT environments.

8. Conclusions

The findings from this study underscore the pressing need for advanced and adaptive security solutions in IIoT environments. While AI-driven approaches have shown great potential in detecting and mitigating emerging threats, significant challenges remain, particularly concerning resource constraints, real-world applicability, and the evolving nature of cyber threats. Addressing these issues requires a combination of innovative security frameworks, continuous updates, and a shift towards more practical deployment strategies that consider the physical limitations of IIoT systems. The systematic analysis of IIoT security highlights several critical findings, shedding light on the current state of security measures and the challenges associated with their implementation. One of the most notable insights is the effectiveness of AI-based solutions in autonomously detecting emerging threats, offering a promising approach to enhance IIoT security [131]. However, conventional defence mechanisms have proven inadequate in safeguarding IIoT environments, as they often fail to address the complex and evolving nature of cyber threats targeting industrial systems [132].

A significant challenge in implementing security solutions within IIoT frameworks stems from resource constraints, which limit the computational capacity available for running sophisticated security algorithms [133]. Additionally, many existing solutions rely primarily on simulated environments for evaluation rather than real-world testbeds, raising concerns about their practical applicability and reliability in live industrial settings [134]. Furthermore, the physical limitations of IIoT devices, such as limited processing power, memory, and energy efficiency, present additional obstacles to the deployment of AI-based DDoS detection and mitigation techniques. Another pressing issue is the need for continuous updates and improvements to security systems to effectively mitigate emerging DDoS attacks and other cyber threats. Without regular updates, even the most advanced security mechanisms may become obsolete, leaving IIoT networks vulnerable [135]. These findings emphasise the urgent need for more adaptable and resource-efficient security solutions capable of addressing the unique constraints of IIoT environments while ensuring robust protection against increasingly sophisticated cyber-attacks such as DDoS.

Author Contributions: Conceptualisation, M.A. and M.C.G.; methodology, M.A. and M.C.G.; investigation, M.A.; literature search, screening, data extraction and analysis, M.A., H.K.; writing original draft preparation, M.A.; writing review and editing, M.C.G., H.K., D.D., and M.J.L.; supervision, M.C.G.; project administration, M.C.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analysed in this study. The original contributions presented in this study are included in the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

AI	Artificial Intelligence	APT	Advanced Persistent Threat
BC	Blockchain	BERT	Bidirectional Encoder Representations from Transformers
CNN	Convolutional Neural Network	DDoS	Distributed Denial of Service
DL	Deep Learning	DNN	Deep Neural Network
DRL	Deep Reinforcement Learning	DT	Decision Tree
FL	Federated Learning	GAN	Generative Adversarial Network
GRU	Gated Recurrent Unit	ICS	Industrial Control System
IDS	Intrusion Detection System	IIoT	Industrial Internet of Things
IoT	Internet of Things	KNN	*k*-Nearest Neighbours
LSTM	Long Short-Term Memory	M2M	Machine-to-Machine
ML	Machine Learning	MLP	Multi-Layer Perceptron
NN	Neural Network	OT	Operational Technology
PCC	Pearson Correlation Coefficient	PLC	Programmable Logic Controller
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses	RF	Random Forest
RL	Reinforcement Learning	RNN	Recurrent Neural Network
SCADA	Supervisory Control and Data Acquisition	SDN	Software-Defined Network
SLR	Systematic Literature Review	SVM	Support Vector Machine
TLS	Transport Layer Security	UAV	Unmanned Aerial Vehicle
WSN	Wireless Sensor Network		

References

1. Chaudhary, S.; Mishra, P.K. DDoS attacks in Industrial IoT: A survey. *Comput. Netw.* **2023**, *236*, 110015. https://doi.org/10.1016/j.comnet.2023.110015.
2. Karie, N.M.; Sahri, N.M.; Haskell-Dowland, P. IoT Threat Detection Advances, Challenges and Future Directions. In Proceedings of the 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), Sydney, NSW, Australia, 21 April 2020; pp. 22–29. https://doi.org/10.1109/ETSecIoT50046.2020.00009.
3. Feng, Y.; Zhang, W.; Yin, S.; Tang, H.; Xiang, Y.; Zhang, Y. A Collaborative Stealthy DDoS Detection Method Based on Reinforcement Learning at the Edge of Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 17934–17948. https://doi.org/10.1109/JIOT.2023.3279615.
4. Nie, L.; Sun, W.; Wang, S.; Ning, Z.; Rodrigues, J.J.P.C.; Wu, Y.; Li, S. Intrusion Detection in Green Internet of Things: A Deep Deterministic Policy Gradient-Based Algorithm. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 778–788. https://doi.org/10.1109/TGCN.2021.3073714.
5. Nguyen, T.G.; Phan, T.V.; Hoang, D.T.; Nguyen, T.N.; So-In, C. Federated Deep Reinforcement Learning for Traffic Monitoring in SDN-Based IoT Networks. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 1048–1065. https://doi.org/10.1109/TCCN.2021.3102971.
