

Review

Proactive Defence in IoT Networks for Digital Health Systems: A Scoping Review

Gihan Gunasekara * , Patricia A. H. Williams  and Ginger Mudd 

College of Science and Engineering, Flinders University, Adelaide 5042, Australia;
trish.williams@flinders.edu.au (P.A.H.W.); ginger.mudd@flinders.edu.au (G.M.)

* Correspondence: gihan.gunasekara@flinders.edu.au

Abstract

The Internet of Things (IoT) plays a significant role in digital health systems, supporting applications such as implantable devices, wearables, activity trackers and ingestibles. However, the rapid expansion of IoT networks has outpaced security measures, introducing significant security challenges. This scoping review examines the extent to which existing IoT security frameworks provide comprehensive coverage and identify key security elements that contribute to proactive defence in digital health environments. The specific research questions addressed are as follows: (1) Are there any IoT network security frameworks to provide comprehensive protection for IoT networks and digital health systems specifically? (2) What key security elements are currently used to develop a robust, proactive IoT security framework? Following the PRISMA-ScR guidelines, a systematic search of four databases was conducted to identify peer-reviewed studies from 2015 to 2024. This review included 255 studies, comprising 50 framework papers and 205 non-framework papers. The results reveal that some frameworks address discrete security areas but generally provide limited integrated security coverage. Key security elements identified include vulnerability assessments, threat modelling, feedback loops and the integration of artificial intelligence (AI) for proactive security measures in IoT networks. This review provides a structured synthesis, highlights research gaps and may inform the future development of more integrated and proactive security frameworks for IoT-enabled digital health systems.

Keywords: Internet of Things (IoT); IoT security; digital health systems; cybersecurity frameworks; proactive defence; scoping review



Academic Editors: Indranil Roy and
Ansuman Bhattacharya

Received: 19 June 2026

Revised: 3 July 2026

Accepted: 9 July 2026

Published: 14 July 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The Internet of Things (IoT) is deployed in a variety of domains and is increasingly embedded in digital health systems. Digital health encompasses the use of digital technologies to improve healthcare delivery and outcomes. The term “digital health systems” refers broadly to IoT-enabled healthcare technologies including wearables, implantable devices, remote monitoring systems, fall detection systems, vital sign monitoring and smart clinical infrastructures. However, securing IoT networks remains challenging due to constrained device resources, the absence of uniform security standards, architectural diversity, and the high value of healthcare data to cybercriminals. Security breaches in digital health systems can compromise patient safety, privacy, institutional reputation, and financial stability [1–3].

The scale of IoT growth further amplifies these risks. In 2024, the Internet of Medical Things (IoMT) was valued at approximately USD 225.8 billion and is projected to grow

to USD 2.29 trillion by 2034 [4]. The number of IoT devices worldwide is expected to exceed 31.2 billion by 2030 [5]. As connectivity expands, the attack surface correspondingly increases, and IoT devices are becoming a growing target for cyberattacks [6]. Even though advances in security technology have been widely implemented in information and communication systems, securing distributed and resource-constrained IoT environments remains an ongoing challenge. IoT networks are distributed, fragmented, and continuously connected, presenting complex and layered attack surfaces making IoT networks more vulnerable [7,8]. Many existing IoT security strategies are reactive, addressing incidents after compromise rather than anticipating evolving threats. In this review, proactive defence refers to approaches that aim to identify and mitigate risks before or during early stages of exploitation through coordinated and integrated security design. In high-sensitivity domains such as digital health, the absence of integrated proactive strategies leaves systems persistently vulnerable.

This review synthesises IoT network security frameworks, individual security elements, and defensive measures proposed for protecting IoT networks in digital health contexts. It examines both comprehensive frameworks and standalone mechanisms, providing a structured overview of how different security approaches are used in IoT-enabled digital health systems. The “comprehensive” refers to the integration of multiple complementary security functions and requirements across IoT environments, rather than relying on a single security mechanism or technology.

Existing review studies have primarily focused on specific IoT security mechanisms, individual threat categories, or particular technologies such as artificial intelligence, blockchain, intrusion detection and prevention. Other studies have examined broader IoT security challenges. However, comparatively fewer studies have examined IoT security frameworks and proactive defence approaches within the context of digital health systems. This scoping review addresses that gap by systematically examining IoT network security frameworks and proactive security elements relevant to digital health systems. Rather than simply mapping existing techniques, it provides a structured synthesis of IoT security frameworks and individual security mechanisms reported in the literature. The main contributions of this scoping review are as follows:

- To systematically map and synthesise existing IoT security frameworks and proactive defence approaches relevant to digital health systems.
- To identify key security elements and mechanisms used to support proactive IoT network defence.
- To examine gaps and limitations in current IoT security research, particularly in digital health environments.
- To provide a structured overview of emerging research trends and future directions for strengthening proactive IoT security in digital health systems.

The remainder of the paper is organised as follows: The Review section outlines the scoping review process, including the criteria for selecting studies and the analysis approach (Stages 1 to 4). The results are divided into two sections: the first (Framework Papers) focuses on security frameworks, and the second (Non-Framework Papers) focuses on security elements outside formal frameworks. Section 4 interprets the findings and highlights their implications. Finally, the Conclusion summarises the key insights and directions for future research in developing a more proactive approach to IoT-enabled digital health systems.

2. Materials and Methods

A scoping review was selected due to the broad and interdisciplinary nature of research on proactive defence in IoT networks. This approach enables a comprehensive mapping of

security frameworks, key security elements and research gaps. It is particularly effective for synthesising emerging and varied literature, providing a structured foundation for developing a proactive defence security framework for IoT networks in digital health [9].

The scoping review aimed to identify studies that discuss IoT network security frameworks, the security elements specific to IoT, and the measures implemented to protect IoT networks. The scoping review method was based on Arksey and O'Malley's (2005) five-stage framework [9]. The PRISMA-ScR guidelines were followed in this review to ensure transparent reporting, and the search was independently screened by two reviewers. A completed PRISMA-ScR checklist is included as a Supplementary Document, and the PRISMA flow diagram is included in the manuscript. The review protocol was not registered.

Stage 1: Identifying the research question.

Stage 2: Identifying relevant studies, which involves defining the keyword search terms and selecting the databases to search.

Stage 3: Selecting studies. This includes the following steps:

- Undertake searches.
- Remove duplicate papers.
- First-round screening on title and abstract using eligibility criteria.
- Second-round screening on full text using inclusion and exclusion criteria.

Stage 4: Charting the data.

Stage 5: Collating, summarising and reporting the results.

2.1. Stage 1—Identifying the Research Question

What security frameworks and security elements have been identified in the literature to provide proactive security for IoT networks in digital health systems?

2.2. Stage 2—Identifying Relevant Studies

To ensure a comprehensive coverage of the literature on Internet of Things (IoT) network security, proactive defence, cybersecurity and digital health, studies published between 2015 and 2024 were considered. The selected timeframe was chosen to capture the evolution of IoT-enabled digital health technologies and associated cybersecurity approaches over the past decade, and the review was conducted in late 2024. As this study was conducted as a scoping review, a broader timeframe was considered to support a comprehensive mapping of the literature. Four major electronic databases were selected: Scopus, ScienceDirect, IEEE Xplore, and PubMed. These databases were selected based on their extensive subject coverage, relevance to the multidisciplinary scope of the review and indexing of peer-reviewed journals and conference proceedings.

