Scientific Research Publishing

Advances in Internet of Things, 2025, 15(1), 1-15
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

Internet of Things Security: Threats, Recent Trends, and Mitigation Approaches

Laila Tageldin

Department of Computer Science, Sudan University of Science and Technology, Khartoum, Sudan
Email: laylataj@hotmail.co.uk

How to cite this paper: Tageldin, L. (2025) Internet of Things Security: Threats, Recent Trends, and Mitigation Approaches. *Advances in Internet of Things*, **15**, 1-15.
https://doi.org/10.4236/ait.2025.151001

Received: January 7, 2025
Accepted: January 24, 2025
Published: January 27, 2025

Abstract

The Internet of Things (IoT) is regarded as the driving force behind the Fourth Industrial Revolution. The convergence of IoT, cloud computing, and smart environments can help ensure people's well-being. One major problem for IoT networks is protecting privacy and overcoming security threats. This paper discusses security threats across IoT networks, which can lead the researchers to develop and implement industry-wide security standards and certifications. In addition, this paper emphasizes the importance of data protection and discusses the security measures and mitigation approaches to secure personal and sensitive information, as well as other security threats within such environments. As well, the primary objective of this work is to present a contemporary review of the prevailing research areas concerning IoT security, which highlights the recent trends in IoT security, identifies inadequacies in the investigated research publications, and discusses the associated difficulties. That will assist researchers in developing an efficient, scalable, resilient, and precise intrusion detection system for IoT devices to counter large-scale attacks.

Keywords

Internet of Things (IoT), IoT Security, IoT Security Threats, IoT Security Measures, Mitigation Approaches

1. Introduction

The Internet of Things (IoT) is an expanding field that connects and communicates devices or objects over the Internet, using its benefits. The idea with this innovation is to automate tasks and link objects that used on a daily basis via the Internet. Sensors and actuators are attached to each object to collect physical data.

IoT opens a new era of connection, revolutionizing how electronic devices communicate and exchange data [1]. Recently, IoT devices are increasingly being

integrated into various aspects of daily life, from smart homes and wearable devices to industrial systems. Highlighting security threats can help users, developers, and organizations become aware of the potential risks associated with these devices [2].

IoT is a network of hardware and software connected to daily activities, providing dependability and convenience. The network is largely made up of heterogeneous devices that use multiple protocols. The technology is developing, introducing numerous new IoT gadgets to the market. Because of their computing, storage, and networking capabilities, IoT devices enable consumers to live more convenient lives. It is also useful in the fields of robotics, healthcare, and data analytics. However, developers and consumers continue to be concerned about the security of the IoT network. The network's diverse structure makes it challenging for engineers to secure it [3].

Although, there are many threats when integrating IoT technologies, such as information transmission between devices, data management, security, and privacy are the most critical problems that must be addressed initially [4].

In addition, IoT technologies provide additional hurdles to the Internet's inherently complicated security landscape. Managing the growing number of linked IoT devices is a huge task. The proliferation of IoT systems introduces new device classes, posing distinct issues that must be addressed. Some may be clear, whereas others might not be so [5].

To facilitate widespread adoption of safe IoT devices and applications, it is essential to engage in organizing the IoT security environment. Consequently, this survey delineates a summary of principal security objectives that must be adhered to during the design, specification, and implementation phases of IoT applications. It situates IoT-related threats within a well-defined IoT architectural model to direct the focus of IoT developers on significant attack vectors that may arise at various levels of IoT-integrated systems [6].

The security of IoT has garnered considerable interest in academia. A significant number of studies examined the security of IoT systems. Most prior surveys examined pertinent security topics, including threats, requirements, and obstacles in IoT. Nonetheless, several developing technologies and methodologies have lately been implemented as viable options to enhance IoT security [7].

IoT devices often have vulnerabilities due to limited computing resources, a lack of security standards, or inadequate updates. This paper provides an overview of the security threats across IoT networks, making it easier to address them proactively. As well, the primary objective of this work is to present a contemporary review of the prevailing research areas concerning IoT security.

This paper is structured as follows. Section 2 presents the methodology that followed throughout the paper. Section 3 provides an overview of literature and all the important concepts of which the reader needs to take cognizance in this paper. Section 4 presents the recent trends and challenges. Section 5 outlines the results and discussion. Section 6 outlines potential avenues for future research.

Section 7 concludes the paper.