6. Alemayehu, M.; Ghanem, M.C.; Kheddar, H.; Dunsin, D.; Kerrache, C.A.; Rathee, G. Low-Latency DDoS Detection for IIoT and SCADA Networks Using Proximal Policy Optimisation and Deep Reinforcement Learning. *Information* **2026**, *17*, 412. https://doi.org/10.3390/info17050412.
7. Sangoleye, F.; Johnson, J.; Tsiropoulou, E.E. Intrusion Detection in Industrial Control Systems Based on Deep Reinforcement Learning. *IEEE Access* **2024**, *12*, 151444–151459. https://doi.org/10.1109/ACCESS.2024.3477415.
8. Alemayehu, M.; Ghanem, M.C.; Kheddar, H. Edge-Optimized Deep and Transfer Learning for Efficient DDoS Detection in IIoT Networks. *Mach. Learn. Knowl. Extr.* **2026**, *8*, 166. https://doi.org/10.3390/make8060166.

9. Borgiani, V.; Moratori, P.; Kazienko, J.F.; Tubino, E.R.R.; Quincozes, S.E. Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks Within Industrial Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 4569–4578. https://doi.org/10.1109/JIOT.2020.3028652.
10. Lu, Y.; Chai, S.; Suo, Y.; Yao, F.; Zhang, C. Intrusion detection for Industrial Internet of Things based on deep learning. *Neurocomputing* **2024**, *564*, 126886. https://doi.org/10.1016/j.neucom.2023.126886.
11. Ferrag, M.A.; Maglaras, L.; Benbouzid, M. Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. *J. Sens. Actuator Netw.* **2023**, *12*, 40. https://doi.org/10.3390/jsan12030040.
12. Rashid, M.M.; Khan, S.U.; Eusufzai, F.; Redwan, M.A.; Sabuj, S.R.; Elsharief, M. A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. *Network* **2023**, *3*, 158–179. https://doi.org/10.3390/network3010008.
13. Kumar, R.; Kandpal, B.; Ahmad, V. Industrial IoT (IIOT): Security Threats and Countermeasures. In Proceedings of the 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Dehradun, India, 14–16 March 2023; pp. 829–833. https://doi.org/10.1109/ICIDCA56705.2023.10100145.
14. Ghanem, M.C.; Chen, T.M.; Ferrag, M.A.; Kettouche, M.E. ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance. *IEEE Access* **2023**, *11*, 129840–129853. https://doi.org/10.1109/ACCESS.2023.3332834.
15. Qureshi, S.S.; He, J.; Zhu, N.; Jia, M.; Qureshi, S.; Ullah, F.; Nazir, A.; Wajahat, A. A New Deep Learning Paradigm for IoT Security: Expanding Beyond Traditional DDoS Detection. *Int. J. Netw. Secur.* **2024**, *26*, 349–360.
16. Irshad, A.; Mallah, G.A.; Bilal, M.; Chaudhry, S.A.; Shafiq, M.; Song, H. SUSIC: A Secure User Access Control Mechanism for SDN-Enabled IIoT and Cyber–Physical Systems. *IEEE Internet Things J.* **2023**, *10*, 16504–16515. https://doi.org/10.1109/JIOT.2023.3268474.
17. Zainudin, A.; Ahakonye, L.A.C.; Akter, R.; Kim, D.S.; Lee, J.M. An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks. *IEEE Internet Things J.* **2023**, *10*, 8491–8504. https://doi.org/10.1109/JIOT.2022.3196942.
18. Kheddar, H.; Dawoud, D.W.; Awad, A.I.; Himeur, Y.; Khan, M.K. Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review. *IEEE Commun. Surv. Tutor.* **2024**, *27*, 2420–2469. https://doi.org/10.1109/COMST.2024.3484491.
19. Zhou, Y.; Cheng, G.; Zhao, Y.; Chen, Z.; Jiang, S. Toward Proactive and Efficient DDoS Mitigation in IIoT Systems: A Moving Target Defense Approach. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2734–2744. https://doi.org/10.1109/TII.2021.3090719.
20. Wang, J.; Liu, J. Deep Learning for Securing Software-Defined Industrial Internet of Things: Attacks and Countermeasures. *IEEE Internet Things J.* **2022**, *9*, 11179–11189. https://doi.org/10.1109/JIOT.2021.3126633.
21. Jyothi, E.V.N.; Kranthi, M.; Sailaja, S.; Sesadri, U.; Koka, S.N.; Reddy, P.C.S. An Adaptive Intrusion Detection System in Industrial Internet of Things (IIoT) Using Deep Learning. In Proceedings of the 2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS), Dehradun, India, 26–27 April 2024; pp. 1–6. https://doi.org/10.1109/ISTEMS60181.2024.10560245.
22. Tharewal, S.; Ashfaque, M.W.; Banu, S.S.; Uma, P.; Hassen, S.M.; Shabaz, M. Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9023719. https://doi.org/10.1155/2022/9023719.
23. Frankó, A.; Hollósi, G.; Ficzere, D.; Varga, P. Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability. *Sensors* **2022**, *22*, 9148. https://doi.org/10.3390/s22239148.
24. Horak, T.; Strelec, P.; Huraj, L.; Tanuska, P.; Vaclavova, A.; Kebisek, M. The Vulnerability of the Production Line Using Industrial IoT Systems under DDoS Attack. *Electronics* **2021**, *10*, 381. https://doi.org/10.3390/electronics10040381.