The literature search was conducted using five predefined search concepts. Search syntax was adapted as necessary to accommodate the capabilities of each database while preserving the underlying search concepts. The search concepts and corresponding Boolean expressions are reported below to improve transparency and facilitate researchers in repeating the search strategy using the same publication period and eligibility criteria.

- IoT network security, searched as "IoT network security".
- Framework for IoT network security, searched as ("Framework for IoT" OR "IoT Framework") AND "Network security".
- IoT in digital health, searched as "IoT" AND "Digital Health".
- IoT network security in digital health, searched as "Digital health" AND "IoT" AND "Network security".
- Proactive defence for internet security, searched as "Proactive defence" AND "Internet security".

Table 1 summarises the search coverage and number of papers retrieved from each database using the predefined search concepts.

Table 1. Summary of records retrieved from each database using the predefined search concepts.

Search Terms	Scopus	Science Direct	IEEE Xplore	PubMed
IoT network security	54	42	183	14
Framework for IoT network security	42	148	27	30
IoT in digital health	31	104	26	92
IoT network security in digital health	29	10	60	4
Proactive defence for internet security	21	14	60	2
Total (993)	177	318	356	142

The retrieved records were exported from each database and screened according to the predefined eligibility criteria described in the following section.

2.3. Stage 3—Selecting Studies

An in-depth search of the selected databases was conducted using predefined keywords and search queries to identify the relevant studies. All identified studies were screened for duplicates, and the duplicate entries were removed. After removing the duplicates, the screening process was conducted in two rounds. In the first-round screening, titles and abstracts of the studies were reviewed against the eligibility criteria to determine their relevance. The eligibility criteria included English-language papers and peer-reviewed studies published between 2015 and 2024. The second-round screening involved a review of the full texts, applying the inclusion and exclusion criteria to finalise the list of studies.

The following criteria were used for paper inclusion:

Existing frameworks developed for the Internet of Things (IoT) security, Internet of Things (IoT) networks OR Internet of Things (IoT) security issues and challenges OR application of artificial intelligence/machine learning/deep learning/neural networks in digital health systems for security OR proactive defence against security threats, vulnerabilities, and techniques in IoT networks. As defined in the introduction, proactive refers to approaches that aim to identify and mitigate risks before or during the early stages of exploitation. Studies proposing structured security architectures or integrated security models were considered “framework papers” while “non-framework papers” refer to studies focused on individual techniques or security mechanisms. The “digital health” studies were considered when they explicitly addressed healthcare, Internet of Health Things (IoHT), Internet of Medical Things (IoMT), patient monitoring, or related digital health environments. General IoT security studies were included when the proposed security frameworks, security mechanisms or approaches were applicable to an IoT-enabled digital health context.

The following criteria were used to exclude papers:

- Studies primarily focused on power efficiency, device design, workflow management, and network architecture without IoT security requirements.
- Studies focused primarily on IoT regulations, governance or policy without technical security.
- Studies centred on big data, data analytics, and analytics techniques without relevance to IoT security.
- Studies that did not include proactive security mechanisms, security frameworks or IoT security considerations.

Two reviewers screened the studies. Conflicting selections were resolved through discussions. The initial search revealed a total of 995 records, comprising 993 records

received from the selected databases and two industry reports identified through other sources. Duplicate records ($n = 121$) were removed, leaving 874 for the first round of screening. The two industry reports did not meet the eligibility criteria and were therefore excluded. After the first round (title and abstract screening), the remaining 332 studies were full-text reviewed (second round), resulting in 255 papers that made up the final set of studies. Figure 1 shows the PRISMA flow diagram for the search. The diagram was created following the PRISMA guidelines using Microsoft Word.

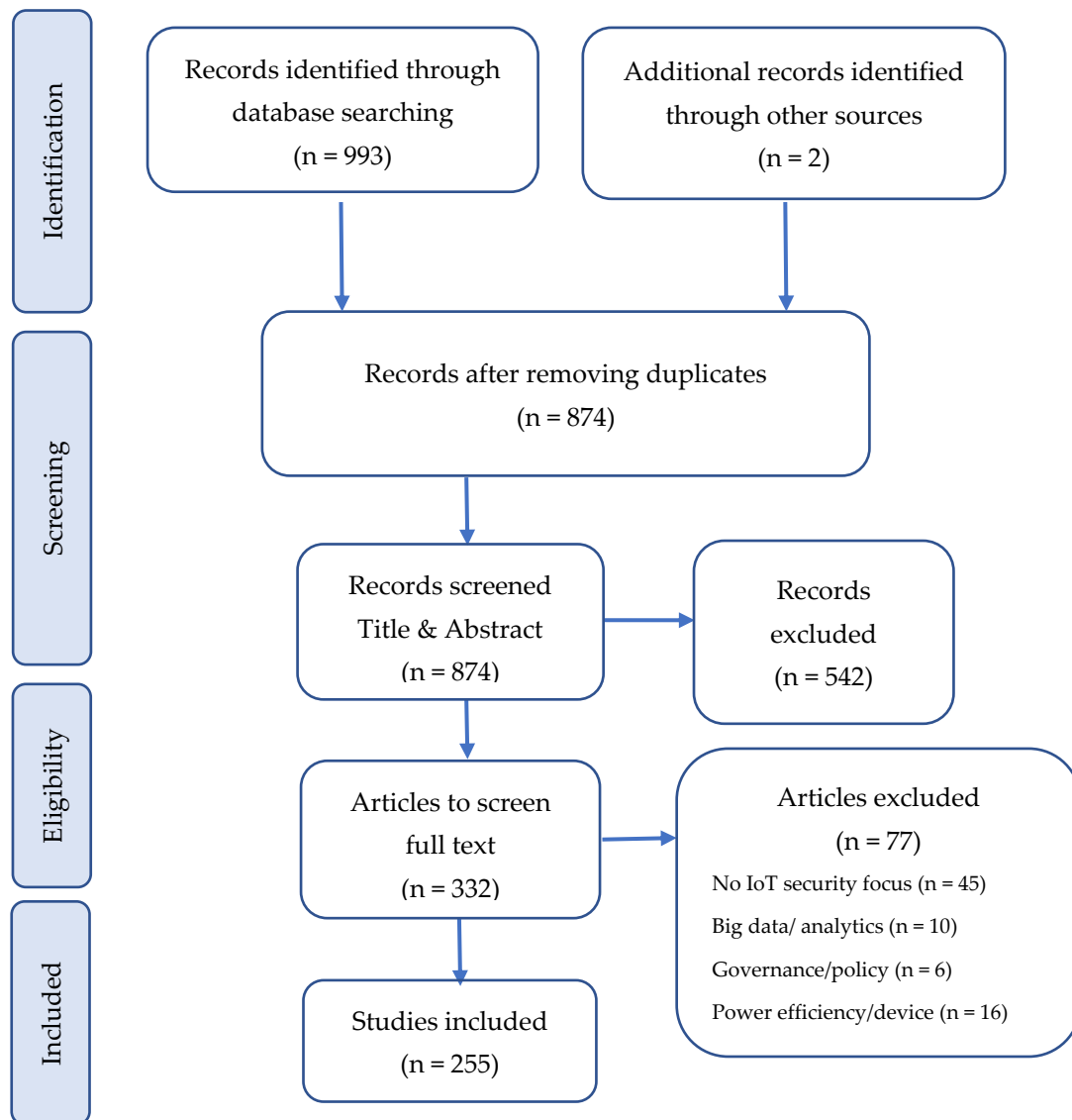


Figure 1. PRISMA flow diagram for study selection.