2. Methodology

The subsequent methodology was followed to direct the discussed problems and security concerns:

- The literature review section represents a background about IoT, and security threats for IoT based on research/review papers between 2019 to 2024.
- Security and privacy threats for IoT taxonomy, it is a structured classification that helps identify, categorize, and assess the different types of security and privacy threats.
- Presents the recent trends of IoT security by introducing innovative solutions that tackle IoT security challenges and offer a comparative analysis of recent research studies centred on these solutions.
- Discussion and result section that helps to interpret the findings in light of the literature review. It bridges the gap between what is known (from existing research) and what has been discovered or observed in the current study. Also, it helps to identify gaps that still exist in the current body of knowledge on security threats, indicating areas that future research could address.

The paper follows these phases.

3. Literature Survey

3.1. Background about IoT

IoT devices combine embedded systems with networking capabilities. Peripherals can incorporate sensors, external memory, and actuators. Sensors in an IoT system enable the gadget to detect its environment. Sensors can monitor temperature, humidity, location, heart rate, and gas. Hardware components include embedded IoT devices combine embedded systems with networking capabilities. Peripherals can incorporate sensors, external memory, and actuators. Sensors in an IoT system enable the gadget to detect its environment. Sensors can monitor temperature, humidity, location, heart rate, and gas. Hardware components include embedded systems, memory, network cards, and more devices. These components are integrated to create a functional IoT device [3].

IoT is driven by the need to gather, exchange, and communicate information automatically, remotely, and without interruption. The IoT is an interconnected collection of online-connected objects or devices with integrated sensors capable of collecting, sending, and exchanging data. Currently, many networked devices lack a clear network standard or border [8].

The IoT environment consists of four key levels. The primary layer uses sensors and actuators to process data and execute various functions. The second layer utilizes a communication network to transfer gathered data. IoT applications often use a middleware layer to connect the network and application layers. The fourth layer includes IoT-based applications such as smart grids, transportation, and industries. Each of the four tiers has unique security challenges. In addition to these

levels, gateways facilitate data flow. There are several security threats associated these gateways [4].

The applications of IoT devices are boundless, resulting in the fast expansion of the market, which is divided into four primary application domains [6] [9]:

- Industrial Internet of Things (IIoT)

IIoT pertains to applications inside production lines, wherein machines engage in communication with one another. They can supervise each other, distribute tasks fairly, detect wear and tear to prevent failure, guarantee uninterrupted production, and provide real-time production data.

- Internet of Medical Things (IoMT)

The basic function of IoMT is to guarantee the ongoing accessibility of information. A patient's cardiac monitor transmits data to a healthcare practitioner for oversight. Additionally, remote access facilitates remote setup. A broader audience use fitness trackers and smartwatches.

- Smart cities

Smart cities are a highly significant category of applications throughout society. The fast increase of the urban population globally drives economic growth in cities. The IoT facilitates the management of fast urbanization by enabling smart city devices to efficiently regulate traffic through the recognition of traffic patterns and the optimization of traffic signal operations. Furthermore, a waste disposal system may be enhanced by outfitting garbage containers with sensors. Rather of ineffectively traversing streets to collect every dumpster, only filled containers will be prioritized for collection. Cities systematically gather a multitude of data, including tax payments, water use statistics, and construction licenses.

- Smart houses

The fourth group of applications is smart houses. The previously mentioned ubiquitous thermostat and the pioneering Internet-enabled toaster are included in this category. Additional devices encompass smart televisions, interconnected light bulbs, window shutters, door locks, and surveillance systems.

Due to increased number of IoT devices that connect to the internet, security concerns increased. Managing security in IoT infrastructure is challenging due to its complexity and heterogeneity. As a result, developers have challenges in adhering to several hardware and software standards.

Recently, IoT frameworks and standards have emerged to help developers create solutions for diverse customer demands [10].

3.2. IoT Security

3.2.1. IoT Security Challenges

Define IoT Conventional security and privacy measures may be inadequate for IoT networks. The evolving characteristics of IoT connection present a novel array of security issues. The subsequent instances are as follows [11] [12]:

- Heterogeneity:

IoT aims to link a vast array of diverse devices to facilitate innovative applications

that enhance the quality of human existence. Consequently, IoT devices are available in several forms and sizes, leading to a varied array of hardware and software configurations.

- Volume:

In the IoT, a vast array of devices, specifically billions of smart gadgets, are interconnected, characterized by the substantial volume, velocity, and structure of real-world data.

