Review

Security in the Internet of Things: Identifying and Analysing Critical Categories

Hannelore Sebestyen * , Daniela Elena Popescu * , Rodica Doina Zmaranda

Posted Date: 30 December 2024

doi: 10.20944/preprints202412.2512.v1

Keywords: IoT security; attack detection; emergent technologies in IoT; IoT vulnerabilities; adaptive security solutions

Review

Security in the Internet of Things: Identifying and Analysing Critical Categories

Hannelore Sebestyen [1], Daniela Elena Popescu [2] and Rodica Doina Zmaranda [3]

[1] Faculty of Automation and Informatics, Politehnica University Timișoara; verman.hanne@gmail.com
[2] Computers and Information Technology Department, University of Oradea; depopescu@uoradea.ro
[3] Computers and Information Technology Department, University of Oradea; dzmaranda@uoradea.ro
* Correspondence: verkman.hanne@gmail.com (H.S.); depopescu@uoradea.ro D.E.P.

Abstract: With the proliferation of IoT-based applications, security requirements are becoming increasingly stringent. Given the diversity of such systems, choosing the most appropriate solutions and technologies according to the challenges is a complex activity. This paper provides an exhaustive evaluation of existing security challenges related to the IoT domain. This review explores the evolving landscape of IoT security, identifying key focus areas, challenges, and proposed solutions as presented in recent research. The study categorizes IoT security efforts into six main areas: attack detection, data management and protection, securing identity management, communication and networking, emergent technologies, and risk management. Each category reflects the critical vulnerabilities and growing complexities of IoT systems. From leveraging machine learning and blockchain for anomaly detection and real-time threat response to optimizing lightweight algorithms for resource-limited devices, researchers propose innovative and adaptive solutions to meet emerging threats. The review underscores the integration of advanced technologies to enhance IoT system security, while also highlighting ongoing challenges. The paper concludes with a synthesis of security challenges and threats of each identified category together with their solutions, aiming to support decision-making during the designing approach of IoT-based applications and to guide future research toward comprehensive and efficient IoT frameworks.

Keywords: IoT security; attack detection; emergent technologies in IoT; IoT vulnerabilities; adaptive security solutions

1. Introduction

1.1. IoT Evolution Overview

The Internet of Things represents one of the most transformative technological advancements of the modern era. By enabling physical objects to connect to the internet, exchange data, and interact autonomously, IoT has dramatically reshaped how we live, work, and communicate. The exponential growth of interconnected devices, ranging from everyday household appliances to sophisticated industrial machines, has created a highly integrated ecosystem that offers unparalleled convenience, efficiency, and potential for innovation [1]. However, this interconnectedness, while opening new avenues for progress, also introduces a series of complex security challenges that cannot be ignored.

According to the IoT Analytics platform, in 2024, the number of IoT connected devices is expected to increase by 13% year-on-year to 18.8 billion, 8.5 billion more than in 2019 [2]. This number is expected to double by 2030, growing to over 40 billion devices.

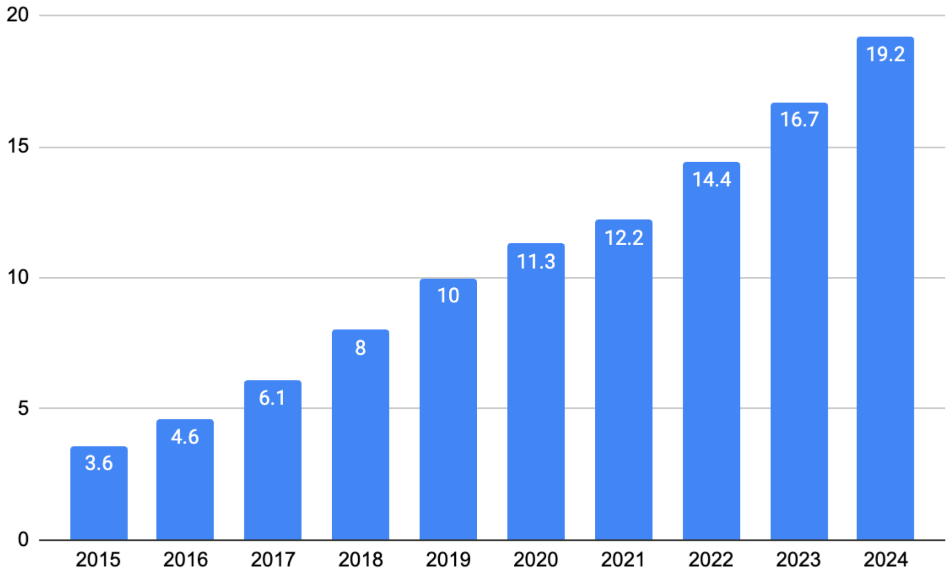


Figure 1. Estimated IoT connected devices (in billions) in the past 10 years [2].

At its essence, the Internet of Things encompasses a vast network of physical objects that are embedded with sensors, software, and various technologies, allowing them to communicate with each other and with centralised systems via the internet. This communication enables real-time data collection and analysis, which powers intelligent automation across a variety of sectors including healthcare, transportation, agriculture, energy management, and urban planning. In smart cities, for instance, IoT technologies are used to optimise traffic flow, reduce energy consumption, enhance public safety, and even manage waste efficiently.

While these capabilities offer a tremendous opportunity to improve efficiency and convenience, they also come with a critical vulnerability: the security of these devices. The very features that make IoT devices appealing—such as the ability to collect and transmit sensitive data—also make them prime targets for cyber threats. Each additional device connected to the internet expands the digital attack surface, creating more potential entry points for malicious actors. A compromised device can serve as an entry gateway for attackers, enabling them to infiltrate entire networks, steal sensitive data, or disrupt critical infrastructure.

The urgency of securing the Internet of Things has never been more pressing. As the number of connected devices continues to rise, so too do the threats and vulnerabilities that they introduce. In the context of IoT, cybersecurity is not just about protecting devices from unauthorised access; it involves safeguarding entire ecosystems of interconnected systems from a range of cyber threats. The risks associated with inadequate security are far-reaching—personal data may be exposed, critical infrastructure can be compromised, and public trust in these technologies may diminish. Several high-profile incidents, such as attacks on unsecured smart home devices, have already underscored the potential consequences of IoT vulnerabilities, raising alarms in both the public and private sectors.

Emerging technologies play a critical role in enhancing security measures against the evolving landscape of cyber threats in IoT environments. By integrating solutions like artificial intelligence, blockchain, machine learning and other innovative technologies, organisations can build more robust defences against sophisticated attacks. For example, AI-powered anomaly detection systems can help identify unusual patterns of behaviour within IoT networks, enabling faster detection of potential breaches. Blockchain, with its decentralised and immutable ledger, offers a way to secure data exchanges between devices and ensure the integrity of communications. Public key Infrastructure systems can provide stronger authentication mechanisms for IoT devices, reducing the likelihood of unauthorised access. As these technologies continue to develop, they will play an essential role in addressing the unique security challenges posed by the interconnected nature of IoT.

doi:10.20944/preprints202412.2512.v1

IoT-related attacks are becoming increasingly sophisticated, with hackers targeting devices with weak or insufficient security measures to gain access to larger networks. Issues such as poor device encryption, lack of proper authentication mechanisms, and outdated software contribute to the growing number of cyber incidents in the IoT landscape. As a result, addressing these vulnerabilities requires a multi-layered and proactive approach to security that encompasses not just technical solutions but also policy frameworks and industry standards.

1.2. Regulatory Overview

Aware of the increasing risks, authorities have developed stricter security standards for IoT devices. In the EU, these standards are embodied in the 2016 General Data Protection Regulation [3] issued by the European Parliament, as a result of technological development and globalisation. The United States issued The IoT Cybersecurity Improvement Act of 2020 in 2020 calling for the National Institute of Standards and Technology and the Office of Management and Budget to develop standards that establish minimum requirements and guidelines for the use and management of IoT devices owned by agencies, i.e., the proper management of information held by them [4]. NIST will need to conduct a review every 5 years of the guidelines and update them as needed.

Over the years there have been groups and organisations that, noticing the need for increased cybersecurity have developed frameworks and standards for different domains. Thus, in 2017 the IoT Cybersecurity Alliance was formed consisting of the firms AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic with the objective of solving the main cybersecurity challenges in the IoT ecosystem using the expertise of the firms involved [5]. Another such grouping is the Industry IoT Consortium, which is active in the industry domain. They developed the first version of the Industry Internet of Things Security Framework in 2016 with the aim of securing ICS/SCADA systems [6]. It provides proposals for architectures that can be used and a set of best practices.

The Internet Engineering Task Force is developing standards for providing secure communication protocols. One such protocol is CoAP - RFC 7252 Constrained Application Protocol developed for resource-constrained networks within the IoT ecosystem. It uses DTLS to secure data exchange [7].

The Organization for Standardization published ISO/IEC 30141, republished in 2024 helps in the design of IoT ecosystems by providing best practices for authentication, data security and network integrity [8]. Other standards related to cybersecurity in the IoT ecosystem are those representing the NIST 8259 series developed by the NIST and EN 303 645 developed by the European Telecommunications Standards Institute.

Despite the existence of these standards, guidelines and frameworks, IoT vulnerabilities are continuously present and the spread of IoT increases the need for solutions.

In this context, the present work carries out a systematic review of main challenges associated with IoT systems, the main contributions being the following:

- Identifying the critical security weaknesses that have been commonly addressed in IoT research;
- Examine the specific difficulties involved in securing IoT devices;
- Review and evaluate solutions aimed at mitigating IoT-related security risks;
- Identifying key trends, best practices, and the usage of emergent technologies such as Artificial Intelligence, Blockchain, Machine Learning and Edge Computing that are shaping the future of IoT security;
- Highlighting the need for robust and comprehensive security strategies to protect sensitive data and to ensure public confidence in IoT technologies.

This review aims to provide researchers and practitioners with a clear synthesis of challenges and solutions, offering a foundational guide for designing resilient and secure IoT systems.

1.3. IoT Architectural Overview

The IoT infrastructure relies on a multitude of interconnected components distributed across various levels of the system, collectively forming its architecture [9]. While there is no universally standardized architecture for IoT systems, the three-layer architecture—comprising the application, network, and perception layers—is the most referenced in the reviewed studies (Figure 2).

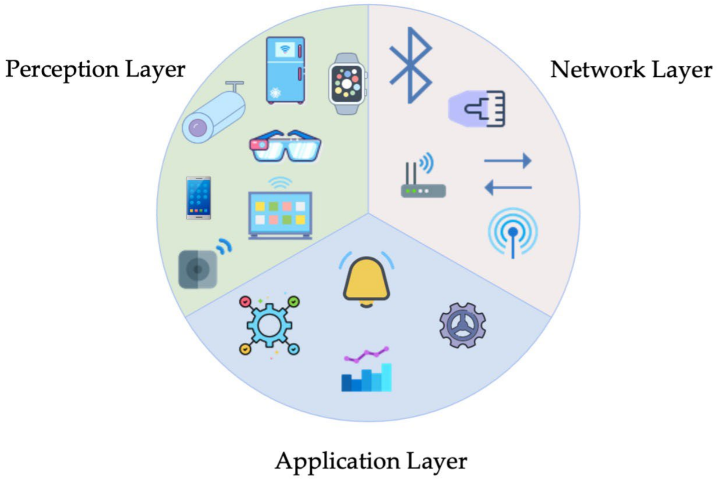


Figure 2. Three layered IoT system architecture [10].