2.4. Stage 4: Charting the Data

For the 255 included studies, the authors, study objectives, security frameworks, security elements, security solutions and techniques were recorded. The extracted data were analysed and categorised into two groups. The first group, comprising 50 papers (Table 2 Summary of frameworks), described studies that propose or describe IoT security frameworks. The second group, comprising 205 papers (Table 3 Categorisation of the non-framework papers), focused on the remaining papers, which did not explicitly present a framework but provided valuable information regarding individual security solutions, such as methods, techniques, or mathematical models. As the aim of this review was to map the existing literature, no critical appraisal of the included studies was conducted.

Table 2. Summary of frameworks.

Year	Ref	Framework Basis	Framework Focus
2016	[10]	Lightweight authentication for WSN	Node registration, node injection, node broadcast authentication, key establishment
2016	[11]	Token-based security concept	Authentication and authorisation of mobile devices in eHealthcare
2017	[12]	Blockchain	Data security and management—internet
2017	[13]	Cloud-based security appliance	IoT network traffic flow
2017	[14]	Lightweight asymmetric cryptography, lattice-based cryptography	To secure the IoT service gateway
2018	[15]	Lightweight authentication—middleware-based	IoT node authentication
2018	[16]	Cloud and fog	IoT transmission and storage IoT applications
2018	[17]	Edge computing	Layers, protocols and applications on an IoT devices
2018	[18]	Anomaly behaviour analysis, IDS	IoT cloud-based applications and services
2018	[19]	Blockchain	Authentication, secure communication of data across IoT networks
2018	[20]	Honey pot-based technique	Detecting attacks—where the IoT devices use the UPnP protocol
2018	[21]	Data provenance (data lineage) techniques	IoT data objects
2018	[22]	Network traffic analysis	DDoS and DoS detection
2018	[23]	Machine learning Semi-supervised methods	Attack detection—FOG
2019	[24]	Graph theoretic threat provenance identification	To provide precise, accurate and quick details of topological characterisation
2019	[25]	Based on RF-PUF (radio-frequency—physical unclonable functions)	Authenticate wireless nodes
2019	[26]	Blockchain	IoT monitoring applications
2019	[27]	Identity-based security mechanism	Security and privacy—integrated internet-based smart grids
2019	[28]	Security protocols, HTTPS-SSL, AES-256 and SHA-3	Secure communication
2019	[29]	Blockchain	IoT device authentication
2019	[30]	Public key crypto—hyper-elliptic curve	Entity authentication Group communication security
2019	[31]	SDN—IOT gateway	To protect IoT-sensitive and private information
2019	[32]	Traffic monitoring—policy-based Traffic monitoring—fine-grained	Traffic monitoring—IOT network segments
2019	[33]	Machine learning	IoT memory anomaly detection
2019	[34]	Blockchain	A security network model with multilayers for IoT networks
2019	[35]	General comparison	Access control architectures—cellular, LoRaWAN, Wi-Fi

Table 2. Cont.

Year	Ref	Framework Basis	Framework Focus
2019	[36]	Blockchain	Patient data privacy, build trust in data for practitioners
2019	[37]	Machine learning	Device identification Detection of abnormal traffic
2019	[38]	Lightweight security mechanisms	Security—data in transit
2019	[39]	Systematic profile-based	IoT malware detection
2019	[40]	Novel policy-based Cyber awareness	IoT network security—channel protection Authentication, authorisation, accounting
2020	[41]	Server-client architecture	Penetration testing
2020	[42]	Blockchain	Medical data security, privacy, reliability
2020	[43]	Multimedia decryption and encryption techniques	Security of medical data (multimedia)
2020	[44]	A decentralised ledger-based data authentication—lightweight	IoT device management IoT data management
2020	[45]	IoT networks—data collection in real time	New training datasets for IDS
2020	[46]	A scheme—average dependence estimator	Intelligent DoS attack detection
2021	[47]	Blockchain, IoT things, AI	Security of e-health data Security of e-health services
2021	[48]	Extracting features using deep and stacked autoencoders Stack extracted features into an ensemble learning model Utilise deep learning with deep feature	IoT anomaly detection Dynamic attack detection
2021	[49]	IoT data generator using IoT flock	IoT network malicious traffic detection
2021	[50]	Moving target defence (MTD) techniques	Detect and mitigate DDoS attacks
2022	[51]	Software define networks Machine learning DDOS	Detection and mitigation—DDOS
2022	[52]	Analysing IoT packet samples—Stackelberg game model	Detection of DDoS attacks
2022	[53]	SDN utilising moving target defence (MTD)	Detection of DDoS attacks
2024	[54]	Blockchain—clever contracts, virtual contracts, validating transactions	IoT wireless networks
2024	[55]	Lightweight cryptographic ciphers, decision tree technique	Deployment of lightweight encryption solutions
2024	[56]	Feature selection using machine learning—Red Fox Optimisation (RFO)	Intrusion detection
2024	[57]	Machine learning (ML) balancing techniques	Real-time anomaly detection
2024	[58]	Ensemble learning	Intrusion detection
2024	[59]	Cost-effective, lightweight edge, AI-based	Secure smart home infrastructure

Table 3. Categorisation of the non-framework papers.

	Thematic Group	Number of Papers (Studies)
1	Access control	18
2	Artificial intelligence, machine learning, deep learning, neural networks	60
3	Attack detection, security assessments, cryptography	15
4	Blockchain: IoT networks—security solution, data security	23
5	Cyber defence, IoT and cloud, risk assessment, security awareness, moving target defence, cyber deception, IoT networks—DDoS detection	25
6	Forensics	1
7	Security prediction	2
8	Software-defined network (SDN)	6
9	Survey studies	26
10	Systematic reviews	3
11	Threat landscaping, threat modelling, IDS and IPS in IoT networks	25
12	Zero trust	1
	Total	205

2.5. Stage 5: Collating, Summarising and Reporting the Results

In line with the standard structure of review articles, the findings from stage 5 are presented in Section 3.

3. Results

Table 2 describes the frameworks found. A framework is defined as a comprehensive structure designed to guide the design, implementation or assessment of security solutions in IoT networks. Such frameworks typically provide key components, processes, and methodologies for securing IoT networks. Table 3 focuses on the papers that do not offer structured frameworks but may contribute essential insights into the diverse approaches to address IoT network security challenges. Presenting results in these two groups allowed for a clearer distinction between the overarching framework-based solutions and individual security solutions. This highlights the importance of both sources: frameworks offer a holistic view, while the other papers provide detailed, specialised information, which is essential to understanding the technical domain of IoT network security. From the 255 studies included in the scoping review, 50 framework papers were selected for the qualitative analysis (Table 2), while the remaining 205 studies were categorised thematically (Table 3) but not individually cited.