- Interconnectivity:

The IoT denotes the interconnection of devices, encompassing the information they transmit and receive from one another, akin to a dialogue. Consequently, IoT networks may be accessed at any time and from any location.

- Structure and vulnerability:

IoT devices are susceptible to several forms of attacks, including cookie theft, cross-site scripting, structured query language injection, session hijacking, and frequently, distributed denial of service. In a substantial, self-organized IoT network, the susceptibility to distributed denial of service attacks often increases.

- Dynamism:

The ongoing addition and removal of IoT devices necessitates a dynamic and responsive network reconfiguration.

- Proximity:

In short-range communications, ad hoc networks may depend on nearby devices. Proximity refers to the ability of an IoT-enabled object to alter its behavior based on its current location.

- Latency and reliability:

The primary problems in industrial IoT networks are low latency and high dependability in wireless communication. Sensitive applications such as surgical instruments, assembly line production, and traffic monitoring necessitate highly dependable and low-latency connectivity.

- Expenditure, resource use, and energy consumption:

An IoT device is a physical component equipped with a sensor that transmits data from one location to another via the Internet. The systems must be structured to minimize resource requirements and expenses resulting from the extensive number of sensors in a complicated system application.

- Security and privacy safeguarding:

Consumer and proprietary data must be safeguarded and protected, especially in sensitive areas such as healthcare applications.

- Intelligent decision-making:

Numerous IoT applications necessitate those complex decisions be made intelligently, aligned with user preferences, and executed in real-time. While many of these difficulties are common across many Internet access points, the limitations of IoT devices, coupled with the dynamic and complex environments in which they function, exacerbate these concerns beyond the reach of conventional security measures.

3.2.2. IoT Security Threats

IoT has lately been integrated into a wide range of devices and applications, transforming the system from linear to rational. Because of its value, IoT utilization is rising on a daily basis. Although, IoT is also having a significant impact on medical science [13]. The healthcare monitoring system is being developed to guarantee that patients receive appropriate emergency assistance. Some health applications have already been created using IoT, such as computer-assisted rehabilitation, emergency notification, and continuous glucose monitoring. These software apps are designed to address various elements of medical difficulties.

IoT applications provide inherent security and privacy problems. Exploitation of IoT devices is posing major security and privacy risks, which have the ability to push IoT into an unpredictable future. As new IoT devices are added to networks, their internet connectivity allows malicious actors to access smart environments and continue in their malicious activities. Many IoT devices have known security flaws, making them vulnerable to attack. Poor privacy and security online can put people's life and health at risk from hostile cyber assaults [14].

However, there are many threats when integrating IoT technologies, such as information transmission between devices, data management, security, and privacy are the most critical problems that must be addressed initially. Cloud computing might be considered one of the most effective answers to all of these challenges and threats [4].

Cloud computing provides computer services such as software, databases, servers, data analytics, and networking via the Internet, allowing for speedier development, economies of scale, and flexible resources. Fog computing in edge devices incorporates data analytics, allowing for real-time processing, cost savings, and improved data privacy. The growth of cloud computing, artificial intelligence, and mobile technology provide an effective foundation for the evolution of the IoT-based devices [13].

Although, Jamming is a widely recognized threat that affects IoT networks. An attacker covertly impedes the network to occupy unneeded channels and hinder genuine communication, causing node issues with availability. An attacker may strategically jam a secondary user's transmission to limit bandwidth usage [9].

Spoofing is a common threat in IoT networks. Attackers send fake broadcast messages using spoofed Mac addresses or RFID tags. The initial networks mistakenly regard the communication as real. This situation is the most typical source of system vulnerability, posing risks to authenticity, integrity, and secrecy [9].

Data tampering threats in IoT commonly target sensitive information via unauthorized networks, causing disruptions or changes.

Security threats such as malware and ransomware may impede IoT development. Although, several security solutions are being developed to ensure the reliability of the IoT [10]. **Figure 1** and **Figure 2** present a summary of security and privacy threats [13].