25. Hristov, A.; Pavlova, G.; Raynova, K. Developing and Experimenting Simulation Model of DDoS Attacks in IIoT Networks Using Python. In Proceedings of the 2023 31st National Conference with International Participation (TELECOM), Sofia, Bulgaria, 16–17 November 2023; pp. 1–4. https://doi.org/10.1109/TELECOM59629.2023.10409747.
26. Hristov, A.V.; Hristov, V.P. Investigation of Time for Conducting a Successful DDoS Attacks in IIoT Network. In Proceedings of the 2024 12th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 13–15 September 2024; pp. 1–4. https://doi.org/10.1109/COMSCI63166.2024.10778501.
27. Kebande, V.R.; Awad, A.I. Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions. *ACM Comput. Surv.* **2024**, *56*, 263. https://doi.org/10.1145/3635030.
28. NETSCOUT Systems. *Unmasking the Swarm: The Evolving Tactics of Botnet-Driven DDoS Attacks*; DDoS Threat Intelligence Report; Issue 16; Technical Report; NETSCOUT Systems, Inc.: Westford, MA, USA, 2026.
29. Tange, K.; Donno, M.D.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2489–2520. https://doi.org/10.1109/COMST.2020.3011208.
30. Alashhab, A.; Zahid, M.S.; Muneer, A.; Abdullahi, M. Low-rate DDoS Attack Detection Using Deep Learning for SDN-enabled IoT Networks. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 371–377. https://doi.org/10.36227/techrxiv.170472893.31491821/v1.

31. Prabavathy, S.; Reddy, I.R.P. Fog Computing based Distributed Denial of Service Attack Detection Method for Large-Scale Internet of Things. In Proceedings of the 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 23–24 March 2023; pp. 70–75. https://doi.org/10.1109/SPIN57001.2023.10116991.
32. Mekala, S.H.; Baig, Z.; Anwar, A.; Zeadally, S. Cybersecurity for Industrial IoT (IIoT): Threats, Countermeasures, Challenges and Future Directions. *Comput. Commun.* **2023**, *208*, 294–320. https://doi.org/10.1016/j.comcom.2023.06.020.
33. Kim, B.K.; Kang, Y. Abnormal Traffic Detection Mechanism for Protecting IIoT Environments. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 17–19 October 2018; pp. 943–945. https://doi.org/10.1109/ICTC.2018.8539533.
34. Snehi, M.; Bhandari, A. Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. *Comput. Sci. Rev.* **2021**, *40*, 100371. https://doi.org/10.1016/j.cosrev.2021.100371.
35. Du, M.; Wang, K. An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 648–657. https://doi.org/10.1109/TII.2019.2917912.
36. Yan, Q.; Huang, W.; Luo, X.; Gong, Q.; Yu, F.R. A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 82–89. https://doi.org/10.1109/MCOM.2018.1700621.
37. Rahman, A.; Islam, M.J.; Band, S.S.; Muhammad, G.; Hasan, K.; Tiwari, P. Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digit. Commun. Netw.* **2023**, *9*, 411–421. https://doi.org/10.1016/j.dcan.2022.11.003.
38. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. https://doi.org/10.1016/j.ipm.2021.102526.
39. Shahidinejad, A.; Abawajy, J. Efficient Provably Secure Authentication Protocol for Multidomain IIoT Using a Combined Off-Chain and On-Chain Approach. *IEEE Internet Things J.* **2024**, *11*, 15241–15251. https://doi.org/10.1109/JIOT.2023.3347677.
40. Fikriansyah, M.I.; Karimah, S.A.; Setiadi, F. Detection of DDOS Attacks in IIoT Case Using Machine Learning Algorithms. In Proceedings of the 2024 International Conference on Data Science and Its Applications (ICoDSA), Kuta, Indonesia, 10–11 July 2024; pp. 117–121. https://doi.org/10.1109/ICoDSA62899.2024.10652225.
41. Laiq, F.; Al-Obeidat, F.; Amin, A.; Moreira, F. DDoS Attack Detection in Edge-IIoT using Ensemble Learning. In Proceedings of the 2023 7th Cyber Security in Networking Conference (CSNet), Montreal, QC, Canada, 16–18 October 2023; pp. 204–207. https://doi.org/10.1109/CSNet59123.2023.10339784.
42. Latif, S.; Zou, Z.; Idrees, Z.; Ahmad, J. A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network. *IEEE Access* **2020**, *8*, 89337–89350. https://doi.org/10.1109/ACCESS.2020.2994079.
43. Jia, Y.; Zhong, F.; Alrawais, A.; Gong, B.; Cheng, X. FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks. *IEEE Internet Things J.* **2020**, *7*, 9552–9562. https://doi.org/10.1109/JIOT.2020.2993782.
44. Abdel-Basset, M.; Chang, V.; Hawash, H.; Chakrabortty, R.K.; Ryan, M. Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7704–7715. https://doi.org/10.1109/TII.2020.3025755.