Table 2 summarises the 50 frameworks found during the scoping review process related to IoT networks, digital health, and proactive defence. It details the year, reference, the framework it is based on, and its focus. These are listed in date order from oldest to newest. This table concisely summarises the frameworks and their respective attributes, facilitating easy comparison and further discussion. The framework-based analysis was pivotal in understanding the technologies, techniques, and mathematical functions used to secure IoT networks. The review’s “framework focus” further allowed for identifying key areas, aspects, or components integral to protecting IoT networks. Table 2 presents the diverse security frameworks identified in the selected studies, sorted by publication year.

The frameworks primarily fall into several key categories: blockchain-based solutions for secure communication and data management, lightweight authentication and cryptographic solutions to secure resource-constrained IoT devices, and cloud and edge computing-based frameworks for distributed data processing and storage. Additionally, artificial intelligence and machine learning frameworks are frequently used for anomaly detection and attack identification in real time, while honeypots and intrusion detection

and prevention systems (IDPSs) are employed to detect and mitigate security incidents in IoT networks. Further, access control mechanisms and software-defined networking-based solutions were used to secure the communication in IoT networks.

The reviewed frameworks in Table 2 indicate an evolution in IoT security research from lightweight authentication, cloud and edge-based security to blockchain-based solutions and artificial intelligence and machine learning security defence strategies. The studies [10–15] are based on lightweight authentication and middleware-based mechanisms for resource-constrained environments emphasising node registration and security key establishment. These approaches have low computational resource requirements. However, these approaches rely on static keys or fixed protocols, which limit their ability to adapt to sophisticated or emerging attacks, such as advanced persistent threats.

Blockchain-based security frameworks [12,19,26,29,34,36,42,47,54] focus on distributed trust and immutable ledger concepts to improve secure authentication, data integrity and privacy preservation. These security solutions contribute to overcoming the single point of failure and increase transparency but are challenged by the energy and computational resource requirements in IoT networks.

Machine learning (ML) [33,37,56,57] and ensemble learning techniques [48,58] have been used for proactive, data-driven intrusion detection and real-time anomaly detection in IoT networks. The performance of these models is constantly challenged by the availability of quality datasets and the heterogeneous nature of IoT devices.

Software-defined networking (SDN) and moving target defence (MTD)-based approaches [50,53] have been used to improve the responsiveness and mitigate distributed denial of service (DDoS) attacks using traffic monitoring and system reconfiguration techniques. While SDNs are used to provide security, they have drawbacks. In the event of a failure in the software-driven controller or having unauthorised access to the controller, the whole network will be unavailable [60]. Further, SDNs are susceptible to topology poisoning and side-channel and botnet attacks [61,62]. Lightweight cryptography and hybrid options [14,38,44,55,59] have been used to secure data transmission and storage in IoT networks. However, balancing the strength of the encryption and computational efficiency continues to pose a challenge.

Table 3 presents the remaining 205 papers that did not relate to frameworks. The table organises these studies into thematic groups that emerged during the analysis, representing a combination of security technologies, functions, techniques and solutions relevant to IoT network security. Collectively, these studies provide a holistic view of widely reported approaches, research trends and advancements in protecting IoT networks. The thematic groups in Table 3 are arranged in alphabetical (A-Z) order for clarity.

Figure 2 presents the distribution of reviewed studies by security solution category. The chart provides a visual summary of the security solutions identified in the literature, with each bar representing the percentage of the total ($n = 205$). Figure 2 complements Table 3 and serves as a reference for the detailed analysis for each category discussed in the following section. Figure 2 was generated using Microsoft Excel graphing.

Overall, the distribution of studies across the identified categories suggests that proactive IoT security research is focused on specific technical mechanisms such as AI-based approaches and blockchain-based protections, while fewer studies adopt broader integrated security approaches. These patterns indicate that the field remains fragmented, particularly in the context of digital health. The findings highlight the need for comprehensive, context-aware and proactive security approaches for digital health systems.

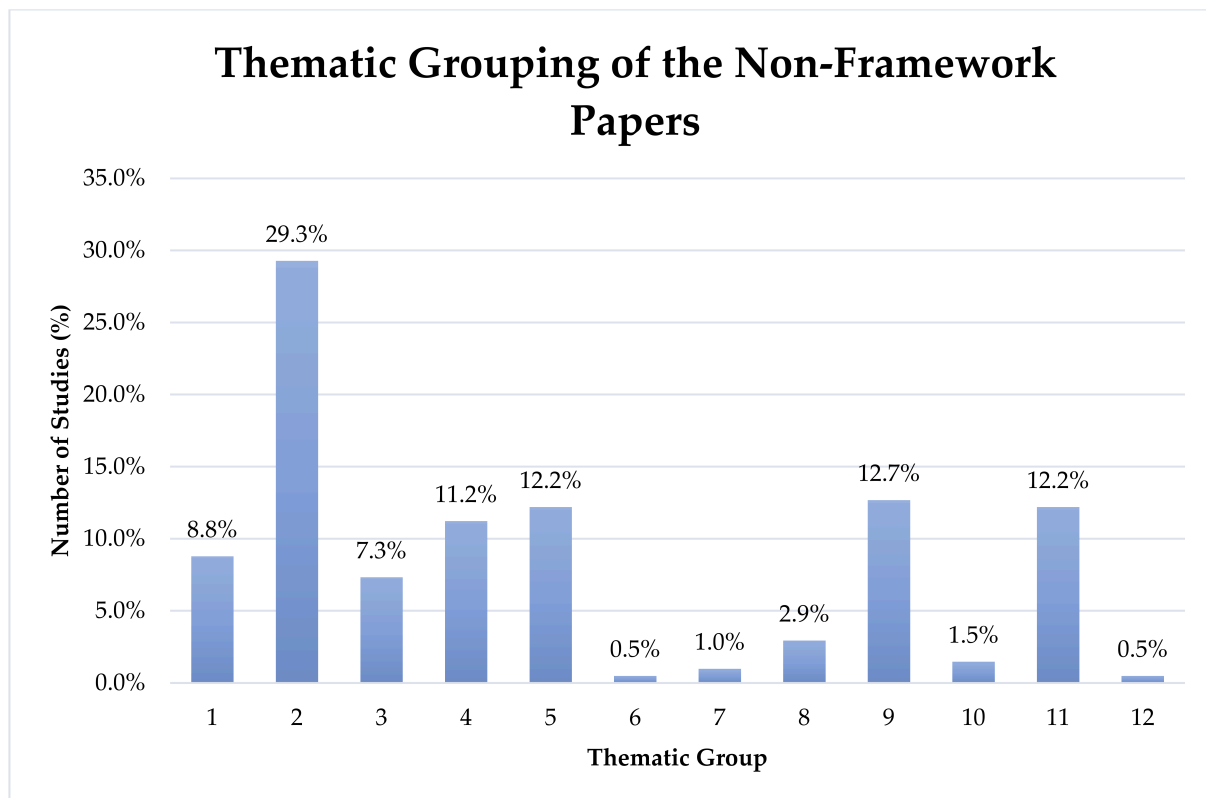


Figure 2. Distribution of non-framework papers.