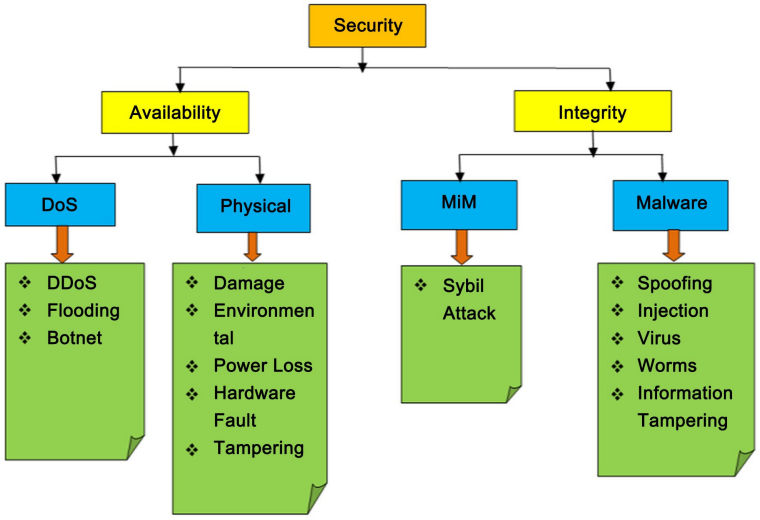

Figure 1. Security threats for IoT.

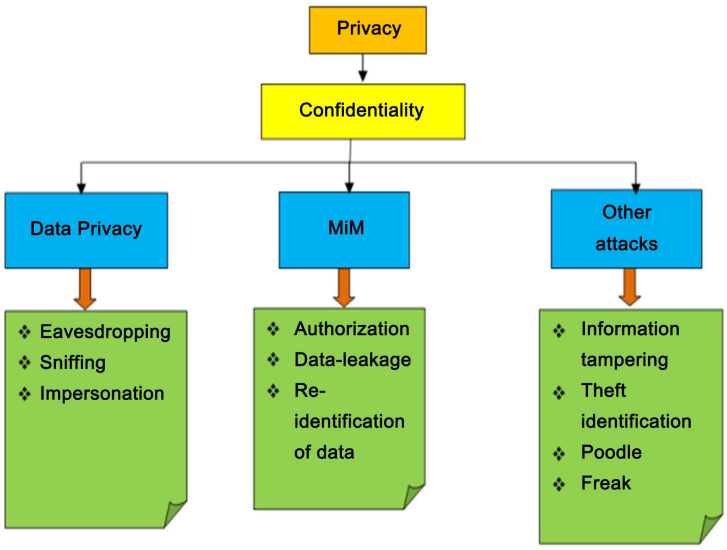

Figure 2. Privacy threats for IoT.

Reference [15] discussed the challenges that face IoT system designers, including the technical limitations of connected devices. They also proposed machine learning techniques to address common attack methods like denial of service (DoS), man-in-the-middle (MIM), and spoofing. The study suggests that machine learning may be useful in combating some threats and needs further investigation.

The fog computing approach has been proposed as an attempt to preserve IoT system data locally to improve security. However, this approach introduces new vulnerabilities, reducing potential security benefits. Fog computing reduces traffic to IoT core processing, but adds complexity for identification, data security, and user confidentiality [15].

The use of fog computing as a potential solution has prompted a wide range of study. The concept of "fog computing" relates to a computing system or architecture

that uses peers' entry nodes as intermediaries between devices for communication and cloud networks. Some studies emphasize peer-to-peer implementations, while others view fog computing as a layer in typical cloud computing infrastructures. Fog computing competes with cloud computing in IoT by offering comparable security benefits while overcoming hurdles like latency, bandwidth, and resource limits [8].

However, countermeasures for IoT threats must ensure the infrastructure's integrity, confidentiality, and availability. Implementing countermeasures might be challenging because to limitations in IoT devices like memory, processing, and battery. Countermeasures should not negatively impact the performance or usefulness of IoT devices, as they are often expected to function well. Intrusion detection and prevention systems can guard against common network assaults, including brute force, malware infection, and DDoS. A data protection system helps prevent data theft from IoT networks [16].

Moreover, to protect data integrity and avoid hacking threats, it's important to utilize standard encryption algorithms and protocols. Proper key management is also crucial to ensure the safety of IoT devices. Poor key management might compromise overall security [17].

4. Recent Trends and Challenges

This section highlights recent trends in IoT security, identifies inadequacies in the investigated research publications, and discusses the associated difficulties. That it will assist researchers in developing an efficient, scalable, resilient, and precise intrusion detection system for IoT devices to counter large-scale attacks.