Each of these layers performs distinct functions, enabled by specific tools and technologies. The Perception Layer operates directly with the physical world, gathering data from its environment and taking necessary actions. Devices at this level are designed for sensing, data collection, and direct interaction with the external environment when required [11]. Examples of devices in this category include sensors, actuators, and other resource-constrained devices [9].

The Network Layer ensures data transfer between the Perception Layer and the Application Layer. This layer encompasses gateway devices responsible for aggregating, storing, and directing data to cloud platforms. These devices facilitate communication with resource-constrained devices using low-power protocols while also interfacing with cloud servers via robust communication protocols [9]. Depending on the connected devices, coverage area, and data volume, various types of wireless networks can be employed to establish these connections [12]:

- Cellular connections utilizing LPWAN, such as LTE-M and NB-IoT standards, as well as unlicensed solutions like LoRa and Sigfox;
- Local and personal area networks, including Wi-Fi and Bluetooth;
- Mesh protocols, with Zigbee and RFID being the most common.

The Application Layer delivers services to end-users via mobile and web applications. A common example is cloud platforms, which process collected data and present it to users through dashboards or control functions.

2. Research Methodology and Paper Structure

The articles underlying this review are open access, allowing interested parties to analyse them and with their help to find the best solutions for IoT security.

2.1. Selection of Article Sources

Most of the articles were found on MDPI, which aims to encourage scientific exchange and has an extensive database of articles dealing with topical issues. It is continuously being enriched with scientific papers on various topics. It offers the possibility to search for articles based on keywords but also based on topics to which several papers are assigned. Other sources considered for finding articles on the topic of this paper were:

- IEEE Xplore, a comprehensive digital library providing access to a wide range of technical literature in engineering, computer science, and related fields;

- Cornell University Arxiv, an open-access repository of preprints spanning multiple disciplines, including computer science and cybersecurity;
- Informatics in Education, which provides access to educational and research-focused papers in informatics;
- Elsevier provides a wide range of services, including access to a vast collection of academic journals, books, and research databases;
- Springer, a platform that provides access to scholarly articles and books on a variety of topics, including advanced technologies and IoT security;
- Nature provides access to cutting-edge, peer-reviewed research, offering high-impact studies that often set benchmarks in their respective field.

These sources collectively ensure comprehensive coverage of the topic, allowing for a diverse range of perspectives and insights to be included in the review.

2.2. Search Method

In the MDPI, the search bar was used to locate articles by title and keywords. The keywords employed included "IoT security," "IoT systems," "IoT communication," "IoT vulnerabilities", "IoT security risk management" and "6G network IoT". This keyword-based search returned hundreds of articles that, to varying degrees, address the topic of security within the IoT ecosystem. To narrow down the results to the most relevant and up-to-date studies, a publication date filter was applied, restricting the selection to articles published between 2023 - 2024. Additionally, a subject-area filter was used, focusing on Engineering, Computer Science & Mathematics.

This approach ensured the inclusion of recent, high-quality studies that align with the technical focus of this review while eliminating outdated or less relevant content.

When an article was identified as part of a specific issue, the entire issue was examined to uncover additional articles connected to the original topic. This approach aimed to deepen the exploration and identify alternative or complementary solutions. The categories of the selected articles from these issues are as follows:

- Machine Learning for Cybersecurity: Threat Detection and Mitigation;
- Network Security in Artificial Intelligence Systems;
- Data Security Approaches for Autonomous Systems, IoT, and Smart Sensing Systems;
- Advanced 5G and beyond Networks;
- Key Enabling Technologies for Beyond 5G Network;
- Advances in Internet of Things Technologies and Cybersecurity.

In the other sources only the search bar was used with the above-mentioned keywords completed with "Generative AI" and "Digital Identity".

2.3. Articles Selection Method

In the identification stage of selection, articles were identified through a comprehensive search across above mentioned sources using predefined keywords related to IoT security. The search included peer-reviewed journals, conference proceedings, and other credible sources. Duplicate records were removed at this stage to streamline the dataset.

During the screening process titles and abstracts of the articles were screened to ensure relevance to the topic of interest. Articles that were clearly off-topic, such as those addressing unrelated domains, were excluded.

To ensure flawless data management, information about the articles that progressed to the screening stage was recorded in a Google Sheet, allowing all authors to access it. The data extracted for each article included the title, keywords, abstract, conclusions, challenges, and proposed solutions. For reference management, the Zotero application was used.

A detailed review of introductory sections, tables, diagrams, and conclusions was conducted to further assess the articles. Articles were excluded if:

- The primary focus diverged from IoT security;

doi:10.20944/preprints202412.2512.v1

- They were editorials, opinion pieces, or predominantly literature reviews without new solutions or insights;
- They lacked a clearly defined or described solution, framework, or implementation related to IoT security.

Articles that passed the screening were assessed for inclusion. Each article was evaluated based on its methodology, the relevance of its findings to IoT security, and the rigor of its contribution. Articles with inadequate methodological detail or insufficient evidence to support claims were excluded.

The final dataset comprised articles meeting all inclusion criteria, which focused on addressing IoT-specific security challenges and presented original and clearly defined solutions. These articles were subjected to detailed qualitative and quantitative analysis in subsequent stages of the review.

In the Prisma Flow below (Figure 3), the paper selection procedure can be seen.

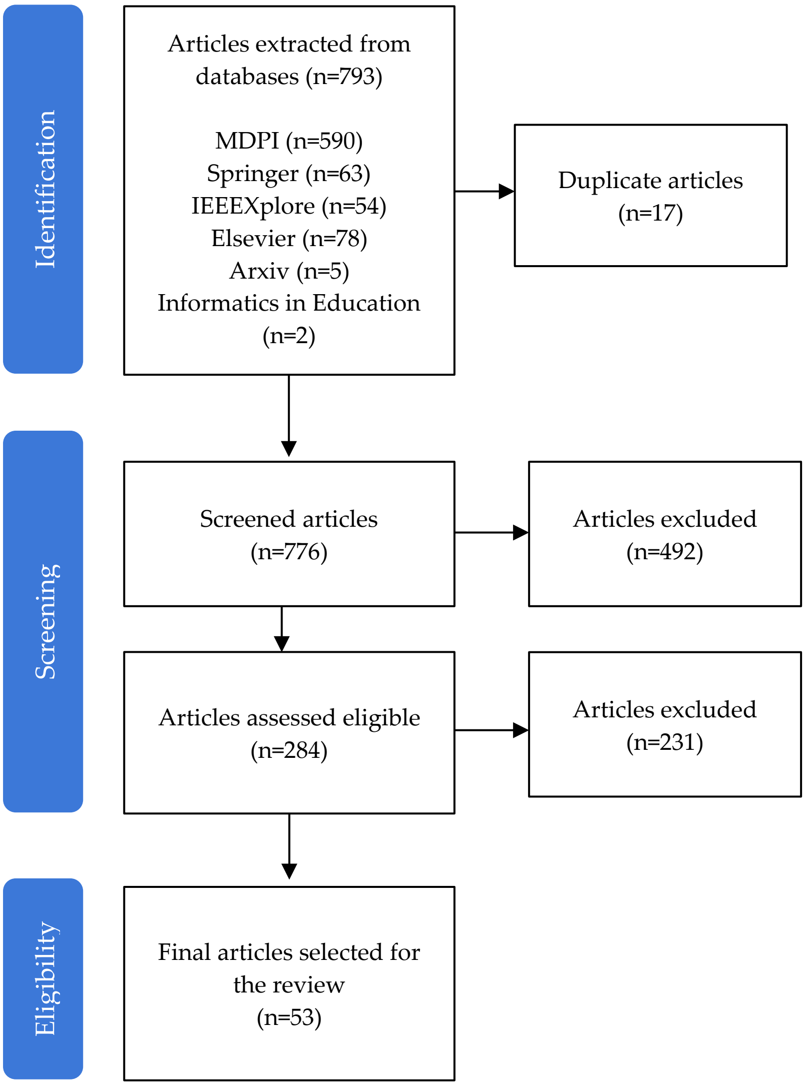

Identification
Articles extracted from databases (n=793)
MDPI (n=590)
Springer (n=63)
IEEEXplore (n=54)
Elsevier (n=78)
Arxiv (n=5)
Informatics in Education (n=2)
Duplicate articles (n=17)
Screening
Screened articles (n=776)
Articles excluded (n=492)
Articles assessed eligible (n=284)
Articles excluded (n=231)
Eligibility
Final articles selected for the review (n=53)

Figure 3. Prisma Flow - the selection procedure.

After selecting the papers, the next step involved grouping them, initially based on specific keywords and the targeted issues addressed by each. In the second phase, preliminary categories were outlined to facilitate the study of vulnerabilities. During a subsequent iteration, some categories were reformulated, and certain articles were reallocated to more appropriate groups. Additionally, several works were found to span multiple identified categories; these were included in all relevant categories to ensure comprehensive coverage.

This structured and iterative approach aimed to refine the categorization process, ensuring that the grouping of articles accurately reflected the diversity and complexity of the vulnerabilities examined in the literature.

In Figure 4, the distribution of articles by their source can be observed.

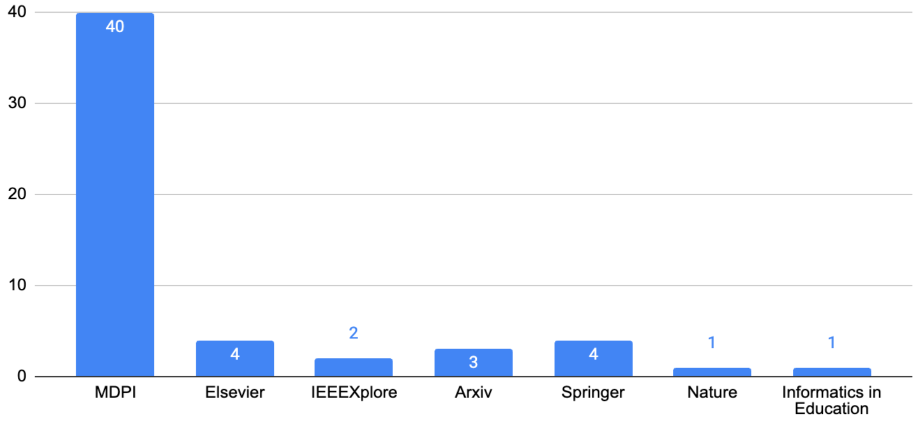


Figure 4. Number of articles by sources.

While figure 4 highlights the distribution of IoT security articles based on their sources, it is equally important to examine how these publications are distributed across academic journals. Considering the substantial number of articles retrieved from the MDPI database, it was found necessary to include a chart illustrating the distribution of these articles across the various journals in which they were published. This perspective provides deeper insight into the scholarly focus and key contributors to the field of IoT security research. Figure 5 illustrates the breakdown of articles by journal, shedding light on which publications are at the forefront of disseminating knowledge in this rapidly evolving domain.