According to Table 3, artificial intelligence-based approaches dominate the present IoT network security research. Sixty studies have utilised artificial intelligence (AI), machine learning (ML), deep learning (DL), and neural networks (NNs) to discuss access control, network traffic analysis, attack detection, and implementing intrusion detection systems. The literature heavily discusses intrusion detection and prevention systems. Various techniques, including AI, ML, DL, NN, and other mathematical functions, are used to analyse network traffic and patterns and detect abnormalities. This highlights trends toward data-driven and adaptive defence mechanisms capable of identifying evolving and unknown attacks that traditional security mechanisms cannot.

Twenty-three studies have utilised blockchain to implement access control mechanisms to identify, authenticate, and authorise users, IoT devices, and wireless nodes and apply security to data in use, transit, and storage. Most blockchain studies focus on information exchange, access and transaction management, trust, continuous integrity, tamper-proofing, provenance, and data traceability [26]. The use of blockchain for security in IoT networks supports transparency and accountability across IoT devices, but its scalability and suitability in low-resource environments remain a challenge.

Twenty-five papers that were focused on cyber defence were found. As a defence concept, moving target defence (MTD) increases the complexity of the network by making constant changes to the attack surface [63]. MTD is used for attack prevention, tolerance, and early identification of attacks such as DDoS attacks. Further studies use cyber threat intelligence, software-defined networks and MTD techniques in cloud-based applications to provide proactive defence mechanisms. Further, papers focus on software security models, solutions, intrusion detection systems, security assessments, prototype architectures, risk assessments, impact analysis, attack detection and general data security concepts. This shows a growing emphasis on proactive threat response and network resilience.

Data encryption and decryption techniques such as cryptography, pseudonymisation and anonymisation, hyperelliptic curve-based public key cryptosystem, lightweight asymmetric cryptography, and lattice-based cryptography have been used for access control and data security.

Cloud, fog, and edge technologies are implemented for security in IoT networks, applications, data transmission, storage, and IoT network traffic analysis. Further, cloud, fog, and edge-based solutions are used to control IoT network traffic flow, identify policy violations, protect IoT services from attacks, and ensure the security and privacy of IoT by deploying software-based appliances.

Twenty-six survey studies discussed different areas in IoT networks and network security-related aspects in digital health systems. The focus areas were security and privacy issues, security challenges, security requirements, secure communication and routing, security vulnerabilities, threats, attacks, AI and IDS, blockchain in IoT, encryption and decryption techniques, cryptography and IoT trust models. The systematic literature review studies discussed enforcing security in IoT, information security, and different security frameworks. Fourteen papers discuss protocol design for privacy, lightweight key establishment, and routing.

Software-defined networks (SDNs), security predictions, zero trust and forensics have a comparatively lower number of studies, highlighting the need for future research. They have been used to implement IoT gateways and policy-based internet traffic monitoring in IoT networks. A research study about “zero trust” describes attempts to prevent advanced persistence attacks (APTs) in local area networks from IoT devices [64]. The study’s primary focus is the local area network, not the IoT network, and it uses the traditional network security concepts of micro-segmentation and the next-generation firewall in conjunction with zero-trust concepts. Two studies have discussed security predictions. Security prediction refers to predicting the future security of the IoT network using mathematical models based on historical IoT data and the network status [65,66].

Tables 1 and 2 provide a comprehensive view of the various approaches to IoT network security, preparing the foundation for a thorough study of the strengths, limitations, and potential applications of these security frameworks and individual security elements within the context of proactive defence strategies. Overall, the analysis reveals that the studies targeted a specific security area or an attack rather than broader integrated security coverage.

4. Discussion

This review’s contribution is in synthesising and structuring a fragmented body of literature on proactive cybersecurity approaches in IoT-enabled digital health systems. While many studies propose architectural or conceptual security solutions, comparatively few provide evidence regarding scalability, deployment feasibility or performance on real-world IoT networks in digital health environments. Many studies rely on simulation-based or testbed evaluations, limiting the understanding of how proposed security solutions perform in practical IoT-enabled digital health systems under constraints, such as resource-constrained devices, interoperability or legacy infrastructure. By classifying studies according to implementation maturity and validation context, this review highlights critical gaps between proposed frameworks and deployable cybersecurity solutions.

This research aimed to identify comprehensive approaches to IoT network security, where “comprehensive” refers to integrating multiple security functions and requirements across IoT environments. Analysis of the studies in Tables 1 and 2 suggests that most papers focus on a specific security area or attack type, while relatively few studies attempt a broader integrated security coverage.

Based on the analysis of the reviewed papers, a comprehensive security framework should incorporate a wide range of security concepts. Key elements, such as artificial intelligence (AI) for anomaly detection, machine learning (ML)-based threat recognition, feedback loops and interrelated security elements, enhance each other's functionality and strengthen the overall security defence. Recent developments beyond the review period further support this trend, with hybrid deep learning approaches being proposed for anomaly detection and adaptive threat identification in IoT ecosystems [67]. In-depth vulnerability assessments, threat modelling and the systematic mapping of these assessments to IoT architecture, particularly in the context of digital health systems, were notably underexplored in the literature. As an emerging approach, the zero-trust security architecture remains underutilised in IoT networks.

The deployment of AI-enabled, blockchain-based and software-defined security solutions is promising. Each technology offers distinct advantages and limitations. AI and ML approaches are capable of anomaly detection and adaptive threat identification, but often require high-quality data and substantial computational resources. Blockchain enhances data integrity, trust and decentralised security management, but scalability, latency and resource consumption remain challenges. SDN enables flexible network management and dynamic control, but introduces potential single points of failure. MTD approaches increase the difficulty of attacker reconnaissance, although they may introduce implementation complexities. Collectively, challenges relating to computational requirements, scalability and interoperability remain significant, particularly in digital health environments. In addition, implementations may face challenges due to legacy systems, resource-constrained devices, diverse devices and regulatory requirements within IoT-enabled digital health systems. Due to the heterogeneous nature of IoT devices, applying traditional security measures is challenging and not straightforward. IoT networks utilise diverse communication protocols and connection methods depending on the application, making a single security solution insufficient. Unlike many general IoT applications, cybersecurity incidents in digital health environments may directly affect patient safety, continuity of care and the availability of healthcare services. These characteristics increase the complexity of implementing and validating proactive cybersecurity solutions in IoT-enabled digital health systems. Consequently, the direct translation of general IoT security solutions into digital health environments is not always straightforward and requires the consideration of healthcare-specific operational, regulatory and patient safety requirements.

Deploying IoT networks without comprehensive security measures can lead to insecure IoT networks, which may expose broader healthcare infrastructure to high risk and allow attackers to exploit weaknesses to gain access to critical systems. Therefore, IoT network security frameworks must be robust and capable of addressing constantly evolving threats, as well as minimising security risk to the greater network. The findings of this review may serve as a foundation for developing a unified and proactive defence security framework for IoT-enabled digital health systems. The identified security elements and research gaps provide a critical foundation for future research aimed at developing integrated, multilayered proactive security frameworks tailored to IoT-enabled digital health systems. By leveraging the identified and collated security elements and addressing the gaps, such frameworks could offer broader, more integrated security protection while remaining adaptable to the diverse and evolving nature of IoT environments.