IoT security trends can be summarized in the following points:

- Choosing the appropriate Intrusion Detection System (IDS) methodology

DDoS assaults, such as Mirai, remain a significant concern since their initial identification in 2016. By July 2019, 63 variations resembling Mirai were identified through the expansion of the attack surface and the utilization of diverse payloads. Identifying botnets is essential and necessitates a multi-faceted strategy to protect susceptible devices. A signature-based preventative methodology is prevalent in network intrusion detection systems and antivirus software. This method necessitates a knowledge database for the storage of existing attack signatures. This method is labor-intensive, necessitates continuous database upgrades for any newly identified malware, and disseminates new database changes across all applications [4].

- Scalable IDS solutions for the IoT

A more scalable method for detecting zero-day threats in the IoT context involves analyzing network packets with deep learning algorithms. Currently, cyber-attacks have evolved to be smart and complex, proliferating rapidly. Deep learning algorithms autonomously learn from historical assaults by scrutinizing available data and doing user behavior analysis to uncover concealed data patterns for the detection of harmful attacks. Due to the resource constraints of IoT devices

and the high computational demands of deep learning models, researchers have proposed offloading computational tasks to edge or fog nodes. A viable and secure IoT strategy must link to edge data centers. This will enhance security via the firewall, facilitate the training of complicated models, and improve intrusion detection systems, while also offering redundancy and failover advantages in the event of a significant cyberattack on a vital site [4].

- Choosing the appropriate dataset

The distinctive features of the IoT environment necessitate meticulous model development and training for intrusion detection. Likewise, resource constraints (reduced memory, processing capacity, energy, etc.) and the network traffic produced by IoT devices necessitate distinct solutions compared to traditional computing systems. Training machine learning and deep learning models on a dataset that is particular to the IoT and encompasses diverse attack flow is essential. Certain research examined in this work utilized legacy datasets that are not specific to IoT and are deficient in contemporary attack scenarios. Models constructed with unbalanced classes or limited attack labels require scrutiny, since their performance may be adversely impacted by these problems [11].

- Ongoing training and annotation

The development of an optimum machine learning and deep learning model relies on training the model using a benchmark dataset. When datasets are extensive, researchers train their machine learning models on a reduced dataset for performance enhancement. In the context of an IDS, this might occasionally result in a biased model if the training phase does not encompass all network traffic patterns. Although such models may initially yield superior performance measures, their deployment in a real-world setting would likely falter due to their inability to generalize patterns that have not been previously seen. Likewise, annotating the extensive dataset is a significant problem and is a labor-intensive endeavor. IDS models require ongoing training on novel network data to acquire new patterns and effectively categorize benign and malicious traffic [12].

- Combined/Ensemble Models

The integration of several machine learning and deep learning models to provide enhanced performance and attack detection is a notable research topic.

Researchers have demonstrated enhanced attack detection outcomes by integrating CNN or RNN with LSTM. Nevertheless, it introduces added complexity, increased training duration, and greater computational resources; for instance, some models such as CNN need data translation into a particular format before to integration with LSTM [16].

- Computational Complexity

The authors indicated that the computing requirements of deep learning models have escalated swiftly, outpacing the availability of specialized hardware and investment in requisite resources. This will rapidly become onerous, necessitating significant enhancements in the near future. Researchers indicated that the gradual enhancement of hardware performance, in contrast to the rapid advancement

of deep learning computer power, constrains the efficacy of deep learning models [17] [18].

5. Results and Discussion

IoT has expanded beyond industrial and commercial applications to include home appliances, hospitals, communications, energy control, and portable devices. When utilizing various technologies, it's crucial to prioritize safety. Since with the benefit comes the harm, and in the event of insecurity, it may return to us with security risks and threats, and hackers and manipulators may exploit vulnerabilities to gain access to data and information, manipulating and misusing it to make it work for them. It may be vulnerable to a variety of assaults, including interference and DOS, floods, black holes and wormholes, sinkhole and Sybil types. The security requirements shift from level to level as every single level satisfies a different need [2].

On the other hand, [19] presented mitigation recommendations for IoT threats. seventeen research papers examined authentication strategies to reduce vulnerabilities and assaults in IoT environments. Several research (ten) have employed encryption approaches to combat cybersecurity threats in the IoT environment. Six research utilized access control approaches, five used AI, a handful used Blockchain technology, and just a single paper utilized a digital signature.

Research on scalability connects with recommendations for standardization and security. Solutions including IPv6 for increased capacity of device connectivity have been proposed, but they have yet to appear as proof of concept with real effects beyond theory. The adaptability of the Internet of Things is an unsettled topic because to its reliance on standards and the rapid adoption of relevant technologies for consumer and industrial applications [8].