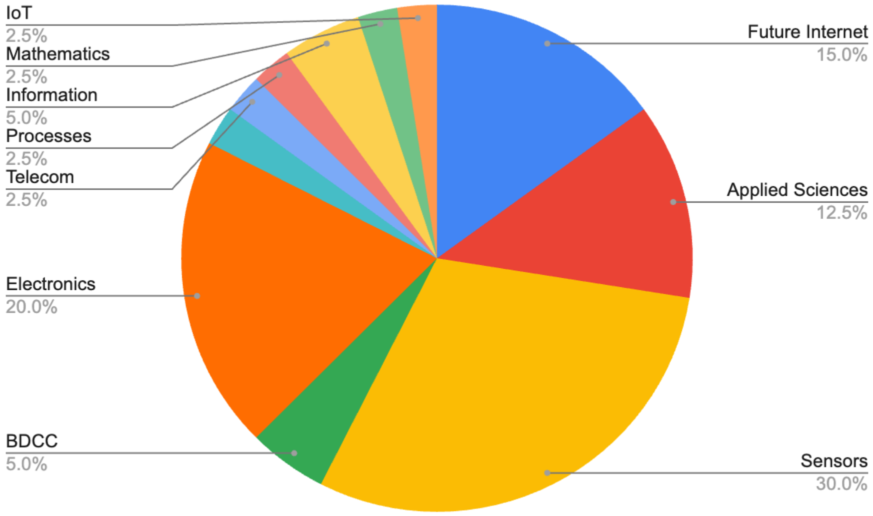


Figure 5. Articles from MDPI by journals.

Following part of this paper is organized into four main sections. The first section identifies and categorizes the principal types of vulnerabilities discussed in the analysed literature, offering a comprehensive overview of IoT attack vectors. The second section explores the challenges associated with these vulnerabilities, examining proposed solutions such as frameworks, methodologies, and mechanisms for attack detection and prevention. Additionally, this section addresses strategies designed to secure sensitive user data and protect privacy, reflecting the increasing importance of safeguarding information in IoT ecosystems.

The discussion section highlights key areas of active research and identifies unresolved challenges that warrant future exploration. Finally, the conclusion synthesizes the key insights derived from this review and proposes potential future research directions for each identified category.

3. Categories Identification and Analyses

By analyzing the current state of the art from the articles subject to this review, table 1 realizes a classification of them, according to the methodology, in the field of IoT systems. For each category, a subclassification of the targeted issues of related articles was identified.

Table 1. Category identification and targeted issues.

Categories	Related Challenges	Targeted Issues	References

Attack detection	Increasing number of cyber-attacks on IoT devices, difficulty in detecting attacks in real time.	Intrusion and anomaly detection;
		DDoS attacks;
		Eavesdropping attacks;
		Concept drift detection and adaptation;
		Botnet detection;
		Cyberattacks
			[10,13–27]

Data management & protection	Vulnerabilities in the storage and transfer of sensitive data, privacy risks.	Data security;
		Data privacy;
		Digital Identity & Identity-based encryption;
		Generative AI
			[28–36]

Securing identity management	Authentication of users and devices, management of unauthorised access.	Device identification;
		Authorization;
			[26, 30, 32-34, 37-48]

Communication & Networking	Security of communications between IoT devices, risks associated with open networks.	Network security;
		Firmware;
		5G & 6G networks
			[15, 26, 49-55]

Emergent technologies	Integrating emerging technologies (e.g. AI, blockchain) into IoT security solutions.	Machine learning;
		Blockchain;
		Artificial intelligence;
		Edge Computing;
		Fog Computing
			[10, 15-18, 22-26, 28-37, 43, 51, 53, 55-60]

Risk management	Identify, address and mitigate potential risks associated with security and privacy in IoT.	Risk management frameworks	[61–64]

3.1. Attack Detection

With the spread of IoT devices, cyber-attacks favored by the poor security of these devices have also increased [13]. The attacks can address different levels of the system such as sensor, network, support or application. These attacks are intended to cause damage to the system or to gain unauthorized access to the system or its data [14, 19]. The larger the area the system encompasses, the more damage these attacks can generate. Also, the rapid spread of the 5G network thanks to the expansion of IoT systems and the increase in data volume has enabled the development of innovative applications, but at the same time has also led to an increase in network level attacks [15, 22]. In order to prevent these attacks, network level intrusion detection systems have been developed that are capable of detecting anomalies in data transmission between devices [23, 24]. IoT networks differ from traditional ones thus it is necessary to develop advanced intrusion detection systems, in most studies the use of ML is recommended, which however poses new challenges [19, 26]. First of all the models need to be trained, the lack of the necessary amount of data and the disadvantage of the long training duration intervene here [25]. Secondly there is the problem of the adaptability of the models to new conditions materialized by new attack methods [18], detection and adaptability to concept drift.

One specific type of cyberattack explored in the selected articles is those initiated by botnet armies. These botnets exploit the vulnerabilities of smart devices connected to IoT systems, which users often neglect to secure properly [14]. Unlike traditional Internet-connected devices such as computers or smartphones, which typically benefit from robust security measures, smart home appliances are frequently overlooked, despite their internet connectivity and inherent risk exposure.

Although botnet detection solutions exist outside of IoT ecosystems, their effectiveness significantly diminishes within IoT environments [14, 16]. Among the attacks facilitated or intensified by these botnets, Distributed Denial of Service attacks stand out as a prominent threat. Figure 6 shows a typical DDoS attack components using botnets, managed by a botmaster.

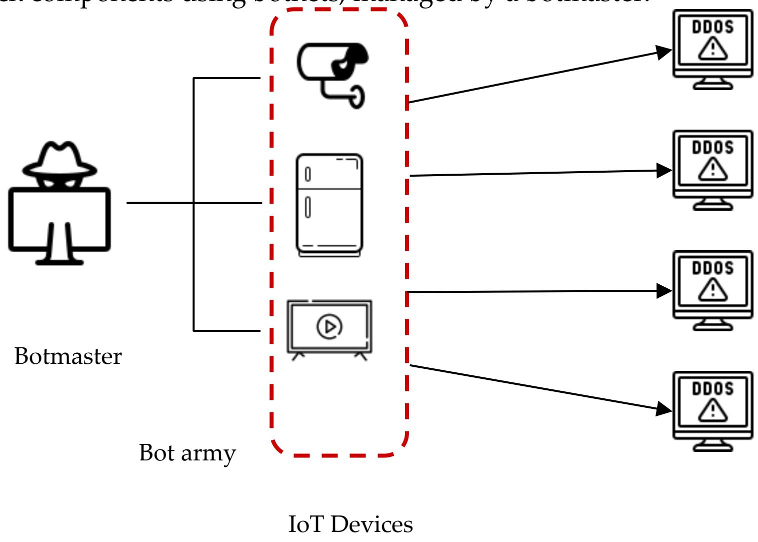


Figure 6. DDoS Attack by Botnets.

3.2. Data Management and Protection

This category includes studies on the management and protection of data in IoT systems, highlighting the vulnerabilities that can arise in data storage and transfer. This is a critical topic given the huge amount of data collected, stored, processed and transmitted within the system. It also changes the way data is accessed. Before, users received data from a specialised service. In IoT, users can communicate directly with sensors. They can obtain data directly, but they can also transmit instructions to devices [28]. In this context, there is an increasing need to ensure a seamless data flow, while at the same time ensuring data privacy through secure, efficient and scalable identity management [28].

Deployment of IoT systems in domains such as medical, automotive, industry, but also in the financial sector, where critical decisions are made based on the data provided by the system, the problem of ensuring trust management, data confidentiality and integrity arises [29].The application of Blockchain technology [29-31] is becoming a method of interest due to the security features it can bring by incorporating it into IoT systems, but there is the issue of scalability and interoperability.

Due to the Internet connectivity of IoT devices that have access to personal data, problems related to the digital identity of users arise, such as unauthorised access to data or identity forgery

[32-34]. There is thus a need to develop advanced identity systems capable of reducing unauthorised access.

There is a trend to use Generative AI within the IoT ecosystem in order to make it more efficient, but this integration leads to new vulnerabilities and risks [35]. Due to the large volume of data handled by Generative AI technology, poor system protection can lead to data privacy breaches and damage data integrity. Also, the generation process itself may contain risks of information leakage [36].

3.3. Securing Identity Management

Identity security management is a critical component of data protection in IoT environments, primarily focusing on authenticating entities involved in data transfer and granting them the necessary authorization [39]. This process is essential to restrict access to sensitive information exclusively to authorized users and devices, thereby mitigating risks of unauthorized access and security breaches [40,41]

Device identification involves recognizing and categorizing devices connected to the network by analyzing their distinctive attributes derived from data traffic [25]. Traditional methods for device identification face challenges in terms of adaptability to newly connected devices and are prone to errors. Emerging solutions leverage blockchain technology, but these approaches present limitations, including the potential exposure of sensitive metadata, which could compromise user privacy [30] and the challenge of achieving scalability while maintaining data security [38]. Relying on centralized servers for authentication introduces vulnerabilities such as a single point of failure [37].

Traditional user authentication methods, such as credentials, certificates, and 2FA, can pose challenges in an IoT system due to the limited resources and capabilities of the devices [47,48]. Furthermore, vulnerabilities arising from poor identity management can be exploited in this context, given the specific characteristics of devices connected to the system.

Studies [42–45] highlight the importance of secure communication and controlled access to stored data. Currently, these processes are often managed through PKI [45,46]. While PKI has been an effective standard for securing communication in traditional systems, emerging challenges in the context of large-scale IoT suggest that it may struggle to meet increasingly complex requirements. Moreover, there is no well-defined protocol for efficiently transferring trust or updating PKI credentials when the responsibility for device maintenance transitions from one service provider to another [45,46].

Key issues include the high costs associated with implementing and maintaining a PKI system, as well as its substantial resource requirements, which can pose significant obstacles for organizations aiming to deploy large-scale IoT solutions [45,46]. Another notable concern is the risk of a single point of failure, where the entire responsibility for access authorization relies on the PKI infrastructure [42–44]. This means that if the PKI infrastructure is compromised or becomes inoperative, the entire security framework of the IoT network could be severely impacted.

The adoption of digital identities introduces additional challenges. For instance, study [32] draws attention to issues in the medical field related to identity management. Digital identities have proven insufficient for accurately identifying patients, with a lack of system integration and limited scalability further complicating the situation. Study [33] examines the limitations of blockchain-based digital identities in terms of authenticity and controllability while also addressing privacy requirements. Challenges also arise in establishing a trusted network and coordinating digital identity management [34].

3.4. Communication and Networking

In order to develop a massive IoT ecosystem, it is essential to ensure secure communication and scalable networks that meet security and performance requirements [25] in the context of a large number of devices with limited resources [53–55]. The creation of such networks requires the implementation of specific protocols, each tailored to the scope of the IoT system in question. These protocols are fundamental to guarantee the integrity, confidentiality and availability of data transmitted between devices. They impose security measures that are essential to cope with cyber-attacks, such as DDoS attacks, communication eavesdropping or man-in-the-middle attacks [49].

Firmware plays a crucial role in the communication within an IoT ecosystem, as it directly affects how devices connect, communicate, and interact with the system. Consequently, network-level security must be analysed with consideration of potential firmware vulnerabilities. Paper [50] highlights this aspect by reviewing studies that focus on addressing these vulnerabilities.

As previously mentioned, the introduction of 5G networks has brought a series of vulnerabilities, partly due to its specific features and partly because of device limitations [15]. Its potential successor, the 6G network, is continuously undergoing tests and studies. The integration of AI technology with 6G in IoT systems offers significant opportunities but also introduces new challenges, particularly with the anticipated increase in the number of connected devices and the volume of data transmitted [51]. This growth necessitates optimising energy consumption and resource allocation to meet performance requirements [52].