Within the scope of this review, the findings addressed the research questions that guided this study. Several studies proposed security frameworks for IoT networks and digital health systems. However, these frameworks generally addressed specific security areas or provided a partial coverage of broader digital health security requirements. Furthermore, evidence of real-world deployment and validation was limited. The review

also identified a broad range of security technologies, functions, techniques and solutions relevant to proactive IoT network security. Collectively, these studies provided a holistic view of widely reported approaches, research trends and advancements in protecting IoT networks and highlighted the importance of integrating multiple security elements to strengthen proactive defence in the digital health context.

The identified research gaps suggest several directions for future work. Future studies should focus on developing and evaluating integrated security frameworks, with validation in real-world digital health environments. Additionally, greater attention should be given to threat modelling, vulnerability assessments, digital forensics, zero-trust architectures and development of evaluation metrics for digital health environments. Further, future research should investigate deployment strategies that address practical implementation challenges such as legacy systems, resource-constrained devices, diverse devices and regulatory requirements in complex digital health environments.

This scoping review has several limitations. First, the review was limited to English-language, peer-reviewed studies between 2015 and 2024, which may have excluded relevant studies published in other languages or outside the selected timeframe. Second, four major databases were searched, and additional relevant studies published elsewhere may not have been captured. Third, no formal appraisal was conducted, and the quality of the included studies was not assessed. Further, the review protocol was not prospectively registered. The review followed a predefined methodology and adhered to the PRISMA-ScR reporting guidelines to promote transparency, methodological rigour and reproducibility while reducing the potential for reporting bias. In addition, this review primarily focused on technical security elements and proactive cybersecurity approaches in IoT-enabled digital health systems. Regulatory, ethical and governance aspects were acknowledged as important to the security of digital health systems. However, they were not examined in detail as the review's primary aim was to map technical security. Future research should integrate regulatory, ethical and governance perspectives to support digital health security frameworks. In addition, future research should investigate evaluation metrics for assessing IoT security frameworks, interoperability challenges and the integration of zero-trust architectures in digital health environments.

Overall, this review provides a structured understanding of critical security elements for proactive IoT network security in digital health systems, offering guidance for developing more integrated and proactive security frameworks for IoT-enabled digital health systems.

5. Conclusions

This scoping review synthesised 255 studies, comprising 50 framework papers and 205 non-framework studies, which examined IoT network security frameworks, security elements, technologies, functions, techniques and solutions relevant to digital health systems. The analysis, categorising frameworks into “framework basis” and “framework focus”, highlighted both broader security approaches and individual security solutions, providing a detailed understanding of the technologies, techniques and security components essential for securing IoT networks. The findings indicate that current research is dominated by artificial intelligence and machine learning approaches, blockchain technologies and intrusion detection and prevention systems, while comparatively less attention has been given to areas such as zero-trust architectures and digital forensics.

This review highlights the ongoing need for both broad, structured security frameworks and specialised technical approaches to address evolving security challenges in IoT-enabled digital health systems. Although numerous studies have proposed conceptual and architectural security solutions, comparatively few have demonstrated real-world deployment and validation in digital health environments. The findings also emphasise

the importance of a technology-agnostic and vendor-neutral security framework, enabling IoT security implementers to adapt security elements to specific operational and health-care use-case requirements. While this review primarily focused on technical security elements, regulatory, ethical and governance considerations remain important areas for future research. By identifying current security approaches, research trends and emerging directions, this study provides a structured synthesis of existing knowledge and supports future research into more integrated, context-aware and proactive validated IoT security frameworks for digital health systems.

Supplementary Materials: The following supporting information can be downloaded at <https://www.mdpi.com/article/10.3390/electronics15143091/s1>. Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) Checklist [68].

Author Contributions: Conceptualisation, G.G. and P.A.H.W.; methodology, G.G.; software, G.G.; validation, G.G., P.A.H.W. and G.M.; formal analysis, G.G.; investigation, G.G. and G.M.; resources, G.G.; data curation, G.G. and G.M.; writing—original draft preparation, G.G.; writing—review and editing, G.G., P.A.H.W. and G.M.; visualisation, G.G.; supervision, P.A.H.W.; project administration, G.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data supporting the findings of this review are available within the article. Original database export files, retrieval counts, screening records and study extraction files are retained by the corresponding author and are available upon reasonable request.

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

References

1. Coventry, L.; Branley, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* **2018**, *113*, 48–52. [CrossRef] [PubMed]
2. Yeng, P.K.; Nweke, L.O.; Woldaregay, A.Z.; Yang, B.; Snekenes, E.A. Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: A systematic review. In *Intelligent Systems and Applications. IntelliSys 2020*; Advances in Intelligent Systems and Computing Series; Springer: Cham, Switzerland, 2021; pp. 1–18. [CrossRef]
3. Triplett, W. Cybersecurity vulnerabilities in healthcare: A threat to patient security. *Cybersecur. Innov. Technol. J.* **2024**, *2*, 15–25. [CrossRef]
4. Internet of Medical Things Market to Hit USD 2294.87 Billion by 2034. 2025. Available online: <https://www.precedenceresearch.com/internet-of-medical-things-market> (accessed on 20 November 2025).
5. Statista. Number of Internet of Things (IoT) Connected Devices Worldwide from 2022 to 2023, with Forecasts from 2024 to 2034 (In Billions). 2023. Available online: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (accessed on 12 September 2025).
6. Check Point Research. Check Point Research Flags a Sharp Increase in Cyberattacks Targeting IoT Devices. Global Security Mag Online. April 2023. Available online: <https://www.globalsecuritymag.com/Check-Point-Research-flags-a-sharp-increase-in-cyberattacks-targeting-IoT.html> (accessed on 9 September 2024).
7. Williams, P.A.H.; McCauley, V. Always connected: The security challenges of the healthcare Internet of Things. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016. [CrossRef]
8. Islam, M.; Aktheruzzaman, K. An analysis of cybersecurity attacks against Internet of Things and security solutions. *J. Comput. Commun.* **2020**, *8*, 11–25. [CrossRef]
9. Arksey, H.; O'Malley, L. Scoping studies: Towards a methodological framework. *Int. J. Soc. Res. Methodol.* **2005**, *8*, 19–32. [CrossRef]
10. Moon, A.H.; Iqbal, U.; Bhat, G.M. Light weight authentication framework for WSN. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 3099–3105. [CrossRef]
11. Zeb, K.; Saleem, K.; Al Muhtadi, J.; Thuemmler, C. U-prove based security framework for mobile device authentication in eHealth networks. In Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Munich, Germany, 14–16 September 2016; pp. 1–6. [CrossRef]