45. Hasan, T.; Malik, J.; Bibi, I.; Khan, W.U.; Al-Wesabi, F. N.; Dev, K.; Huang, G. Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2952–2963. https://doi.org/10.1109/TNSE.2022.3168533.
46. Alkhafaji, N.; Viana, T.; Al-Sherbaz, A. Integrated Genetic Algorithm and Deep Learning Approach for Effective Cyber-Attack Detection and Classification in Industrial Internet of Things (IIoT) Environments. *Arab. J. Sci. Eng.* **2024**, *50*, 12071–12095. https://doi.org/10.1007/s13369-024-09663-6.
47. Gupta, R.; Jadav, N.K.; Mankodiya, H.; Alshehri, M.D.; Tanwar, S.; Sharma, R. Blockchain and Onion-Routing-Based Secure Message Exchange System for Edge-Enabled IIoT. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1965–1976. https://doi.org/10.1109/TII.2022.3191444.
48. Mrabet, H.; Alhomoud, A.; Jemai, A.; Trentesaux, D. A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. *Appl. Sci.* **2022**, *12*, 4641. https://doi.org/10.3390/app12094641.
49. Salim, M.M.; Comivi, A.K.; Nurbek, T.; Park, H.; Park, J.H. A Blockchain-Enabled Secure Digital Twin Framework for Early Botnet Detection in IIoT Environment. *Sensors* **2022**, *22*, 6133. https://doi.org/10.3390/s22166133.
50. Arat, F.; Akleylek, S. Attack Path Detection for IIoT-Enabled Cyber Physical Systems: Revisited. *Comput. Secur.* **2023**, *128*, 103174. https://doi.org/10.1016/j.cose.2023.103174.
51. Mosteiro-Sanchez, A.; Barcelo, M.; Astorga, J.; Urbieta, A. Securing IIoT using Defence-in-Depth: Towards an End-to-End Secure Industry 4.0. *J. Manuf. Syst.* **2020**, *57*, 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011.
52. Pedroso, C.; Santos, A. Dissemination control in dynamic data clustering for dense IIoT against false data injection attack. *Int. J. Netw. Manag.* **2022**, *32*, e2201. https://doi.org/10.1002/nem.2201.

53. Yang, Y.S.; Lee, S.H.; Chen, W.C.; Yang, C.S.; Huang, Y.M.; Hou, T.W. Securing SCADA Energy Management System under DDos Attacks Using Token Verification Approach. *Appl. Sci.* **2022**, *12*, 530. https://doi.org/10.3390/app12010530.
54. Yu, Y.; Chen, R.; Li, H.; Li, Y.; Tian, A. Toward Data Security in Edge Intelligent IIoT. *IEEE Netw.* **2019**, *33*, 20–26. https://doi.org/10.1109/MNET.001.1800507.
55. Zhou, H.; Pal, S.; Jadidi, Z.; Jolfaei, A. A Fog-Based Security Framework for Large-Scale Industrial Internet of Things Environments. *IEEE Internet Things Mag.* **2023**, *6*, 64–68. https://doi.org/10.1109/IOTM.002.2200195.
56. Zhou, L.; Guo, H.; Deng, G. A fog computing based approach to DDoS mitigation in IIoT systems. *Comput. Secur.* **2019**, *85*, 51–62. https://doi.org/10.1016/j.cose.2019.04.017.
57. Toko, T.M.N.N.; Bellaiche, M.; Halabi, T. A Game-theoretic Approach for DDoS Attack Mitigation in IIoT Deterministic Networking. In Proceedings of the NOMS 2024 IEEE Network Operations and Management Symposium, Seoul, Republic of Korea, 6–10 May 2024; pp. 1–5. https://doi.org/10.1109/NOMS59830.2024.10575184.
58. Mounika, G.; Sai, V.R.; Yeshaswini, V.; Hemalatha, P.; Sharan, A.S. SDN-Based Framework for Real-Time DDoS Detection and Mitigation using Mininet, POX, and Snort. In Proceedings of the 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA), Salem, India, 4–6 August 2025; pp. 77–84. https://doi.org/10.1109/ICSCSA66339.2025.11170764.
59. Srivastava, A.; Sinha, D. FP-growth-based signature extraction and unknown variants of DoS/DDoS attack detection on real-time data stream. *J. Inf. Secur. Appl.* **2025**, *89*, 103996. https://doi.org/10.1016/j.jisa.2025.103996.
60. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7059–7067. https://doi.org/10.1109/TII.2021.3084753.
61. Yeasmin, S.; Baig, A. Permissioned Blockchain-based Security for IIoT. In Proceedings of the 2020 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 9–12 September 2020; pp. 1–7. https://doi.org/10.1109/IEMTRONICS51293.2020.9216343.
62. Rajesh, H.; Moradpoor, N.; Waqas, M.; Maglaras, L. A Blockchain-Powered Defence System Against DDos Attacks with Incentivised Collaboration. In Proceedings of the 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Lucca, Italy, 9–11 June 2025; pp. 721–728. https://doi.org/10.1109/DCOSS-IoT65416.2025.00111.