3.5. Emergent Technologies

The integration of AI and Machine Learning into IoT systems significantly enhances cognitive capabilities [29,30,35,36,51] and offers a promising approach for detecting and mitigating cyber-attacks in IoT environments [15]. The reviewed articles include studies focused on ML algorithm [15, 19, 25, 27, 56-58] others exploring Deep Learning through the use of neural networks [22,24], and some examining ML training techniques such as transfer learning, federated learning, and split learning [24, 43, 59, 60]. However, implementing these technologies introduces new challenges due to the nature of connected devices, the substantial resource demands required for their deployment, and the time-intensive process of model training. Additionally, adapting these models to real-time conditions remains a significant difficulty.

There is also a significant number of studies of blockchain technology in IoT systems. It, due to its characteristics of data immutability, decentralisation and transparency [28, 29, 31 - 34, 37, 43, 44, 56] has become a point of interest in order to secure the IoT system. Blockchain technology provides a decentralised network, it eliminates the single point of control, thus attacks on the system become much more difficult [30]. Challenges in blockchain arise due to the heterogeneity of devices using different communication protocols and relying on other technologies and requiring connection to blockchain. Response delays introduced by transaction confirmation in blockchain can be a negative aspect.

To address the need for processing large volumes of data from diverse devices, Edge Computing has emerged as a solution to enhance computational performance in IoT systems [17, 18, 21, 53, 55]. This approach involves positioning computational resources closer to the data source at the network's edge [51]. Additionally, Edge Computing can be integrated with Fog Computing to facilitate IoT interoperability with Cloud technology [17]. However, incorporating these technologies into IoT systems introduces new security challenges, particularly when compromised devices launch attacks targeting fog layer services.

3.6. Risk Management

Risk management in IoT systems plays a critical role in assessing and addressing cyber risks that could impact the system. Several types of risks can be identified, including those related to IoT ethics, data security and privacy risks, and technical risks [61]. The complexity of IoT systems poses significant challenges in analysing and identifying these risks [63]. Human involvement, the diversity of IoT application domains, and IoT-specific cybersecurity challenges add further difficulties to the risk management process [62]. Additional challenges include the lack of robust management strategies, the absence of standardised IoT security measures, and a reactive approach to developing strategies in response to attacks rather than adopting a proactive stance [64].

4. Identified Challenges and Solutions

4.1. Attack Detection

An essential step in securing the IoT ecosystem lies in the detection of attacks. IoT network security specialists are focused on developing the most effective methods for detecting and preventing cyberattacks, aiming to mitigate their impact on critical infrastructures as well as on sensitive data. While numerous solutions have been proposed and analysed to address the current challenges in IoT security, these approaches are not without vulnerabilities. What follows is an overview of recent proposals put forth by researchers to enhance security within IoT systems.

4.1.1. Intrusion and Anomaly Detection & Concept Drift Detection and Adaption

To protect IoT infrastructures, it is essential to employ two major categories of systems: Intrusion Detection Systems and Intrusion Prevention Systems [13]. The study in [13] focuses specifically on developing an anomaly detection system, analysing various detection techniques within IoT ecosystems while identifying several challenges and limitations of current methods. To address these challenges, the authors propose integrating Incremental Learning, Transfer Learning, and Deep Learning techniques to develop scalable detection models capable of continuous updates, enhancing system performance, and reducing costs and resource requirements. These models can also adapt to contextual changes, a phenomenon known as concept drift.

Another approach to developing an efficient detection system is presented in [15], where the authors examine detection methods used in IoT, including signature-based recognition, anomaly-based detection, hybrid methods, and collaborative approaches among IoT devices. They also draw comparisons between their strengths and weaknesses. Collaborative methods are further explored in [18] to ensure information availability during an attack. This approach relies on secondary devices supporting primary devices in case of an attack, ensuring the continuity of critical information delivery to users. By employing redundancy and cooperation among devices, this strategy enhances the system's resilience and availability in attack scenarios.

The effectiveness of modern methods based on emerging technologies is also highlighted in [15], which discusses the development of detection systems based on deep learning, a branch of machine learning. This technique has proven highly effective in detecting attacks within 5G networks. Using deep learning, intrusion detection pipelines have been created to leverage powerful algorithms capable of identifying and mitigating security threats in real time [21].

An adaptive and high-performing IDS was implemented in the context of electric vehicle charging stations using neural network architectures that combined LSTM and GRU models [22].

One challenge in implementing IDS systems is the prevalence of false-positive alarms. To address this issue and improve classification accuracy, TL and the CBAM [23] can be used. These techniques, through the use of channel and spatial attention, refine feature maps for greater precision.

In anomaly detection systems, careful consideration must be given to the selection of the network architecture, as it is a key factor in achieving more effective anomaly detection. This was demonstrated in [26], where two architectures, EPA and MUD, were compared. The authors showed the superior performance of EPA over MUD. While MUD focuses solely on stateless communication states, EPA provides a comprehensive evaluation of all communication states, offering more detailed analysis for anomaly detection.

4.1.2. DDoS Attacks

The reviewed articles highlight a strong interest in addressing specific cyberattacks that can cause significant damage. For instance, [17] proposes a tailored solution for detecting DDoS attacks, taking into account the phenomenon of concept drift. The solution involves an adaptive online framework capable of adjusting its performance in real-time based on changes in the network environment. Concept drift detection is achieved using ADWIN and DDM methods, while learning capabilities are enhanced through ARF, SRPs, and KNN methods.

In [10], a solution is proposed for detecting DDoS attacks in Information-Centric Networking for IoT networks using machine learning algorithms such as SVM, RF, and KNN. However, the best results were obtained by applying DT and RF classifiers [19], trained on features selected using GA.

Feature extraction was further improved by converting non-image data into image data through deep learning techniques, particularly VGG16 and Inception [24]. The Inception technique, specifically the TCN model within the Inception structure, is proposed in [25] for identifying devices connecting to the network. This method focuses on packet feature extraction, feature selection, and, ultimately, extracting the temporal characteristics of the packets.

4.1.3. Botnet

As IoT systems proliferate, the risk of botnet-driven attacks also increases. The study in [16] examines traditional attack detection methods, which, despite their high resource consumption, are effective in identifying attacks generated by IoT-based botnets. Such approaches can serve as a valid starting point for developing new detection and prevention techniques.

To address the limitations of traditional methods in the IoT context, a botnet attack mitigation framework called IMTIBot was developed [14]. This framework segregates network traffic into normal and abnormal categories and leverages ensemble learning classifiers, combining multiple machine learning models to enhance detection accuracy.

4.1.4. Eavesdropping Attacks

The studies [18] and [19] address the issue of eavesdropping, a challenge that has received relatively little attention in specialised literature. The collaborative method described in [18] ensures signal accuracy for devices within the network while simultaneously disrupting signals to devices attempting unauthorised interception of messages.

In [19], a BP neural network model is proposed for detecting eavesdropping attacks in environments with a low signal-to-noise ratio. Meanwhile, [20] highlights infrared communication and the risk of "listening" to signals emitted by remote controls. To prevent data theft in this context, the authors propose an encryption method that regenerates keys each time the remote control's power button is pressed.

Table 2. Key Challenges and Solutions in Attack Detection.

Challenge	Related Challenges	Key Threats	Solutions
Anomaly detection in IOT	Managing data diversity and scalability in the IoT ecosystem	Limited scalability and resilience in detecting cyber attacks	Integration of ML techniques such as Incremental Learning, Transfer Learning and Deep Learning to obtain scalable and adaptable models able to handle concept drift
References	[13, 22, 23]		
Detection and Prevention of DDoS and Botnet attacks	Response time optimization, limited computational resources of devices	Continuous evolution of DDoS, Botnet attacks and inability of the system to adapt in real time	Using ML techniques to improve response time, system adaptability and network traffic classification
References	[10, 14-18, 25, 26]		

Anomaly detection efficiency	High number of false alarms, balancing detection accuracy and resource consumption	High resource consumption required by traditional detection systems	Use of ML methods for intrusion detection, collaborative systems for effort sharing; Selection of the right architecture
References	[14, 19, 24, 27]		
Eavesdropping attack detection	Unauthorised interception of communication signal, difficulty of detection in low signal-to-noise ratio environments	Balancing the effectiveness of signal disruption for malicious devices without degradation of quality for legitimate users, detection of interception when signal is weak	Introducing intentional signal perturbations to disrupt eavesdroppers; Backpropagation neural network model specifically designed for detecting eavesdropping attacks in low SNR scenarios; Signal encryption or modulation techniques to protect against unauthorised interception
References	[19–21]		

4.2. Data Management & Protection

In the domain of data management and protection, the primary challenges revolve around device and user authorization, ensuring data integrity, and maintaining data confidentiality. Effective solutions must address the verification of identities to prevent unauthorised access, protect data from unauthorised modifications to guarantee its accuracy, and implement robust encryption mechanisms to safeguard sensitive information from breaches and interception.

4.2.1. Data Security and Privacy

Building on the Hyperledger Fabric framework, the authors of [29] propose an innovative concept based on the idea of Blockchain as a Service (BaaS) for securing and protecting data. This integration is achieved through a novel architecture combined with an encrypted data structure utilising public and private keys, offering a high level of security for data management.

Conversely, [28] introduces a blockchain-based platform that leverages smart contracts to enhance data protection. This solution builds upon a three-tier architecture with the addition of a new layer called the Blockchain Composite Layer. This extra layer improves functionality and security, enabling decentralised and automated management of transactions and data. To increase trust in transactions within Ethereum-based blockchain frameworks, [30] proposes introducing a legitimacy rating mechanism through a consensus method and a decentralised proof matrix. Cloud environment security is further enhanced using neural networks for anomaly prediction, providing an additional layer of protection against emerging threats.

The study in [31], emphasises cloud data security, proposing blockchain technology combined with a distributed agent model as a solution. Files are assigned a unique hash value generated using a Merkle hash tree, enabling continuous monitoring to verify their integrity. In case of discrepancies, real-time alerts are sent to the file owners.

4.2.2. Digital Identity & Identity-Based Encryption

The study [32] highlights the role of blockchain technology in securing digital identity through decentralised identity solutions, consent management, and lifecycle management to ensure relevance and accuracy. Blockchain technology also addresses challenges such as scalability and unauthorised access.

In blockchain-based digital identity systems, proposed solutions for enhancing data security include separating identity verification from credential issuance, utilising linkable ring signatures to protect the verifier's identity, employing cryptographic methods for revocation to maintain privacy, and leveraging smart contracts for system management and auditability [33].

Another blockchain-based solution is proposed in [34], featuring high-resistance dynamic encryption, encrypted SSL-VPN channels, and dynamic key mechanisms. The proposed system emphasises anonymous authentication, robust security classifications, and access controls to prevent unauthorised data access and brute-force attacks.

4.2.3. Generative AI

Protecting data privacy and integrity in the context of the proliferation of Generative AI is crucial. In this regard, the authors of [35] propose a multi-faceted approach that includes techniques such as encryption, anonymization, access control, continuous monitoring, protocol development, multi-layered security mechanisms, and AI-powered safeguards.

Federated Learning combined with partial training can protect privacy in machine learning applications within IoT systems [36]. In this approach, IoT devices train smaller sub-models based on a large model hosted on a cloud server, and the server aggregates these sub-models to update the global model. TEE are employed to secure sensitive user data, protecting it from external threats before it is sent to generative models for inference.

Table 3. Key Challenges and Solutions in Data Management and Protection.