According to studies, authentication is the most effective mitigating mechanism for IoT threats. Some researchers have proposed AI to mitigate IoT threats that standard mitigation strategies cannot handle. A few pieces of IoT researches utilized blockchain technology to mitigate cybersecurity vulnerabilities and assaults [19]. This paper encourages future researches to focus on machine learning, AI, and blockchain mechanisms as approaches to mitigate the discussed security threats.

However, discussing security threats drives the need for standardized security protocols across IoT devices. This can lead to the development and implementation of industry-wide security standards and certifications.

IoT applications now face different security problems. There is currently no clear architecture or standard framework to guide an IoT application. An IoT application is a collaborative effort involving several persons and sectors, rather than a solitary product. Various items and technologies are employed across all layers, from sensing to application. Edge nodes hold several sensors and actuators. There are several communication protocols, including cellular networks, WiFi, IEEE 802.15.4, Insteon, dash7, and Bluetooth. A handshake mechanism is necessary

between all these standards [12].

In IoT applications, cost effectiveness, security, dependability, privacy, coverage, latency, and other factors must be considered due to the wide range of protocols, technologies, and devices. Optimizing one statistic for improvement may negatively impact another [19].

In [20] authors proposed a proactive defense framework that facilitates the best implementation of proactive defense in a software defined networking (SDN) based IoT environment. The employed approach has utilized the SDN architecture to enable adaptable deployment and seamless integration of protection measures. Through the utilization of moving target defense tactics and cyber deception, we have implemented protection systems that misdirect attackers, leading them to erroneous judgments and exhausting their resources with minimum effect on resources.

Reference [21] introduced an innovative method to improve IoT security by utilizing crowdsourced threat intelligence and incorporating blockchain technology with ML models. The collective threat data is securely maintained on a blockchain network, allowing ML models to access and derive insights from a variety of threat situations.

The use of blockchain technology has initiated a fundamental transformation in IoT security. A major impact is the improvement of data integrity. The unchangeable characteristic of the blockchain guarantees that data logged inside the IoT ecosystem remains intact, offering a reliable account of all operations. The significance of immutability is especially paramount in essential applications like healthcare and industrial control systems, where data integrity can result in life-or-death outcomes [21] [22].

Blockchain also resolves the problem of centralized data storage. mitigating the danger of a singular point of failure. Our private blockchain network, comprising IoT devices as nodes, disseminates data throughout the network, enhancing its resilience to assaults. Despite the breach of certain nodes, the system's integrity remains unblemished [23].

As mentioned before, in the context of IoT security, both cloud and fog computing offer distinct advantages and face unique challenges compared to traditional security methods. Cloud computing provides scalable and flexible resources, enabling efficient data storage and processing for IoT devices. This scalability allows for the implementation of comprehensive security measures, such as advanced encryption protocols and continuous monitoring systems, which can be more challenging to deploy in traditional, localized infrastructures. However, the centralized nature of cloud computing introduces potential vulnerabilities, including latency issues and data privacy concerns, as sensitive information is transmitted to and stored in centralized data centers. Additionally, the reliance on constant internet connectivity can be a limitation in scenarios where network access is intermittent or unreliable [24].

Fog computing addresses some of these challenges by extending computational resources closer to the edge of the network, near the IoT devices themselves. This

proximity reduces latency, allowing for real-time data processing and more immediate security responses, which are critical in applications such as autonomous vehicles or industrial automation. Moreover, by processing data locally, fog computing can enhance privacy and reduce the amount of sensitive information transmitted to central servers. However, this decentralized approach also presents challenges, including the need for robust security measures across a larger number of nodes, each potentially vulnerable to physical tampering or cyberattacks. Managing security in such a distributed environment requires sophisticated strategies to ensure consistency and resilience across the network [24].

Traditional security methods often rely on well-established perimeter defenses, such as firewalls and intrusion detection systems, designed for centralized networks. While effective in certain contexts, these approaches may not adequately address the dynamic and distributed nature of IoT ecosystems. The integration of cloud and fog computing into IoT security frameworks offers opportunities to enhance scalability, responsiveness, and data privacy. However, it also necessitates careful consideration of the associated challenges, including potential vulnerabilities introduced by increased complexity and the need for comprehensive management of distributed resources.