63. Moudoud, H.; Abou El Houda, Z.; Brik, B. A Blockchain-Based Cross-Domain DDoS Mitigation in Consumer Networks. *IEEE Trans. Consum. Electron.* **2025**, *71*, 7095–7104. https://doi.org/10.1109/TCE.2025.3559451.
64. Mohy-Eddine, M.; Guezzaz, A.; Benkirane, S.; Azrour, M.; Farhaoui, Y. An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security. *Big Data Min. Anal.* **2023**, *6*, 273–287. https://doi.org/10.26599/BDMA.2022.9020032.
65. Ellappan, V.; Manikandan, N.; Alotaibi, S.S.; Althubiti, S.A.; Alruwaili, M.; Abdel-Khalek, S.; Mansour, R.F. Sliding Principal Component and Dynamic Reward Reinforcement Learning Based IIoT Attack Detection. *Sci. Rep.* **2023**, *13*, 20843. https://doi.org/10.1038/s41598-023-46746-0.
66. Kumar, P.; Mullick, S.; Das, R.; Nandi, A.; Banerjee, I. IoTForge Pro: A Security Testbed for Generating Intrusion Dataset for Industrial IoT. *IEEE Internet Things J.* **2024**, *11*, 36245–36258. https://doi.org/10.1109/JIOT.2024.3501017.
67. Qaddoori, S.L.; Ali, Q.I. An Efficient Security Model for Industrial Internet of Things (IIoT) System Based on Machine Learning Principles. *Al-Rafidain Eng. J.* **2023**, *28*, 329–240.
68. Qaiser, G.; Chandrasekaran, S.; Chai, R.; Zheng, J. Classifying DDoS Attack in Industrial Internet of Services Using Machine Learning. In Proceedings of the 2023 15th International Conference on Computer and Automation Engineering (ICCAE), Sydney, Australia, 3–5 March 2023; pp. 546–550. https://doi.org/10.1109/ICCAE56788.2023.10111178.
69. Sivakumar, S.; Raffik, R.; Kumar, K.K.; Hazela, B. Scada energy management system under the distributed decimal of service attack using verification techniques by IIoT. In Proceedings of the 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 5–7 January 2023; pp. 1–4. https://doi.org/10.1109/ICECONF57129.2023.10083924.
70. Salim, M.M.; Azzaoui, A.E.; Deng, X.; Park, J.H. FL-CTIF: A federated learning based CTI framework based on information fusion for secure IIoT. *Inf. Fusion* **2024**, *102*, 102074. https://doi.org/10.1016/j.inffus.2023.102074.
71. Estupiñán Cuesta, E.P.; Martínez Quintero, J.C.; Avilés Palma, J.D. DDoS Attacks Detection in SDN Through Network Traffic Feature Selection and Machine Learning Models. *Telecom* **2025**, *6*, 69. https://doi.org/10.3390/telecom6030069.
72. Mallela, R.B.; O, S.; Goud, E.A.; Rapaka, A.; Sruthi, P.R.; Yasaswi, S.N. Optimizing IoT DDoS Detection with Hybrid Feature Selection and Ensemble Learning. In Proceedings of the 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 6–8 August 2025; pp. 1004–1008. https://doi.org/10.1109/ICSCDS65426.2025.11166901.
73. Hirsi, A.; Audah, L.; Alhartomi, M.A.; Salh, A.; Ansa, G.O.; Hamdi, M.M.; Saputri, D.G.; Ahmed, S.; Farah, A. HSF: A Hybrid SVM-RF Machine Learning Framework for Dual-Plane DDoS Detection and Mitigation in Software-Defined Networks. *IEEE Access* **2025**, *13*, 112303–112323. https://doi.org/10.1109/ACCESS.2025.3583712.

74. Guezzaz, A.; Azrour, M.; Benkirane, S.; Mohy-Eddine, M.; Attou, H.; Douiba, M. A Lightweight Hybrid Intrusion Detection Framework Using Machine Learning for Edge-Based IIoT Security. *Int. Arab J. Inf. Technol.* **2022**, *19*, 822–828. https://doi.org/10.34028/iajit/19/5/14.
75. Khan, I.A.; Keshk, M.; Pi, D.; Khan, N.; Hussain, Y.; Soliman, H. Enhancing IIoT Networks Protection: A Robust Security Model for Attack Detection in Internet Industrial Control Systems. *IEEE Access* **2024**, *12*, 15244–15259. https://doi.org/10.1016/j.adhoc.2022.102930.
76. Zainudin, A.; Akter, R.; Kim, D.S.; Lee, J.M. FedDDoS: An Efficient Federated Learning-based DDoS Attacks Classification in SDN-Enabled IIoT Networks. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 1279–1283. https://doi.org/10.1109/ICTC55196.2022.9952610.
77. Amaizu, G.C.; Nwakanma, C.I.; Bhardwaj, S.; Lee, J.M.; Kim, D.S. Composite and Efficient DDoS Attack Detection Framework for B5G Networks. *Comput. Netw.* **2021**, *188*, 107871. https://doi.org/10.1016/j.comnet.2021.107871.
78. Benaddi, H.; Jouhari, M.; Ibrahimi, K.; Othman, J.B.; Amhoud, E.M. Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks. *Sensors* **2022**, *22*, 8241. https://doi.org/10.3390/s22218241.