Challenge	Related Challenges	Key Threats	Solutions
Data Privacy and Security	Ensuring data integrity and secure storage on decentralised networks and in the Cloud	Data access by unauthorised entities and attacks on data integrity	Blockchain-based frameworks (Hyperledger Fabric), decentralised data management, encrypted data structures and federated learning to ensure data privacy by preventing unauthorised access
References	[29–31]		
Securing Digital Identity	Mitigating unauthorised access and maintaining accurate lifecycle management of identities	Handling a large number of transactions and identity verifications efficiently in a decentralised system, Protecting against brute-force and advanced cryptographic attacks, ensuring encryption mechanisms are robust and dynamic	Separation of identity verification and credential issuance; Linkable ring signatures, smart contracts, encrypted SSL-VPN channels; Robust security classifications and access controls
References	[32–34]		

Data privacy and integrity in context of Generative AI technologies	Protecting sensitive data across distributed systems while balancing security, computational efficiency, and privacy during AI model training, aggregation, and inference	Data breaches, unauthorised access, exploitation of sensitive user inputs, and privacy leakage during Federated Learning model aggregation	Employing encryption, anonymization, and multi-level security mechanisms, Using Trusted Execution Environments (TEE) to protect data inputs during model inference
References	[35, 36]		

4.3. Securing Identity Management

Identity security management in IoT addresses key issues such as authentication, authorization and identity management of connected devices. Researchers are exploring and developing new protocols, technologies and frameworks to ensure secure interactions in the IoT ecosystem, given the limited resources and vulnerability of devices.

4.3.1. Device Identification

Paper [26] proposes a device identification scheme based on extracting time series characteristics of data packets, which are subsequently used as unique fingerprints of the devices. Another approach, presented in [42], involves using the wireless channel state characteristics of devices for identification. Although wireless channels can be unstable, this drawback is compensated by using a locally sensitive hashing algorithm, which improves the stability and accuracy of the identification. An alternative method, based on Paillier homomorphic encryption, is described in [41] allowing verification of device identity without decrypting the message, an efficient approach for privacy preserving.

On the other hand, the paper [43] proposes a multi-layered solution for securely distributing data to users in IoT networks based on blockchain technology. This solution manages authentication, key and message exchange in a decentralised and secure way. The framework uses the ACE protocol for data encryption, ensuring robust protection of information transmitted between devices and users.

To prevent attacks and ensure the authenticity and integrity of data, [48] proposes a framework based on Bloom filters and hash chains. This system could serve as a viable solution in the context of an increasingly complex IoT ecosystem, providing enhanced protection against cyberattacks and ensuring a secure and efficient data flow.

Digital identity, as a method of representing devices within the IoT ecosystem, is discussed in works [32–34,37]. Despite the advantages of blockchain-based digital identity systems, they have several drawbacks, such as issues with identity authenticity, controllability, and privacy protection [33,37]. The study in [32] provides an overview of the challenges and solutions in the medical field. To address these weaknesses, works [33,37] propose a system where the roles of identity verification and credential issuance are separated to reduce the risk of identity-related information leakage. Privacy is enhanced through the use of linkable ring signatures, zero-knowledge proof encryption techniques, and AES. Using a similar approach, the authors of [33,37] developed a Multi-Factor Authentication method utilising blockchain and zero-knowledge proofs. They address weaknesses such as single points of failure and privacy vulnerabilities in blockchain technology through a DAM. Part of the proposed MFA process also includes using NFTs as authentication tokens.

The paper [34] identifies a number of dimensions of digital identity characteristics for users. It proposes a collaborative framework between governmental institutions and non-governmental blockchain alliances, based on a delegated model. It proposes a zero-trust model for digital identity management and big data security.

4.3.2. Authentication

A new framework proposed in [38], based on edge computing and blockchain, explores the use of Ethereum 2 Layer roll-ups to enhance scalability and reduce bottlenecks in the device authentication process. This approach could alleviate the pressure on authentication systems and enable more efficient resource management, given the exponential growth in the number of connected devices. At the same time, [30] introduces an Ethereum-based mechanism that ensures data security through a unique legitimacy score, applicable both at the device level and at the cloud level.

Regarding authentication, [47] suggests a mutual authentication and key agreement protocol designed to address threats in the edge-fog-cloud architecture of 5G networks. This protocol involves mutual identity verification between devices and fog nodes, adding an extra layer of security in the resource access process.

Another notable contribution, [44] proposes a one-time pad protocol to ensure secure communication in IoT, where keys are generated through a multiparty sum of random numbers derived from noise and physical phenomena detected by sensors. This method adds an additional layer of security by using natural phenomena in the encryption process. Similarly, [39] explores the use of sensors to support authentication, suggesting that factors such as the sensor's state and the environment in which it operates can play a crucial role in determining a device's legitimacy.

Furthermore, [40] proposes a three-phase authentication protocol, the first phase being user registration, followed by data encryption using the ECC-AES model and key generation via the SI-AO.

The study [45] addresses the lack of protocols for trust transfer from one service provider to another by developing a framework that minimizes the need for manual intervention by automating the IoT device registration process and issuing operational certificates for new service providers. Paper [46] introduces a new architecture to eliminate the single point of failure issue in the use of PKI, which is easily applicable in IoT systems with resource-constrained devices. This architecture involves the use of ECC cryptography, certificates, and a decentralized PKI system divided into zones, with each zone having a master zone responsible for the devices within that specific zone.

Table 4. Key Challenges and Solutions in Securing Identity Management.

Challenge	Related Challenges	Key Threats	Solutions
Device identification	Device identification management	Unauthorised access, data breaches, instability of wireless channels, single points of failure, identity privacy vulnerabilities, and insufficient protection in IoT and blockchain-based identity systems	Blockchain and Edge Computing based multilevel frameworks; cryptographic techniques like zero-knowledge proofs, AES, ring signatures, distributed authentication mechanisms, and secure data-sharing protocols; Device identification using time series;
References	[26, 32-34, 41-43, 48]		

Authentication	Securing credentials in low-resource environments	Increased vulnerability due to limited resources in the authentication context	Using Ethereum Layer 2 roll-ups, mutual authentication, decentralised PKI, one-time pad encryption, sensor-based verification, ECC-AES encryption, and automated IoT trust transfer
References	[30, 38-40, 44 - 47]		

4.4. Communication & Networking

Communication and Networking in IoT relies on different protocols and technologies, i.e. a variety of networks, each of which involves certain vulnerabilities. Some of the studied articles also propose solutions to mitigate these risks.

4.4.1. Network Security

The solution proposed in article [25], described in the *Attack detection* subsection, also addresses the issue of network security and communication between system components by improving device identification. This ensures enhanced network security against device-specific attacks. For detecting representative attacks within a network, study [54] proposes a solution utilising 110 neural networks. Additionally, it improves the attack-sharing loss function, reducing the number of false alarms and thus contributing to a higher detection rate of actual attacks on the system.

In study [49], the focus began with the goal of increasing the security of the MQTT protocol, ideal for use in systems where devices have limited resources. To this end, it concentrated on the impact of task-specific feature selection. For anomaly detection, five ML algorithms were analysed: DT, KNN, RF, AdaBoost, and XGBoost, with RF proving to deliver the best results.

Article [53] introduces the concept of an IoT Proxy, aimed at offloading security aspects to a more powerful gateway equipped with VNSFs. This approach would mitigate the limitations of devices, such as constrained computational capacity and memory. Addressing the challenges encountered in IoT systems, study [55] proposes a protocol and an algorithm for grouping devices based on coverage, storage capacity, and power. This solution would lead to better network scalability, optimised consumption, and improved load balancing.

4.4.2. Firmware

Another critical aspect in IoT systems is the vulnerability of IoT devices at the firmware level. Study [50] provides a review of firmware vulnerabilities, identifying the challenges encountered at this level and methods to mitigate them. To achieve the desired level of security, the proposed solutions include the development of standards and guidelines for stakeholders involved in IoT system development, the application of emerging technologies to deliver intelligent and adaptive solutions, the use of reverse engineering for firmware analysis, and the development of hybrid frameworks to unify various approaches.

4.4.3.5. G & 6G Networks

The challenges introduced by the characteristics of 5G and 6G networks have been explored in a series of articles. Among the challenges addressed in study [52] are spectrum scarcity and network security. It proposes solutions such as dynamic spectrum sharing and blockchain-based security. Studies [15] and [51] complement these by recommending the use of emerging technologies like AI for anomaly detection at the network level, aiming to reduce response time and optimise resource consumption [51].

The development of ML methods provides scalability for protection systems as the attack surface expands, while maintaining efficiency and detection accuracy [15]. Another proposal from the authors of study [15] focuses on designing and evaluating robust models based on open, standardised datasets tailored for IoT in 5G/6G environments, which also incorporate new forms of attacks.

Table 5. Key Challenges and Solutions in Communication & Networking.

Challenge	Related Challenges	Key Threats	Solutions
Firmware security	Ensuring firmware security in context of diverse IoT device ecosystems	Firmware vulnerabilities leading to unauthorised access, data breaches, and exploitation by attackers through unpatched or outdated software.	Developing IoT security standards, leveraging emerging technologies for adaptive solutions, employing reverse engineering for firmware analysis, and implementing hybrid frameworks for unified security approaches.
References	[50]		
Network Scalability and Load Balancing	Dealing with the diversity of connected device types and resource requirements; Optimise resource allocation	Scalability with increasing devices connected to the system, impacting load management and resource utilisation	Grouping devices based on capacity and coverage; Load balancing optimization protocols; Dynamic feature selection for efficient data processing
References	[25, 49, 53-55]		
Integrating 6G in IoT	Managing high-speed data transfer, spectrum allocation and latency requirements	Spectrum availability and security issues in 6G applications	Dynamic spectrum-sharing, AI and blockchain integration for secure 6G applications and protocol development for real-time response in 6G networks in IoT systems
References	[15, 51- 52]		

4.5. Emergent Technologies

Recent studies are increasingly focusing on developing solutions using emerging technologies such as machine learning, artificial intelligence, edge computing, behavioural analytics, and blockchain technology [19]. According to the analysis conducted by the authors of study [57], there has been a noticeable rise in interest among researchers since 2023 regarding the integration of these technologies into IoT system security methods. These technologies offer enhanced capabilities for detecting system-level anomalies and can be continuously trained to adapt to environmental changes and emerging attack methods.

4.5.1. Machine Learning

The use of ML methods is proposed due to their ability to mitigate and prevent cyberattacks by continuously updating databases with potential attack signatures and performing real-time network traffic analysis for anomaly detection [10, 15]. ML proves valuable in predicting potential threats, making decisions, and optimising resource allocation during an attack [57]. The reviewed articles include evaluations of algorithms to determine which is most effective for classification and feature selection [19, 56, 58]. By optimising model complexity and selecting lightweight algorithms, a balance can be achieved between anomaly detection efficiency and computational performance.

The use of deep learning, as a subset of ML, is recommended due to its capabilities in processing complex patterns, ensuring efficient detection of anomalies and intrusions, reducing false positives, and enabling device identification based on unique features extracted from network traffic [26]. In this context, advanced neural network models are analysed [23, 25].

The reviewed articles also address the issue of selecting a training strategy for ML models. Transfer learning emerges as a solution to reduce the time and computational effort required for training new models [24], leveraging prior knowledge during the training process. Collaborative training solutions are also proposed, such as Federated Learning, which enables distributed model training across IoT devices. This strategy involves sharing model updates while preserving data privacy [43], effectively reducing the risk of man-in-the-middle attacks, malware, eavesdropping, and energy theft [60]. Complementing this approach, Split Learning is proposed, which divides the model training task between devices and a server, ensuring privacy by sharing only intermediate representations instead of raw data or complete models [59]. This method also enhances the efficiency and scalability of the training process.