However, IoT provides significant advantages for businesses, but it also takes on several problems. Insufficient administration has been a difficulty for IoT-based applications. The issue is that developers prioritize gathering meaningful data from objects via sensors. They do not consider how data will be collected. Because of the ambiguity, attackers can obtain users' data and utilize it as needed. Developers must shift their attention to how they receive the data [25].

Users contribute private information to IoT apps. Consequently, privacy must be given. Privacy implies that the private data of users is protected and cannot be accessed by outsiders. Researchers have presented many strategies in research papers to promote security and privacy. These strategies have failed to provide confidentiality and security in IoT applications. Future research should address these main issues in IoT technology [26].

Operational issues are unavoidable as the variety of IoT devices expands and is deployed in various smart settings. In a setting wherein IoT gadgets and services are implemented, operational problems include those that might produce waste, deplete resources, influence the efficiency of operations, make a business unsuccessful, and limit growth [14].

6. Future Work

This paper highlights the challenges of dealing with threats, vulnerabilities, and attacks on IoT devices due to their resource constraints and inadequate security mechanisms. However, industry leaders are making progress to enhance the capabilities of even low-powered embedded SoCs and microprocessors. There is promise for improved IoT device security.

As a future work for this paper, there is a chance to expand the paper by

investigating promising remediation techniques such as Zero Trust Architectures, security-augmented architectural layers, the use of well-trained machine learning and deep learning models, cloud and edge computing solutions, and simply prioritizing security in general.

Establishing and carrying out IoT security controls is challenging due to the absence of standardized ways that can expand beyond traditional network needs for smart environments. To address existing and upcoming IoT security challenges, researchers and stakeholders should establish novel privacy standards and evaluation frameworks [14].

7. Conclusions

Security is crucial in practically all applications for IoT that have been or are currently being deployed. IoT applications are fast expanding and gaining traction in most established sectors. Although operators offer many IoT applications using current networking technologies, several of them require enhanced security from the technology they utilize [12].

IoT technologies provide additional hurdles to the Internet's inherently complicated security landscape. Managing the growing number of linked IoT devices is a huge task. The proliferation of IoT systems introduces new device classes, posing distinct issues that must be addressed. Some may be clear, whereas others might not be so [5].

Although, the IoT business is rapidly expanding, IoT security is a relatively new field. Cyberattacks aim to exploit vulnerabilities in IoT devices. Recognizing hazards from unsecured IoT devices, using them in certain settings, and implementing necessary security measures are the first steps towards addressing the issue [6].

This paper outlined the current security threats for IoT that guide researchers and developers in focusing on the most pressing issues, which can influence the design of more secure IoT systems and promote the adoption of best practices. As well, the primary objective of this work is to present a contemporary review of the prevailing research areas concerning IoT security, which highlights the recent trends in IoT security, identifies inadequacies in the investigated research publications, and discusses the associated difficulties. That will assist researchers in developing an efficient, scalable, resilient, and precise intrusion detection system for IoT devices to counter large-scale attacks. Also, it helps to identify gaps that still exist in the current body of knowledge on IoT security, indicating areas that future research could address.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Amoo, O.O., Osasona, F., Atadoga, A., Ayinla, B.S., Farayola, O.A. and Abrahams,

T.O. (2024) Cybersecurity Threats in the Age of IoT: A Review of Protective Measures. *International Journal of Science and Research Archive*, **11**, 1304-1310. https://doi.org/10.30574/ijsra.2024.11.1.0217

[2] Najmi, K.Y., AlZain, M.A., Masud, M., Jhanjhi, N.Z., Al-Amri, J. and Baz, M. (2023) A Survey on Security Threats and Countermeasures in IoT to Achieve Users Confidentiality and Reliability. *Materials Today*: *Proceedings*, **81**, 377-382. https://doi.org/10.1016/j.matpr.2021.03.417

[3] IEEE (2019) 2019 International Carnahan Conference on Security Technology (ICCST).