12. Varshney, G.; Gupta, H. A security framework for IOT devices against wireless threats. In Proceedings of the 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, India, 10–11 August 2017; pp. 1–6. [\[CrossRef\]](#)
13. Hadar, N.; Siboni, S.; Elovici, Y. A lightweight vulnerability mitigation framework for IoT devices. In *IoTS&P '17: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 71–75. [\[CrossRef\]](#)
14. Sridhar, S.; Smys, S. Intelligent security framework for IoT devices: Cryptography based end-to-end security architecture. In Proceedings of the IEEE 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2017; pp. 1–5. [\[CrossRef\]](#)
15. Ansari, A.M.; Hussain, M. Middleware based node authentication framework for IoT networks. In Proceedings of the IEEE 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018; pp. 31–35. [\[CrossRef\]](#)
16. Hussain, M.; Al-Haiqi, A.; Zaidan, A.A.; Zaidan, B.B.; Kiah, M.; Iqbal, S.; Iqbal, S. Abdulnabi M: A security framework for mHealth apps on Android platform. *Comput. Secur.* **2018**, *75*, 191–217. [\[CrossRef\]](#)
17. Hsu, R.H.; Lee, J.; Quek, T.Q.S.; Chen, J.C. Reconfigurable security: Edge-computing-based framework for IoT. *IEEE Netw.* **2018**, *32*, 92–99. [\[CrossRef\]](#)
18. Pacheco, J.; Tunc, C.; Hariri, S. Security framework for IoT cloud services. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–6. [\[CrossRef\]](#)
19. Krishnan, K.N.; Jenu, R.; Joseph, T.; Silpa, M.L. Blockchain based security framework for IoT Implementations. In Proceedings of the 2018 International CET Conference on Control, Communication, and Computing (IC4), Thiruvananthapuram, India, 5–7 July 2018; pp. 425–429. [\[CrossRef\]](#)
20. Hakim, M.A.; Aksu, H.; Uluagac, A.S.; Akkaya, K. U-PoT: A honeypot framework for UPnP-based IoT devices. In Proceedings of the 2018 IEEE 37TH International Performance Computing and Communications Conference (IPCCC), Orlando, FL, USA, 17–19 November 2018; pp. 1–8. [\[CrossRef\]](#)
21. Nwafor, E.; Campbell, A.; Hill, D.; Bloom, G. Towards a provenance collection framework for Internet of Things devices. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; pp. 1–6. [\[CrossRef\]](#)
22. Setikere, S.; Sachidananda, V.; Elovici, Y. Out of kilter: Holistic exploitation of denial of service in internet of things. In *Security and Privacy in Communication Networks. SecureComm 2018*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Series; Springer: Cham, Switzerland, 2018; pp. 43–52. [\[CrossRef\]](#)
23. Rathore, S.; Park, J.H. Semi-supervised learning based distributed attack detection framework for IoT. *Appl. Soft Comput.* **2018**, *72*, 79–89. [\[CrossRef\]](#)
24. Ahuja, A.; Gandhi, H.; Shorey, R.; Kulkarni, D.; Tew, J. PlumeWalk: Towards threat provenance localization for IoT networks. In Proceedings of the 2019 11th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 7–11 January 2019; pp. 383–390. [\[CrossRef\]](#)
25. Ashtari, A.; Shabani, A.; Alizadeh, B. A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification. In Proceedings of the 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 28–29 August 2019; pp. 21–26. [\[CrossRef\]](#)
26. Ahmed, A.H.; Omar, N.M.; Ibrahim, H.M. Secured framework for IoT using blockchain. In Proceedings of the 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 8–10 December 2019; pp. 270–277. [\[CrossRef\]](#)
27. Sani, A.S.; Yuan, D.; Jin, J.; Gao, L.; Yu, S.; Dong, Z.Y. Cyber security framework for Internet of Things-based Energy Internet. *Future Gener. Comput. Syst.* **2019**, *93*, 849–859. [\[CrossRef\]](#)
28. Chattopadhyay, A.K.; Nag, A.; Ghosh, D.; Chanda, K. A secure framework for IoT-based healthcare system. In *Proceedings of International Ethical Hacking Conference 2018*; Advances in Intelligent Systems and Computing Series; Springer: Singapore, 2019; pp. 383–393. [\[CrossRef\]](#)
29. Albalawi, K.; Azim, M.M.A. Cloud-based IoT Device authentication scheme using blockchain. In Proceedings of the 2019 IEEE Global Conference on Internet of Things (GCIoT), Dubai, United Arab Emirates, 4–7 December 2019; pp. 1–7. [\[CrossRef\]](#)
30. Kavitha, S.; Alphonse, P.J.A.; Reddy, Y.V. An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system. *J. Med. Syst.* **2019**, *43*, 260. [\[CrossRef\]](#) [\[PubMed\]](#)
31. Kim, Y.; Nam, J.; Park, T.; Scott-Hayward, S.; Shin, S. SODA: A software-defined security framework for IoT environments. *Comput. Netw.* **2019**, *163*, 106889. [\[CrossRef\]](#)