4.5.2. Blockchain

Blockchain technology is recommended for integration into IoT systems due to its numerous advantages. Blockchain replaces traditional data management systems with a decentralised architecture, enabling direct data transactions without intermediaries [28, 57]. This technology can handle large volumes of transactions while simplifying processes within the system [57]. Through smart contracts, transactions can be automated based on well-defined rules, reducing the need for manual interventions and lowering transaction costs [28, 33, 43].

The management of large data volumes can be improved using off-chain data storage, with only data hashes stored on the blockchain [29]. This approach ensures data integrity without overloading the blockchain. Ethereum-based frameworks can function as a trapdoor to ensure data confidentiality in IoT systems [30]. During the off-chain data repositioning process, encryption and decentralised operations are employed to maintain data privacy.

Thanks to ledgers that record every transaction, traceability is enhanced, fostering greater trust in the system [28, 31, 43, 57]. Frameworks like Hyperledger Fabric reduce the risk of unauthorised data access by restricting it to authorised nodes only [29].

Blockchain ensures confidentiality, integrity, and availability [32]. Data confidentiality is achieved through digital identity encryption methods. Immutable records on the blockchain prevent unauthorised data modifications, maintaining integrity [33, 34, 57]. The decentralised nature of blockchain technology enhances availability, with data stored across multiple nodes [32].

Blockchain technology has also been proposed to enhance authentication processes by integrating Zero-Knowledge Proofs. This method ensures privacy without disclosing sensitive data while verifying the authenticity of OTPs and confirming user identity [37].

4.5.3. Artificial intelligence

The use of Artificial Intelligence, particularly Artificial Immune Systems, aids in detecting and mitigating malware attacks at the IoT device or gateway level, addressing risks without requiring extensive resources [60]. AI methods incorporating Differential Privacy can protect sensitive biometric data by adding controlled noise to the data, mitigating the risk of data leakage during transfer [60].

AI in IoT facilitates the development of intelligent, adaptive security solutions tailored to the diverse applications of IoT systems [60]. It can also complement blockchain technology through its analytical capabilities, particularly in handling large data volumes. AI identifies patterns and anomalies, assisting in transaction validation within blockchain systems [30] Additionally, it can optimise transactions by dynamically adjusting parameters [30].

AI enhances ML capabilities, and Generative AI can be employed to create diverse datasets for training models when real-world datasets are limited [35]. Generative AI can also simulate scenarios to improve decision-making and predictive capabilities [35, 36]. Moreover, this technology enhances human-device interaction, as AI models can interpret human voice with greater accuracy [36]. AI can further reduce failure risks by analysing historical data to predict maintenance requirements for devices [30].

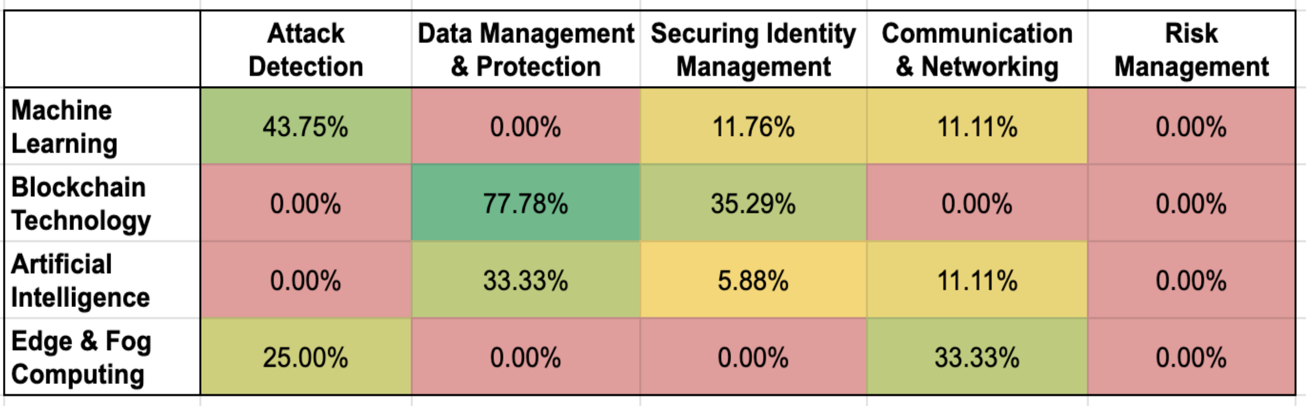
AI is also pivotal in addressing challenges associated with the introduction of 6G networks. It can optimise network performance, deliver personalised services in 6G based on user behaviour, and enable innovative applications such as holographic communication and augmented reality [51].

4.5.4. Edge Computing & Fog Computing

Edge Computing and Fog Computing can enhance the efficiency of cooperation between IoT systems and the Cloud while also improving their security and scalability [16].These technologies involve performing computational processes closer to the data source [55], although this approach may result in higher energy consumption for the selected devices [24]. Nevertheless, the proposed solution reduces latency, enabling faster attack detection [17] and preventing their propagation within the system [22, 53].

Additionally, these approaches decrease the amount of data transmitted to the Cloud, reducing bandwidth requirements [23] and optimising data transmission across the network [51].

The representation below shows the use of emerging technologies in the categories identified.



	Attack Detection	Data Management & Protection	Securing Identity Management	Communication & Networking	Risk Management
Machine Learning	43.75%	0.00%	11.76%	11.11%	0.00%
Blockchain Technology	0.00%	77.78%	35.29%	0.00%	0.00%
Artificial Intelligence	0.00%	33.33%	5.88%	11.11%	0.00%
Edge & Fog Computing	25.00%	0.00%	0.00%	33.33%	0.00%

Figure 7. Heat map of Emergent Technologies usage in identified categories.

Due to the specific nature of Risk Management, this category does not employ emergent technologies in the reviewed articles. Instead, it focuses on creating frameworks to achieve standardizations and risk management models aimed at guiding organisations in formulating cybersecurity implementation policies for IoT systems. However, even in this area, the cognitive capabilities of ML and AI could be utilised to adapt rules based on the application domain, identify latent risks, and update regulations in response to new threats and technological advancements.

The heatmap highlights that the four emergent technologies have varying levels of adoption across the identified categories. Machine Learning is most frequently suggested in solutions for attack detection, owing to its capabilities in traffic analysis, anomaly detection, and optimization of limited resources. Blockchain technology demonstrates its prominence in the data management & protection category, attributed to its decentralisation features and ability to ensure data integrity and confidentiality. This category also sees significant use of Artificial Intelligence, particularly Generative AI, which can generate necessary conditions, such as test data for training ML models, validate transactions within blockchain systems, and support data integrity assurance. Edge and Fog Computing emerge as deployment suggestions for attack detection systems and as solutions for securing networks and facilitating communication between edge devices and servers. These technologies contribute by reducing latency, improving security, and ensuring efficient network operations.

4.6. Risk Management

The complexity and dynamic nature of the IoT ecosystem have necessitated the development of strategies tailored to this context. To address this need, various risk management methodologies have been proposed. For instance, [61] outlines several types of risks and identifies the main frameworks employed in managing them. Similarly, [62] conducts a literature review on risk management, also examining the frameworks discussed in [61]. Both studies highlight vulnerabilities in existing methodologies.

A novel framework for risk management, IOTA-SRM, is introduced in [63] to address the limitations of current frameworks. This systematic approach manages risk across different architectural levels within IoT systems. Additionally, the IoTSRM2 proposed in [64] underscores the necessity for comprehensive solutions. These approaches emphasize multi-layered cybersecurity strategies, incorporating encryption, machine learning for threat detection, and blockchain to ensure secure communications. A critical aspect of these frameworks is the focus on security at various architectural levels within IoT systems, particularly at the device and network levels, which are highly vulnerable to attacks such as DDoS and data interception.

Table 6. Key Challenges and Solutions in Risk Management.

Challenge	**Related Challenges**	**Key Threats**	**Solutions**

Lack of standardisation in risk management approach	Identifying threats and managing vulnerabilities, ensuring resilience in compliance with data protection standards	Balancing security constraints and devices;
		Performing real-time updates;
		Complying with GDPR and IoT-specific regulations while maintaining system functionality
			Creating risk assessment models;
			Threat modelling;
			Using ML for real-time risk assessment;
			Compliance-oriented frameworks

References	[61–64]		

5. Discussion

Following the analysis of the selected articles and the identification of the categories of topics addressed by them, a bar chart was made to observe the weight of concern regarding the listed categories. It should be noted that those articles that fell under more than one category were considered for each.

doi:10.20944/preprints202412.2512.v1

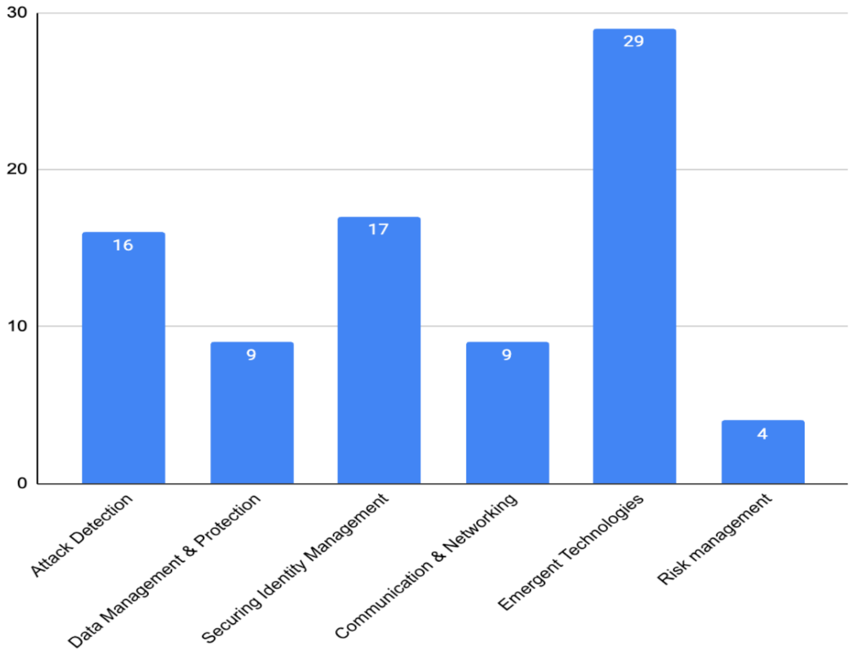


Figure 8. Articles by categories.

The bar chart analysis reveals that three of the six categories—Securing Identity Management, Attack Detection, and Emergent Technologies—garner heightened attention. Among these, Emergent Technologies dominate the chart, reflecting their extensive adoption in proposed solutions. This widespread utilisation stems from their ability to process large datasets, reduce anomaly detection time, and adapt to the rapidly evolving landscape of threats and attack types specific to IoT systems. Suggested approaches include leveraging ML techniques for predicting and preventing attacks, employing blockchain technology to enhance security through decentralisation, and deploying Edge and Fog Computing to minimise latency and prevent the propagation of attacks across systems.