[4] Khan, Y., Su'ud, M.B.M., Alam, M.M., Ahmad, S.F., Salim, N.A. and Khan, N. (2022) Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. *Electronics*, **12**, Article No. 88. https://doi.org/10.3390/electronics12010088

[5] Wheelus, C. and Zhu, X. (2020) IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. *IoT*, **1**, 259-285. https://doi.org/10.3390/iot1020016

[6] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M. and Stiller, B. (2022) Landscape of IoT Security. *Computer Science Review*, **44**, Article ID: 100467. https://doi.org/10.1016/j.cosrev.2022.100467

[7] Harbi, Y., Aliouat, Z., Refoufi, A. and Harous, S. (2021) Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE Access*, **9**, 113292-113314. https://doi.org/10.1109/access.2021.3103725

[8] Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A. and Brown, J. (2020) A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers*, **9**, Article No. 44. https://doi.org/10.3390/computers9020044

[9] Zaman, S., Alhazmi, K., Aseeri, M.A., Ahmed, M.R., Khan, R.T., Kaiser, M.S., *et al.* (2021) Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. *IEEE Access*, **9**, 94668-94690. https://doi.org/10.1109/access.2021.3089681

[10] Riyaz Naik, S.M., Nazme, B. and Farooq, S.M. (2018) A Study on Internet of Things (IoT) & Its Security Issues. *International Journal of Research and Analytical Reviews*, **5**, 800-803.

[11] Sarker, I.H., Khan, A.I., Abushark, Y.B. and Alsolami, F. (2022) Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. *Mobile Networks and Applications*, **28**, 296-312. https://doi.org/10.1007/s11036-022-01937-3

[12] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019) A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, **7**, 82721-82743. https://doi.org/10.1109/access.2019.2924045

[13] Podder, P., Rubaiyat Hossain Mondal, M., Bharati, S. and Kumar Paul, P. (2021) Review on the Security Threats of Internet of Things. *International Journal of Computer Applications* (*IJCA*), **176**.

[14] Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R. (2021) A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, **9**, 121975-121995. https://doi.org/10.1109/access.2021.3109886

[15] Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I. and Guizani, M. (2020) A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys & Tutorials*, **22**, 1646-1685.

https://doi.org/10.1109/comst.2020.2988293

[16] Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A. (2019) IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, **6**, 8182-8201.

[17] Alizadehsani, R., Roshanzamir, M., Izadi, N.H., Gravina, R., Kabir, H.M.D., Nahavandi, D., *et al.* (2023) Swarm Intelligence in Internet of Medical Things: A Review. *Sensors*, **23**, Article No. 1466. https://doi.org/10.3390/s23031466

[18] Ahmad, R. and Alsmadi, I. (2021) Machine Learning Approaches to IoT Security: A Systematic Literature Review. *Internet of Things*, **14**, Article ID: 100365. https://doi.org/10.1016/j.iot.2021.100365

[19] Albalawi, A.M., Almaiah, D., Albalawi, A.M. and Amin Almaiah, M. (2022) Assessing and Reviewing of Cyber-Security Threats, Attacks, Mitigation Techniques in IoT Environment. *Journal of Theoretical and Applied Information Technology*, **100**, 2988-3011. https://www.researchgate.net/publication/360614150

[20] Rehman, Z., Gondal, I., Ge, M., Dong, H., Gregory, M. and Tari, Z. (2024) Proactive Defense Mechanism: Enhancing IoT Security through Diversity-Based Moving Target Defense and Cyber Deception. *Computers & Security*, **139**, Article ID: 103685. https://doi.org/10.1016/j.cose.2023.103685

[21] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., *et al.* (2024) Collaborative Threat Intelligence: Enhancing IoT Security through Blockchain and Machine Learning Integration. *Journal of King Saud University—Computer and Information Sciences*, **36**, Article ID: 101939. https://doi.org/10.1016/j.jksuci.2024.101939

[22] Harahsheh, K.M. and Chen, C. (2023) A Survey of Using Machine Learning in IoT Security and the Challenges Faced by Researchers. *Informatica*, **47**. https://doi.org/10.31449/inf.v47i6.4635

[23] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S. and Islam, S.M.R. (2024) A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. *Future Internet*, **16**, Article No. 40. https://doi.org/10.3390/fi16020040

[24] Singh, N., Buyya, R. and Kim, H. (2024) Securing Cloud-Based Internet of Things: Challenges and Mitigations. *Sensors*, **25**, Article No. 79. https://doi.org/10.3390/s25010079

[25] Aziz Al Kabir, M., Elmedany, W. and Sharif, M.S. (2023) Securing IoT Devices against Emerging Security Threats: Challenges and Mitigation Techniques. *Journal of Cyber Security Technology*, **7**, 199-223. https://doi.org/10.1080/23742917.2023.2228053

[26] Burhan, M., Rehman, R.A., Khan, B. and Kim, B. (2018) IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, **18**, Article No. 2796. https://doi.org/10.3390/s18092796