79. Karacayılmaz, G.; Artuner, H. A Novel Approach Detection for IIoT Attacks via Artificial Intelligence. *Clust. Comput.* **2024**, *27*, 10467–10485. https://doi.org/10.1007/s10586-024-04529-w.
80. Magaia, N.; Fonseca, R.; Muhammad, K.; Segundo, A.H.F.N.; Neto, A.V.L.; Albuquerque, V.H.C.D. Industrial Internet-of-Things Security Enhanced With Deep Learning Approaches for Smart Cities. *IEEE Internet Things J.* **2021**, *8*, 6393–6405. https://doi.org/10.1109/JIOT.2020.3042174.
81. Nandanwar, H.; Katarya, R. Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Syst. Appl.* **2024**, *249*, 123808. https://doi.org/10.1016/j.eswa.2024.123808.
82. Qaiser, G.; Chandrasekaran, S.; Chai, R.; Zheng, J. Classification of DDoS traffic for Industrial Internet of Services using Deep learning approaches. In Proceedings of the 2023 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings), Mount Pleasant, MI, USA, 16–17 September 2023; pp. 1–9. https://doi.org/10.1109/AIBThings58340.2023.10292480.
83. Rahman, M.A.; Hossain, M.S. A Deep Learning Assisted Software Defined Security Architecture for 6G Wireless Networks: IIoT Perspective. *IEEE Wirel. Commun.* **2022**, *29*, 52–59. https://doi.org/10.1109/MWC.006.2100438.
84. Sankaran, K.S.; Kim, B.H. Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. *Sustain. Energy Technol. Assessments* **2023**, *56*, 102983. https://doi.org/10.1016/j.seta.2022.102983.
85. Yu, K.; Tan, L.; Mumtaz, S.; Al-Rubaye, S. Securing Critical Infrastructures: Deep-Learning-Based Threat Detection in IIoT. *IEEE Commun. Mag.* **2021**, *59*, 76–82. https://doi.org/10.1109/MCOM.101.2001126.
86. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* **2022**, *10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809.
87. Ain, N.U.; Sardaraz, M.; Tahir, M.; Abo Elsoud, M.W.; Alourani, A. Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach. *Sensors* **2025**, *25*, 1346. https://doi.org/10.3390/s25051346.
88. Akhi, M.; Eising, C.; Dhirani, L.L. Securing IoT Using Lightweight TCN for Edge Deployment on Raspberry Pi 4. *IEEE Open J. Commun. Soc.* **2026**, *7*, 442–460. https://doi.org/10.1109/OJCOMS.2025.3649498.
89. Halder, S.; Newe, T. Radio fingerprinting for anomaly detection using federated learning in LoRa-enabled Industrial Internet of Things. *Future Gener. Comput. Syst.* **2023**, *143*, 322–336. https://doi.org/10.1016/j.future.2023.01.021.
90. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network intrusion detection for IoT security based on learning techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. https://doi.org/10.1109/COMST.2019.2896380.
91. Jadav, N. K.; Kakkar, R.; Mankodiya, H.; Gupta, R.; Tanwar, S.; Agrawal, S.; Sharma, R. GRADE: Deep Learning and Garlic Routing-Based Secure Data Sharing Framework for IIoT Beyond 5G. *Digit. Commun. Netw.* **2023**, *9*, 422–435. https://doi.org/10.1016/j.dcan.2022.11.004.
92. Kaur, A. Intrusion Detection Approach for Industrial Internet of Things Traffic Using Deep Recurrent Reinforcement Learning Assisted Federated Learning. *IEEE Trans. Artif. Intell.* **2025**, *6*, 37–50. https://doi.org/10.1109/tai.2024.3443787.
93. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON-IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862.
94. Memos, V.A.; Psannis, K.E.; Lv, Z. A Secure Network Model Against Bot Attacks in Edge-Enabled Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7998–8006. https://doi.org/10.1109/TII.2022.3162837.

95. Selvarajan, S.; Srivastava, G.; Khadidos, A. O.; Khadidos, A. O.; Baza, M.; Alshehri, A.; Lin, J. C.-W. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *J. Cloud Comput.* **2023**, *12*, 38. https://doi.org/10.1186/s13677-023-00412-y.
96. Taher, F.; Abdel-Salam, M.; Elhoseny, M.; El-Hasnony, I.M. Reliable Machine Learning Model for IIoT Botnet Detection. *IEEE Access* **2023**, *11*, 49319–49336. https://doi.org/10.1109/ACCESS.2023.3253432.
97. Villegas-Ch, W.; Govea, J.; Gutierrez, R.; Mera-Navarrete, A. Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection. *IEEE Access* **2025**, *13*, 16933–16958. https://doi.org/10.1109/ACCESS.2025.3532800.
98. Jyothsna, B.; Jyothsna, V. Design of an Improved Model for DDoS Mitigation in SDN-IoT Using TGNN, QAOA, and the Federated Adversarial Learning Process. *Eng. Technol. Appl. Sci. Res.* **2025**, *15*, 29056–29061.