However, integrating emergent technologies introduces new challenges, such as vulnerabilities and the resource constraints inherent to IoT devices. Training AI and ML models demands substantial computational resources, presenting a significant hurdle. Additionally, regulatory issues and ethical dilemmas arise, particularly when systems must make decisions that might involve trade-offs or sacrifices. Addressing these challenges will require innovative solutions to maximise the benefits of these technologies while mitigating their drawbacks.

5.1. Securing Identity Management

This category reflects the need to ensure that only authorised entities have access to the network. The increasing prevalence of threats targeting identity theft, unauthorised system access, and credential theft underscores the urgency of developing robust identity protection mechanisms. These include multi-factor authentication and strict access controls. Future implementations may combine emergent technologies such as AI, Blockchain, and ML with biometric identification methods. Such an approach could improve the accuracy of biometric authentication, enhance data security, and ensure adaptability to new threats.

5.2. Attack Detection

Attack detection is a cornerstone of IoT security, critical for identifying and mitigating threats promptly to prevent significant losses for both systems and users. The focus in this category highlights the importance of real-time system monitoring, adaptability to evolving threats, incident

doi:10.20944/preprints202412.2512.v1

response capabilities, and resource optimization. The reviewed studies emphasise integrating ML techniques to develop adaptive detection systems with faster response times and collaborative methods that distribute detection tasks across system components.

5.3. Communication & Networking and Data Management & Protection

These two categories received equal attention, reflecting their continued importance in establishing a secure infrastructure.

5.3.1. Communication & Networking

Secure communication and networking are essential to maintaining a reliable flow of data within IoT systems. The studies reviewed propose protocols tailored for 5G and 6G networks and methods to integrate AI for faster response times and reduced resource consumption. Dynamic spectrum sharing is suggested as a solution to bandwidth limitations; however, it introduces challenges such as interference and unauthorised access that need to be addressed.

5.3.2. Data Management & Protection

This category focuses on ensuring encryption, implementing backup strategies, and adhering to data protection regulations to mitigate data breaches that could lead to financial or reputational damage. The advent of quantum computing poses a significant challenge to classical encryption systems, as quantum computers could easily break traditional cryptographic algorithms.

5.4. Risk Management

As a complementary category, risk management underscores the importance of regulations in building robust cybersecurity methodologies for IoT systems. This domain has fewer studies, as it is often reactive, requiring the occurrence of specific limitations to inspire experimentation and the development of effective frameworks. Incorporating ML and AI into risk management could enable dynamic rule adaptation based on application domains, identification of latent risks, and updates to guidelines in response to emerging threats and technological evolution.

Following the analysis of the selected articles based on the identified categories, the proposed solutions highlight efforts to implement scalable and adaptable attack detection and prevention systems capable of handling concept drift. Another key focus in the attack detection field is optimizing response time and reducing false alarms. These systems also need to function effectively in resource-constrained environments with limited computational capacity. Researchers are experimenting with machine learning techniques to address these challenges; however, issues such as long model training times and the need for continuous adaptability remain significant.

In the area of data security and management, several articles propose blockchain-based frameworks to ensure authorized data access and protect data integrity during distribution and storage. These frameworks can be enhanced with Edge Computing, encryption techniques like zero-knowledge proofs, and secure data-sharing protocols.

For the Network and Communication category, solutions address challenges arising from the diversity of connected devices and spectrum allocation. Proposed approaches include grouping devices by capacity and coverage, enabling dynamic spectrum sharing, and developing IoT security standards to secure device firmware.

The Risk Management category also emphasizes the need for standardization. Articles in this category propose the development of compliance-oriented frameworks, threat modelling techniques, and risk assessment models.

6. Conclusions and Future Work

This paper presented a systematic review of the latest IoT security research, aiming to identify key directions for enhancing both the security and trustworthiness of IoT systems.

The paper starts by identifying and categorising critical aspects of IoT security, specifically focusing on Attack Detection, Communication & Networking, Securing identity management, Data Management & Protection, Risk Management and using Emergent Technologies.

After the conducted analysis from the paper, it can be concluded that Attack detection techniques are increasingly relying on advanced ML and deep learning models for precise anomaly detection, reduced false positives, and real-time responsiveness. Data management and protection emphasise dynamic, blockchain-based solutions to secure sensitive information while ensuring scalability. Identity management has advanced through blockchain and Edge Computing-based multilevel frameworks, cryptographic techniques such as zero-knowledge proofs, AES, ring signatures, distributed authentication mechanisms, and secure data-sharing protocols. Device identification using time series, Ethereum Layer 2 roll-ups, mutual authentication, decentralised PKI, one-time pad encryption, sensor-based verification, ECC-AES encryption, and automated IoT trust transfer further enhances the security of IoT systems.

Networking and communication challenges, particularly with 5G/6G environments, are being tackled through dynamic spectrum sharing and secure protocols. Emerging technologies such as AI and Edge Computing are proving instrumental in adaptive security measures, offering real-time anomaly detection and resource efficiency. Despite these advancements, challenges remain, including the need for standardised datasets, robust evaluation methods, and scalable solutions that can adapt to an expanding attack surface.

Future research should prioritize enhancing communication and networking security by exploring quantum-resistant cryptography to safeguard IoT systems against potential quantum computing threats. Additionally, the secure management of large-scale IoT data must be addressed through innovative approaches such as blockchain for data integrity and privacy-preserving techniques like homomorphic encryption. Investigating secure fallback strategies to ensure system resilience during failures or breaches is essential for reliable IoT deployments. Finally, optimizing resource management in IoT systems using AI and machine learning can improve efficiency, adaptability, and threat mitigation capabilities. Table 7 presents a synthesis of future research directions derived from the analysis.

Table 8. Future research directions in IoT security.

Category	Future directions
Attack detection	Develop AI and ML-based techniques to improve real-time anomaly detection and threat prediction
Data management & protection	Integrating blockchain and privacy-preserving techniques
Securing identity management	Decentralized identity solutions and advanced authentication mechanisms
Communication & Networking	Quantum-resistant cryptography
Emergent technologies	Optimize resource management using AI and ML
Risk management	Investigate secure fallback strategies

Author Contributions: Conceptualization, H.S. and D.E.P.; methodology, H.S., D.E.P. and R.D.Z.; resources, H.S. and D.E.P.; writing—original draft preparation, H.S., and D.E.P.; writing—review and editing, D.E.P., R.D.Z. and H.S.; visualization D.E.P.; supervision, D.E.P. and R.D.Z.; project administration D.E.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

2FA	Two-factor authentication

doi:10.20944/preprints202412.2512.v1

ACE	Associative Cryptographic Encryption
ADWIN	Adaptive Windowing
AI	Artificial Intelligence
ARF	Adaptive Random Forest
CBAM	Convolutional Block Attention Module
CoAP	The Constrained Application Protocol
DAM	Distributed Authentication Mechanism
DDM	Deep Drift Model
DDoS	Distributed Denial of Service
DT	Decision Tree
ECC	Elliptic Curve Cryptography
ECC-AES	Elliptic Curve Cryptography with Advanced Encryption Standard
EPA	Extended Protocol Architecture
GA	Genetic Algorithms
GDPR	General Data Protection Regulation
GRU	Gated Recurrent Unit
ICN-IoT	Information-Centric Networking for IoT
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IoT	Internet of Things
IOTA-SRM	IoT architecture-based Security Risk Management
IoTSRM2	IoT Security Risk Management Strategy Model
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization
KNN	k-Nearest Neighbours
LPWAN	Low-Power Wide-Area Networks
LSTM	Long Short-Term Memory
LTE-M	Long Term Evolution for Machines
MFA	Multi-factor authentication
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MUD	Manufacturer Usage Description
NB-IoT	Narrow Band-Internet of Things
NFT	Non-Fungible Token
NIST	National Institute of Standards and Technology
OTP	One-Time Password
PKI	Public Key Infrastructure
RF	Random Forest
RFC	Request For Comments
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisition
SI-AO	Self-Improved Aquila Optimizer
SRPs	Sampled Randomized Pooling Strategy

SSL-VPN	Secure Sockets Layer Virtual Private Network
SVM	Support Vector Machine
TCN	Temporal Convolutional Network
TL	Transfer Learning
VGG16	Visual Geometry Group 16 (number of layers with learnable parameters)
VNSFs	Virtual Network Security Functions

References

1. Greengard, S. Internet of Things. *Encyclopedia Britannica* 2024. Available online: https://www.britannica.com/science/Internet-of-Things (accessed on 01.10.2024).
2. IoT Analytics, *State of IoT 2024: Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally*, Available online: https://iot-analytics.com/number-connected-iot-devices (accessed on 01.11.2024).
3. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016, Available online: https://eur-lex.europa.eu/legal-content (accessed on 04.11.2024).
4. H.R.1668 - IoT Cybersecurity Improvement Act of 2020, Available online: https://www.congress.gov/bill/116th-congress/house-bill/1668 (accessed on 04.11.2024).
5. AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic Form IoT Cybersecurity Alliance 2017, Available online: https://about.att.com/story/iot_cybersecurity_alliance.html (accessed on 04.11.2024).
6. The Industry IoT Consortium, An Industry IoT Foundational Publication, Available online: https://www.iiconsortium.org/iisf (accessed on 04.11.2024).
7. CoAP RFC 7252 Constrained Application Protocol, Available online: https://coap.space/ (accessed on 04.11.2024).
8. ISO/IEC 30141 Internet of Things (IoT) — Reference Architecture, Available online: https://www.iso.org/standard/88800.html (accessed on 04.11.2024).
9. Unpacking IoT Architecture: Layers and Components Explained, Available online: https://deviceauthority.com/unpacking-iot-architecture-layers-and-components-explained/ (accessed on 02.12.2024).
10. Bukhowah, R.; Aljughaiman, A.; Rahman, M.M.H. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. *Electronics (Basel)* **2024**, *13*, 1031. https://doi.org/10.3390/electronics13061031.
11. Domínguez-Bolaño, T.; Campos, O.; Barral, V.; Escudero, C.J.; García-Naya, J.A. An Overview of IoT Architectures, Technologies, and Existing Open-Source Projects. *Internet of Things* **2022**, *20*, 100626. https://doi.org/10.1016/j.iot.2022.100626.
12. Tkhir, P. 4 Types of IoT Networks: Overview and Use Cases 2023.
13. 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/10.1109/ACCESS.2021.3073408.
14. Garg, U.; Kumar, S.; Mahanti, A. IMTIBOT: An Intelligent Mitigation Technique for IoT Botnets. *Future Internet* **2024**, *16*, 212. https://doi.org/10.3390/fi16060212.
15. Chen, Z.; Liu, J.; Shen, Y.; Simsek, M.; Kantarci, B.; Mouftah, H.T.; Djukic, P. Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats. *ACM Comput. Surv.* **2023**, *55*, 1–37. https://doi.org/10.1145/3530812.
16. Woodiss-Field, A.; Johnstone, M.N.; Haskell-Dowland, P. Examination of Traditional Botnet Detection on IoT-Based Bots. *Sensors* **2024**, *24*, 1027. https://doi.org/10.3390/s24031027.
17. Beshah, Y.K.; Abebe, S.L.; Melaku, H.M. Drift Adaptive Online DDoS Attack Detection Framework for IoT System. *Electronics (Basel)* **2024**, *13*, 1004. https://doi.org/10.3390/electronics13061004.

18. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors* **2024**, *24*, 713. https://doi.org/10.3390/s24020713.
19. Farraj, A.; Hammad, E. A Physical-Layer Security Cooperative Framework for Mitigating Interference and Eavesdropping Attacks in Internet of Things Environments. *Sensors* **2024**, *24*, 5171. https://doi.org/10.3390/s24165171.
20. Li, M.; Dou, Z. Active Eavesdropping Detection: A Novel Physical Layer Security in Wireless IoT. *EURASIP J. Adv. Signal Process.* **2023**, *2023*, 119. https://doi.org/10.1186/s13634-023-01080-5.
21. Kim, M.; Suh, T. Eavesdropping Vulnerability and Countermeasure in Infrared Communication for IoT Devices. *Sensors* **2021**, *21*, 8207. https://doi.org/10.3390/s21248207.
22. Moubayed, A. A Complete EDA and DL Pipeline for Softwarized 5G Network Intrusion Detection. *Future Internet* **2024**, *16*, 331. https://doi.org/10.3390/fi16090331.
23. Kilichev, D.; Turimov, D.; Kim, W. Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models. *Mathematics* **2024**, *12*, 571. https://doi.org/10.3390/math12040571.
24. Abdelhamid, S.; Hegazy, I.; Aref, M.; Roushdy, M. Attention-Driven Transfer Learning Model for Improved IoT Intrusion Detection. *BDCC* **2024**, *8*, 116. https://doi.org/10.3390/bdcc8090116.
25. Chen, J.; Xiao, J.; Xu, J. VGGIncepNet: Enhancing Network Intrusion Detection and Network Security through Non-Image-to-Image Conversion and Deep Learning. *Electronics (Basel)* **2024**, *13*, 3639. https://doi.org/10.3390/electronics13183639.
26. Hu, L.; Zhao, B.; Wang, G. A Network Device Identification Method Based on Packet Temporal Features and Machine Learning. *Applied Sciences* **2024**, *14*, 7954. https://doi.org/10.3390/app14177954.
27. Aroon, N.; Liu, V.; Kane, L.; Li, Y.; Tesfamicael, A.D.; McKague, M. An Architecture of Enhanced Profiling Assurance for IoT Networks. *Electronics (Basel)* **2024**, *13*, 2832. https://doi.org/10.3390/electronics13142832.
28. Yang, Z.; Liu, Y.; Jin, X.; Luo, X.; Xu, Y.; Li, M.; Chen, P.; Tang, B.; Lin, B. BDIDA-IoT: A Blockchain-Based Decentralized Identity Architecture Enhances the Efficiency of IoT Data Flow. *Applied Sciences* **2024**, *14*, 1807. https://doi.org/10.3390/app14051807.
29. Eghmazi, A.; Ataei, M.; Landry, R.J.; Chevrette, G. Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. *IoT* **2024**, *5*, 20–34. https://doi.org/10.3390/iot5010002.
30. Khan, B.U.I.; Goh, K.W.; Khan, A.R.; Zuhairi, M.F.; Chaimanee, M. Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities. *Processes* **2024**, *12*, 1825. https://doi.org/10.3390/pr12091825.
31. Wei, P.; Wang, D.; Zhao, Y.; Tyagi, S.K.S.; Kumar, N. Blockchain Data-Based Cloud Data Integrity Protection Mechanism. *Future Generation Computer Systems* **2020**, *102*, 902–911. https://doi.org/10.1016/j.future.2019.09.028.
32. Jena, S.K.; Barik, R.C.; Priyadarshini, R. A Systematic State-of-Art Review on Digital Identity Challenges with Solutions Using Conjugation of IOT and Blockchain in Healthcare. *10.1007/s13369-024-09178-* **2024**, *25*, 101111. https://doi.org/10.1016/j.iot.2024.101111.
33. Song, Z.; Yan, E.; Song, J.; Jiang, R.; Yu, Y.; Chen, T. A Blockchain-Based Digital Identity System with Privacy, Controllability, and Auditability. *Arab J Sci Eng* **2024**. https://doi.org/10.1007/s13369-024-09178-0.
34. Wang, F.; Gai, Y.; Zhang, H. Blockchain User Digital Identity Big Data and Information Security Process Protection Based on Network Trust. *Journal of King Saud University - Computer and Information Sciences* **2024**, *36*, 102031. https://doi.org/10.1016/j.jksuci.2024.102031.
35. Xu, H.; Li, Y.; Balogun, O.; Wu, S.; Wang, Y.; Cai, Z. Security Risks Concerns of Generative AI in the IoT 2024.
36. Wang, X.; Wan, Z.; Hekmati, A.; Zong, M.; Alam, S.; Zhang, M.; Krishnamachari, B. IoT in the Era of Generative AI: Vision and Challenges 2024.
37. Jose Diaz Rivera, J.; Muhammad, A.; Song, W.-C. Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. *IEEE Open Journal of the Communications Society* **2024**, *5*, 2792–2814. https://doi.org/10.1109/OJCOMS.2024.3391728.
38. Bojič Burgos, J.; Pustišek, M. Decentralized IoT Data Authentication with Signature Aggregation. *Sensors* **2024**, *24*, 1037. https://doi.org/10.3390/s24031037.

39. Saideh, M.; Jamont, J.-P.; Vercouter, L. Opportunistic Sensor-Based Authentication Factors in and for the Internet of Things. *Sensors* **2024**, *24*, 4621. https://doi.org/10.3390/s24144621.
40. Munshi, A.; Alshawi, B. Hybrid Encryption Model for Secured Three-Phase Authentication Protocol in IoT. *JSAN* **2024**, *13*, 41. https://doi.org/10.3390/jsan13040041.
41. Tun, N.W.; Mambo, M. Secure PUF-Based Authentication Systems. *Sensors* **2024**, *24*, 5295. https://doi.org/10.3390/s24165295.
42. Zhang, B.; Zhang, T.; Xi, Z.; Chen, P.; Wei, J.; Liu, Y. Secure Device-to-Device Communication in IoT: Fuzzy Identity from Wireless Channel State Information for Identity-Based Encryption. *Electronics (Basel)* **2024**, *13*, 984. https://doi.org/10.3390/electronics13050984.
43. Wang, J.; Li, J. Blockchain and Access Control Encryption-Empowered IoT Knowledge Sharing for Cloud-Edge Orchestrated Personalized Privacy-Preserving Federated Learning. *Applied Sciences* **2024**, *14*, 1743. https://doi.org/10.3390/app14051743.
44. Fenner, J.; Galeas, P.; Escobar, F.; Neira, R. Secure IoT Communication: Implementing a One-Time Pad Protocol with True Random Numbers and Secure Multiparty Sums. *Applied Sciences* **2024**, *14*, 5354. https://doi.org/10.3390/app14125354.
45. Höglund, J.; Bouget, S.; Furuhed, M.; Preuß Mattsson, J.; Selander, G.; Raza, S. AutoPKI: Public Key Infrastructure for IoT with Automated Trust Transfer. *Int. J. Inf. Secur.* **2024**, *23*, 1859–1875. https://doi.org/10.1007/s10207-024-00825-z.
46. El-Hajj, M.; Beune, P. Decentralized Zone-Based PKI: A Lightweight Security Framework for IoT Ecosystems. *Information* **2024**, *15*, 304. https://doi.org/10.3390/info15060304.
47. Zhang, J.; Ouda, A.; Abu-Rukba, R. Authentication and Key Agreement Protocol in Hybrid Edge–Fog–Cloud Computing Enhanced by 5G Networks. *Future Internet* **2024**, *16*, 209. https://doi.org/10.3390/fi16060209.
48. Baird, I.; Ghaleb, B.; Wadhaj, I.; Russell, G.; Buchanan, W.J. Securing IoT: Mitigating Sybil Flood Attacks with Bloom Filters and Hash Chains. *Electronics (Basel)* **2024**, *13*, 3467. https://doi.org/10.3390/electronics13173467.
49. Al Hanif, A.; Ilyas, M. Effective Feature Engineering Framework for Securing MQTT Protocol in IoT Environments. *Sensors* **2024**, *24*, 1782. https://doi.org/10.3390/s24061782.
50. Bakhshi, T.; Ghita, B.; Kuzminykh, I. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors* **2024**, *24*, 708. https://doi.org/10.3390/s24020708.
51. Maduranga, M.W.P.; Tilwari, V.; Rathnayake, R.M.M.R.; Sandamini, C. AI-Enabled 6G Internet of Things: Opportunities, Key Technologies, Challenges, and Future Directions. *Telecom* **2024**, *5*, 804–822. https://doi.org/10.3390/telecom5030041.
52. Singh, C.; Kumar, M.; Upadhyay, M.; Chauhan, P.; Sharma, M. A 6G Network: Future of Nations? Challenges in 6G Communications. *Tuijin Jishu/Journal of Propulsion Technology* **2023**, *44*, 73–76.
53. Canavese, D.; Mannella, L.; Regano, L.; Basile, C. Security at the Edge for Resource-Limited IoT Devices. *Sensors* **2024**, *24*, 590. https://doi.org/10.3390/s24020590.
54. Ehmer, J.; Savaria, Y.; Granado, B.; David, J.-P.; Denoulet, J. Network Attack Classification with a Shallow Neural Network for Internet and Internet of Things (IoT) Traffic. *Electronics (Basel)* **2024**, *13*, 3318. https://doi.org/10.3390/electronics13163318.
55. Achkouty, F.; Gallon, L.; Chbeir, R. RDSC: Range-Based Device Spatial Clustering for IoT Networks. *Sensors* **2024**, *24*, 5851. https://doi.org/10.3390/s24175851.
56. Ortiz-Ruiz, E.; Bermejo, J.R.; Sicilia, J.A.; Bermejo, J. Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia. *Electronics (Basel)* **2024**, *13*, 824. https://doi.org/10.3390/electronics13050824.
57. Valencia-Arias, A.; González-Ruiz, J.D.; Verde Flores, L.; Vega-Mori, L.; Rodríguez-Correa, P.; Sánchez Santos, G. Machine Learning and Blockchain: A Bibliometric Study on Security and Privacy. *Information* **2024**, *15*, 65. https://doi.org/10.3390/info15010065.
58. El-Sofany, H.; El-Seoud, S.A.; Karam, O.H.; Bouallegue, B. Using Machine Learning Algorithms to Enhance IoT System Security. *Sci Rep* **2024**, *14*, 12077. https://doi.org/10.1038/s41598-024-62861-y.

59. Priyadarshini, I. Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning. *BDCC* **2024**, *8*, 21. https://doi.org/10.3390/bdcc8030021.
60. Alrubayyi, H.; Alshareef, M.S.; Nadeem, Z.; Abdelmoniem, A.M.; Jaber, M. Security Threats and Promising Solutions Arising from the Intersection of AI and IoT: A Study of IoMT and IoET Applications. *Future Internet* **2024**, *16*, 85. https://doi.org/10.3390/fi16030085.
61. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process. *EURASIP J. on Info. Security* **2020**, *2020*, 8. https://doi.org/10.1186/s13635-020-00111-0.
62. Parsons, E.K.; Panaousis, E.; Loukas, G.; Sakellari, G. A Survey on Cyber Risk Management for the Internet of Things. *Applied Sciences* **2023**, *13*, 9032. https://doi.org/10.3390/app13159032.
63. Affia, A.O.; Nolte, A.; Matulevičius, R. IoT Security Risk Management: A Framework and Teaching Approach. *Informatics in Education* **2023**. https://doi.org/10.15388/infedu.2023.30.
64. Popescu, T.; Popescu, A.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet* **2021**, *13*, 148. https://doi.org/10.3390/fi13060148.

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.