32. Nobakht, M.; Russell, C.; Hu, W.; Seneviratne, A. IoT-NetSec: Policy-based IoT network security using OpenFlow. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 955–960. [\[CrossRef\]](#)
33. Myers, J.; Babun, L.; Yao, E.; Helble, S.; Allen, P. MAD-IoT: Memory anomaly detection for the internet of things. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [\[CrossRef\]](#)
34. Rashid, M.A.; Pajooh, H.H. A security framework for IoT authentication and authorization based on blockchain technology. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 264–271. [\[CrossRef\]](#)
35. Behrad, S.; Tuffin, S.; Bertin, E.; Crespi, N. Network access control for the IoT: A comparison between cellular, Wi-Fi and LoRaWAN. In Proceedings of the 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 19–21 February 2019; pp. 195–200. [\[CrossRef\]](#)
36. Chakraborty, S.; Aich, S.; Kim, H. A secure healthcare system design framework using blockchain technology. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 17–20 February 2019; pp. 260–264. [\[CrossRef\]](#)
37. Salman, O.; Elhajj, I.H.; Chehab, A.; Kayssi, A. A machine learning based framework for IoT device identification and abnormal traffic detection. *Trans. Emerg. Telecommun. Technol.* **2019**, *33*, e3743. [\[CrossRef\]](#)
38. Satamraju, K.P.; Malarkodi, B. Design and evaluation of a lightweight security framework for IoT applications. In Proceedings of the TENCON 2019—2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019; pp. 522–526. [\[CrossRef\]](#)
39. Han, W.; Xue, J.; Wang, Y.; Liu, Z.; Kong, Z. MalInsight: A systematic profiling based malware detection framework. *J. Netw. Comput. Appl.* **2019**, *125*, 236–250. [\[CrossRef\]](#)
40. Zarca, A.M.; Garcia-Carrillo, D.; Bernabe, J.B.; Ortiz, J.; Marin-Perez, R.; Skarmeta, A. Enabling virtual AAA management in SDN-based IoT networks. *Sensors* **2019**, *19*, 295. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Yadav, G.; Paul, K.; Allakany, A.; Okamura, K. IoT-PEN: A penetration testing framework for IoT. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; pp. 196–201. [\[CrossRef\]](#)
42. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Blockchain leveraged decentralized IoT eHealth framework. *Internet Things* **2020**, *9*, 100159. [\[CrossRef\]](#)
43. Murthy, S.; Kavitha, C.R. A smart and secure framework for IoT device based multimedia medical data. In *Computational Vision and Bio-Inspired Computing. ICCVBIC 2019; Advances in Intelligent Systems and Computing Series*; Springer: Cham, Switzerland, 2020; pp. 583–588. [\[CrossRef\]](#)
44. Xu, L.; Chen, L.; Gao, Z.; Fan, X.; Suh, T.; Shi, W. DIoTA: Decentralized-ledger-based framework for data authenticity protection in IoT systems. *IEEE Netw.* **2020**, *34*, 38–46. [\[CrossRef\]](#)
45. Al-Hadhrani, Y.; Hussain, F.K. Real time dataset generation framework for intrusion detection systems in IoT. *Future Gener. Comput. Syst.* **2020**, *108*, 414–423. [\[CrossRef\]](#)
46. Baig, Z.A.; Sanguanpong, S.; Firdous, S.N.; Vo, V.N.; Nguyen, T.G.; So-In, C. Averaged dependence estimators for DoS attack detection in IoT networks. *Future Gener. Comput. Syst.* **2020**, *102*, 198–209. [\[CrossRef\]](#)
47. Ikharo, B.; Obiagwu, A.; Obasi, C.; Hussein, S.U.; Akah, P. Security for Internet-of-Things enabled e-health using blockchain and artificial Intelligence. In Proceedings of the 2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS), Abuja, Nigeria, 15–16 July 2021; pp. 1–4. [\[CrossRef\]](#)
48. Tsogbaatar, E.; Bhuyan, M.H.; Taenaka, Y.; Fall, D.; Gonchigsumlaa, K.; Elmroth, E.; Kadobayashi, Y. DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT. *Internet Things* **2021**, *14*, 100391. [\[CrossRef\]](#)
49. Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A framework for malicious traffic detection in IoT healthcare environment. *Sensors* **2021**, *21*, 3025. [\[CrossRef\]](#) [\[PubMed\]](#)
50. Zhou, Y.; Cheng, G.; Yu, S. An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 5366–5380. [\[CrossRef\]](#)
51. Aslam, M.; Ye, D.; Tariq, A.; Asad, M.; Hanif, M.; Ndzi, D.; Chelloug, S.A.; Elaziz, M.A.; Al-Qaness, M.A.A.; Jilani, S.F. Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. *Sensors* **2022**, *22*, 2697. [\[CrossRef\]](#) [\[PubMed\]](#)
52. Chen, X.; Xiao, L.; Feng, W.; Ge, N.; Wang, X. DDOS defense for IoT: A Stackelberg game model-enabled collaborative framework. *IEEE Internet Things J.* **2022**, *9*, 9659–9674. [\[CrossRef\]](#)
53. Galadima, H.; Seeam, A.; Ramsurrun, V. Cyber deception against DDoS attack using moving target defence framework in SDN IOTEDGE networks. In Proceedings of the IEEE 3rd International Conference on Next Generation Computing Applications (NextComp), Flic-en-Flac, Mauritius, 6–8 October 2022; pp. 1–6. [\[CrossRef\]](#)

54. Shrivastava, K.; Singh, S.; Chaudhary, P.; Singh, R.; Saraswat, B.K. Garg A: An improved blockchain based security framework for IoT enabled wireless network. In Proceedings of the 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, 9–11 May 2024; pp. 913–918. [\[CrossRef\]](#)
55. Garah, A.; Mbarek, N.; Kirgizov, S. Enhancing IoT data confidentiality and energy efficiency through decision tree-based selfmanagement. *Internet Things* **2024**, *26*, 101219. [\[CrossRef\]](#)
56. Sunanda, N.; Shailaja, K.; Kandukuri, P.; Krishnamoorthy; Rao, V.S.; Godla, S.R. Enhancing IoT network security: ML and blockchain for intrusion detection. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 947–958. [\[CrossRef\]](#)
57. Tyagi, A.; Singh, A.; Yadav, A.; Mehra, P.S. A survey on artificial intelligence-based cyber security in IoT networks. In Proceedings of the 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 15–16 March 2024; pp. 238–243. [\[CrossRef\]](#)
58. Osman, M.; He, J.; Zhu, N.; Mokbal, F.M.M. An ensemble learning framework for the detection of RPL attacks in IoT networks based on the genetic feature selection approach. *Ad Hoc Netw.* **2024**, *152*, 103331. [\[CrossRef\]](#)
59. Thakur, P.; Goel, S.; Puthooran, E. Edge AI enabled IoT framework for secure smart home infrastructure. *Procedia Comput. Sci.* **2024**, *235*, 3369–3378. [\[CrossRef\]](#)
60. Omar, T.; Ho, A.; Urbina, B. Detection of DDoS in SDN environment using entropy-based detection. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019; pp. 1–4. [\[CrossRef\]](#)
61. Gao, S.; Li, Z.; Xiao, B.; Wei, G. Security threats in the data plane of software-defined networks. *IEEE Netw.* **2018**, *32*, 108–113. [\[CrossRef\]](#)
62. Ja’fari, F.; Mostafavi, S.; Mizanian, K.; Jafari, E. An intelligent botnet blocking approach in software defined networks using honeypots. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 2993–3016. [\[CrossRef\]](#)
63. Ge, M.; Cho, J.H.; Ishfaq, B.; Kim, D. *Modeling and Analysis of Integrated Proactive Defense Mechanisms for Internet of Things*; Kamhoua, C.A., Njilla, L.L., Kott, A., Shetty, S., Eds.; Wiley Online Library: Hoboken, NJ, USA, 2020. [\[CrossRef\]](#)
64. da Rocha, B.C.; de Melo, L.P.; de Sousa, R.T. Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model. In Proceedings of the 2021 Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, 18–19 November 2021; pp. 1–6. [\[CrossRef\]](#)
65. Xiao, K.; Zhang, Y.; He, Y.; Xu, G.; Wang, C. Industrial IoT network security situation prediction based on improved SSA-BiLSTM. In *Wireless Sensor Networks. CWSN 2022*; Communications in Computer and Information Science Series; Springer: Singapore, 2022; Volume 1715, pp. 212–224. [\[CrossRef\]](#)
66. Yang, H.; Zhang, L.; Zhang, X.; Zhang, J. An adaptive IoT network security situation prediction model. *Mob. Netw. Appl.* **2022**, *27*, 371–381. [\[CrossRef\]](#)
67. Kumar, D.; Pawar, P.P.; Addula, S.R.; Meesala, M.K.; Oni, O.; Cheema, Q.N.; Haq, A.U.; Sajja, G.S. AI-Powered Security for IoT Ecosystems: A Hybrid Deep Learning Approach to Anomaly Detection. *J. Cybersecur. Priv.* **2025**, *5*, 90. [\[CrossRef\]](#)
68. Tricco, A.C.; Lillie, E.; Zarin, W.; O’Brien, K.K.; Colquhoun, H.; Levac, D.; Moher, D.; Peters, M.D.; Horsley, T.; Weeks, L.; et al. PRISMA Extension for Scoping Reviews (PRISMA ScR): Checklist and Explanation. *Ann. Intern. Med.* **2018**, *169*, 467–473. [\[CrossRef\]](#) [\[PubMed\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.