99. Ali, S.; Li, Q.; Yousafzai, A. Blockchain and Federated Learning-based Intrusion Detection Approaches for Edge-enabled Industrial IoT Networks: A Survey. *Ad Hoc Networks* **2024**, *152*, 103320. https://doi.org/10.1016/j.adhoc.2023.103320.
100. Alotaibi, B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. *Sensors* **2023**, *23*, 7470. https://doi.org/10.3390/s23177470.
101. Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics* **2020**, *9*, 1177. https://doi.org/10.3390/electronics9071177.
102. Latif, S.; Driss, M.; Boulila, W.; Huma, Z.e.; Jamal, S.S.; Idrees, Z.; Ahmad, J. Deep Learning for the Industrial Internet of Things (IIoT): A Comprehensive Survey of Techniques, Implementation Frameworks, Potential Applications, and Future Directions. *Sensors* **2021**, *21*, 7518. https://doi.org/10.3390/s21227518.
103. Nuaimi, M.; Fourati, L.C.; Hamed, B.B. Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review. *J. Netw. Comput. Appl.* **2023**, *215*, 103637. https://doi.org/10.1016/j.jnca.2023.103637.
104. Ortega-Fernandez, I.; Liberati, F. A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. *Energies* **2023**, *16*, 635. https://doi.org/10.3390/en16020635.
105. Shahin, M.; Maghanaki, M.; Hosseinzadeh, A.; Chen, F.F. Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems. *Adv. Eng. Inform.* **2024**, *62*, 102685. https://doi.org/10.1016/j.aei.2024.102685.
106. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Netw.* **2021**, *123*, 102685. https://doi.org/10.1016/j.adhoc.2021.102685.
107. Urquhart, L.; McAuley, D. Avoiding the internet of insecure industrial things. *Comput. Law Secur. Rev.* **2018**, *34*, 450–466. https://doi.org/10.1016/j.clsr.2017.12.004.
108. Zhukabayeva, T.; Buja, A.; Pacolli, M. Evaluating Security Mechanisms for Wireless Sensor Networks in IoT and IIoT. *J. Robot. Control* **2024**, *5*, 100371. https://doi.org/10.18196/jrc.v5i4.21683.
109. Wainwright, R.; Bagheri, M.; Salama, A.; Saatchi, R. Software-Defined Networking Security Detection Strategies and Their Limitations with a Focus on Distributed Denial-of-Service for Small to Medium-Sized Enterprises. *Appl. Sci.* **2025**, *15*, 12389. https://doi.org/10.3390/app152312389.
110. Abdulrahman, N.F.; Singh, M.S.J. Deep learning approaches for DDoS attack detection in communication networks and iot: A comprehensive review. *J. Kejuruter.* **2025**, *37*, 323–333.
111. Vadlamudi, S.; Viswa Bharathy, A.M. Systematic Study on AI-Enabled Defense Against DDoS Attacks in IoT. In Proceedings of the 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), Bidar, India, 24–25 January 2025; pp. 1–7. https://doi.org/10.1109/ICISCN64258.2025.10934519.
112. Harshitha, R.; Naralasetti, N.; Kolipakula, P.K.; Guntamukkala, S.; Faisal, S.M. Systematic Analysis of ML Techniques for Identifying DDoS Attacks in SDN Environments. In Proceedings of the 2025 IEEE 6th India Council International Subsections Conference (INDISCON), Rourkela, India, 21–23 August 2025; pp. 1–9. https://doi.org/10.1109/INDISCON66021.2025.11254618.
113. Hassan, M.M.; Huda, S.; Sharmeen, S.; Abawajy, J.; Fortino, G. An Adaptive Trust Boundary Protection for IIoT Networks Using Deep-Learning Feature-Extraction-Based Semisupervised Model. *IEEE Trans. Ind. Inform.* **2021**, *17*, 2860–2870. https://doi.org/10.1109/TII.2020.3015026.
114. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A Machine Learning Security Framework for Iot Systems. *IEEE Access* **2020**, *8*, 114066–114077. https://doi.org/10.1109/ACCESS.2020.2996214.
115. Gavric, N.; Bhandari, G.P.; Shalaginov, A. Towards Resource-Efficient DDoS Detection in IoT: Leveraging Feature Engineering of System and Network Usage Metrics. *J. Netw. Syst. Manag.* **2024**, *32*, 69. https://doi.org/10.1007/s10922-024-09848-2.
116. Lawal, M.A.; Shaikh, R.A.; Hassan, S.R. A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing. *Procedia Comput. Sci.* **2021**, *182*, 13–20. https://doi.org/10.1016/j.procs.2021.02.003.

117. Dake, D.K.; Gadze, J.D.; Klogo, G.S. DDoS and Flash Event Detection in Higher Bandwidth SDN-IoT using Multiagent Reinforcement Learning. In Proceedings of the 2021 International Conference on Computing, Computational Modelling and Applications (ICCMA), Brest, France, 14–16 July 2021; pp. 1–6. https://doi.org/10.1109/ICCMA53594.2021.00011.
118. Mishra, N.; Pandya, S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access* **2021**, *9*, 59353-59377. https://doi.org/1109/ACCESS.2021.3073408.
119. Abuhasel, K.A.; Khan, M.A. A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing. *IEEE Trans. Ind. Inform.* **2023**, *19*, 8241–8252. https://doi.org/10.1109/ACCESS.2020.3004711.
120. Oesch, S.; Chaulagain, S.; Weber, J.; Sager, S.; Carter, D.; Agbe, N.; Poloskey, G.; Lindsley, B.; Nichols, J.; Huffer, K.; et al. Towards a High Fidelity Training Environment for Autonomous Cyber Defense Agents. In Proceedings of the 17th Cyber Security Experimentation and Test Workshop, Philadelphia, PA, USA, 13 August 2024; pp. 91–99. https://doi.org/10.1145/3675741.3675752.
121. Lopez-Martin, M.; Carro, B.; Sanchez-Esguevillas, A. Application of deep reinforcement learning to intrusion detection for supervised problems. *Expert Syst. Appl.* **2020**, *141*, 112963. https://doi.org/10.1016/j.eswa.2019.112963.
122. Lin, F.; Zhou, Y.; An, X.; You, I.; Choo, K.K.R. Fair Resource Allocation in an Intrusion-Detection System for Edge Computing: Ensuring the Security of Internet of Things Devices. *IEEE Consum. Electron. Mag.* **2018**, *7*, 45–50. https://doi.org/10.1109/MCE.2018.2851723.
123. Oh, C.; Ha, J.; Roh, H. A Survey on TLS-Encrypted Malware Network Traffic Analysis Applicable to Security Operations Centers. *Appl. Sci.* **2021**, *12*, 155. https://doi.org/10.3390/app12010155.
124. Kheddar, H.; Himeur, Y.; Awad, A.I. Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review. *J. Netw. Comput. Appl.* **2023**, *220*, 103760. https://doi.org/10.1016/j.jnca.2023.103760.
125. Jain, R. *WUSTL-IIOT-2018: ICS (SCADA) Cybersecurity Dataset*; Washington University in St. Louis: St. Louis, MO, USA, 2018. Available online: https://www.cse.wustl.edu/~jain/iiot/index.html (accessed on 25 June 2026).
126. Morris, T.; Gao, W. Industrial Control System Traffic Data Sets for Intrusion Detection Research. In *Proceedings of the Critical Infrastructure Protection VIII*; Butts, J., Shenoi, S., Eds.; IFIP Advances in Information and Communication Technology; Springer: Berlin/Heidelberg, Germany, 2014; Volume 441, pp. 65–78. https://doi.org/10.1007/978-3-662-45355-1_5.
127. Canadian Institute for Cybersecurity. *CICAPT-IIoT Dataset*; University of New Brunswick: Fredericton, NB, Canada, 2024.
128. Zhou, X.; Cheng, Z.; Wang, C.; Wang, S.; Tao, C.; Zhou, Z.; Chen, X.; Luo, J.; Wang, D.; Zhou, H. A dataset collected in real-world industrial control systems for network attack detection. *Sci. Data* **2026**, *13*, 399. https://doi.org/10.1038/s41597-026-06738-x.
129. Liu, Y.; Tsang, K.F.; Wu, C.K.; Wei, Y.; Wang, H.; Zhu, H. IEEE P2668-Compliant Multi-Layer IoT-DDoS Defense System Using Deep Reinforcement Learning. *IEEE Internet Things J.* **2022**, *9*, 12456–12467. https://doi.org/10.1109/TCE.2022.3213872.
130. Li, Y.; Zuo, Y.; Song, H.; Lv, Z. Deep Learning in Security of Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 22133–22146. https://doi.org/10.1109/JIOT.2021.3106898.
131. Manaa, M.E.; Hussain, S.M.; Alasadi, S.A.; Al-Khamees, H.A.A. DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments. *Intel. Artif.* **2024**, *27*, 152–165. https://doi.org/10.4114/intartif.vol27iss74pp152-165.
132. Song, W.; Li, X.; Afroz, S.; Garg, D.; Kuznetsov, D.; Yin, H. MAB-Malware: A Reinforcement Learning Framework for Attacking Static Malware Classifiers. *arXiv* **2021**, arXiv.2003.03100. https://doi.org/10.48550/arXiv.2003.03100.
133. Liu, J.; Wang, X.; Shen, S.; Yue, G.; Yu, S.; Li, M. A Bayesian Q-Learning Game for Dependable Task Offloading Against DDoS Attacks in Sensor Edge Cloud. *IEEE Internet Things J.* **2021**, *8*, 7546–7561. https://doi.org/10.1109/JIOT.2020.3038554.
134. Hamouda, D.; Ferrag, M.A.; Benhamida, N.; Seridi, H.; Ghanem, M.C. Revolutionizing intrusion detection in industrial IoT with distributed learning and deep generative techniques. *Internet Things* **2024**, *26*, 101149. https://doi.org/10.1016/j.iot.2024.101149.
135. Zhang, T.; Feng, C.; Zhang, H.; Guo, S.; Lin, H.; Yu, S.R.; Wang, J. How to Mitigate DDoS Intelligently in SD-IoV: A Moving Target Defense Approach. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1097–1106. https://doi.org/10.1109/TII.2022.3190556.