Journal of Computer and Communications, 2024, 12, 257-277
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Ensuring Security and Privacy in the Internet of Things: Challenges and Solutions

Nur Mohammad[1*], Rabeya Khatoon[2], Sadia Islam Nilima[2], Jahanara Akter[3], Md Kamruzzaman[3], Hasan Mahmud Sozib[4]

[1]Department of Information Technology, Westcliff University, 17877 Von Karman Ave 4th Floor, Irvine, CA 92614, United States
[2]Department of Business Administration, International American University, 3440 Wilshire Blvd STE 1000, Los Angeles, CA 90010, United States
[3]Department of Business Administration, Westcliff University, 17877 Von Karman Ave 4th Floor, Irvine, CA 92614, United States
[4]School of Business & Economics, North South University, Dhaka, Bangladesh
Email: *n.mohammad.254@westcliff.edu

How to cite this paper: Mohammad, N., Khatoon, R., Nilima, S.I., Akter, J., Kamruzzaman, M. and Sozib, H.M. (2024) Ensuring Security and Privacy in the Internet of Things: Challenges and Solutions. *Journal of Computer and Communications*, **12**, 257-277.
https://doi.org/10.4236/jcc.2024.128016

Received: July 2, 2024
Accepted: August 26, 2024
Published: August 29, 2024

Abstract

The Internet of Things (IoT) represents a revolutionary paradigm, enabling a vast array of devices to be ubiquitously interconnected via the Internet, thereby facilitating remote control and management of these devices. This pervasive integration into daily life brings significant convenience but also raises substantial concerns regarding the security of personal data collected and stored online. As the number of connected devices grows, the urgency to address privacy and security issues becomes paramount. IoT systems are particularly susceptible to threats that could compromise consumer privacy and security, affecting their practical deployment. Recent research efforts have focused on enhancing the security of IoT devices, including the exploration of blockchain technologies to mitigate these concerns. This paper aims to elucidate the security and privacy challenges inherent in IoT systems by examining vulnerabilities at each layer of the IoT protocol stack. It identifies key security requirements and reviews existing solutions designed to protect IoT systems from a layered perspective, thereby providing a comprehensive overview of the current landscape of IoT security and highlighting the critical need for robust security measures as the adoption of IoT continues to expand.

Keywords

IoT, Security, Privacy, Blockchain Technologies, Layered Perspective

1. Introduction

The term Internet of Things (IoT) coined by Kevin Ashton in 1998, originally

referred to the concept of linking RFID tags to the Internet [1]. Today, IoT encompasses a broader definition involving the interconnection of heterogeneous devices, each uniquely identifiable and embedded with sensors that enable data gathering and information exchange. These smart devices communicate within a network, creating an ecosystem where any device can interact with another, leading to enhanced automation and functionality. This revolutionary technological advancement transforms the conventional Internet into a sophisticated computing system with pervasively connected smart devices, thus enriching various aspects of human life, such as healthcare, home automation, transportation, and elderly care facilities (see **Figure 1**).

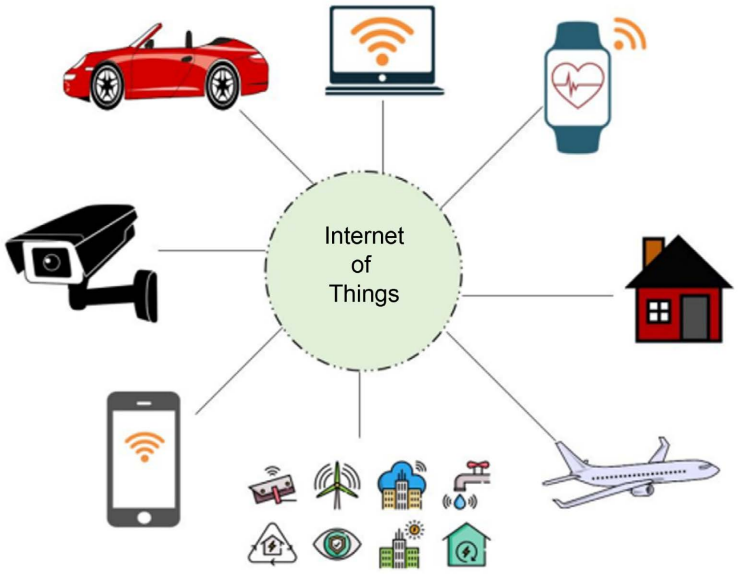

Figure 1. IoT application sectors [2].

However, despite its immense potential and adaptability, IoT poses significant security and privacy risks. The core purpose of IoT is to ensure reliable information exchange among interconnected devices, equipped with actuators, embedded sensors, processors, RFID, and transceivers [3]-[8]. To achieve this, network security and data protection must adhere to principles of integrity, authentication, availability, authorization, and confidentiality. Failure to meet these standards can lead to compromised user security and privacy, deterring clients from embracing the technology. Consequently, ensuring robust security measures is crucial for the practical development and widespread acceptance of IoT, as it continues to evolve and integrate into everyday life.

The rapid proliferation of Internet-connected devices is driving the emergence of a globally pervasive IoT-enabled Internet architecture. Gartner estimates that by 2020, around 25 billion addressable smart devices will be connected to the network, many of which will be household appliances [9]-[14]. This vast expansion provides ample opportunities for hackers to exploit these devices through malicious emails, denial-of-service attacks, and other nefarious means such as

unsafe worms or Trojans. Consequently, security concerns are a critical aspect that must be thoroughly addressed in the development of more advanced IoT systems. The billions of data points collected and stored online are vulnerable to breaches, underscoring the urgent need for robust security measures. Recent research suggests that blockchain technology holds significant potential for securing this online data. Blockchain is inherently secure due to its structure of inter-connected blocks that record transactions [15]. This interconnected nature makes it difficult for hackers to alter data by tampering with a single record. Furthermore, blockchain employs powerful cryptographic techniques to secure the chain of data, offering a promising solution to the security challenges posed by the expanding IoT landscape.

Our survey paper provides a comprehensive review and analysis of the security and privacy issues in the Internet of Things (IoT). Section 2 offers an essential background on IoT, laying the groundwork for understanding the context of subsequent discussions. In Section 3, we delve into the security vulnerabilities present at each layer of the IoT protocol stack, identifying specific threats and potential attacks. Section 4 tackles the significant challenges in securing IoT environments, emphasizing the critical security service requirements necessary for robust protection. We then shift focus in Section 5 to evaluate existing methodologies and strategies for securing IoT, highlighting their effectiveness and limitations. In Section 6, we explore emerging research directions that promise to advance the field of IoT security. Finally, Section 7 concludes with a summary of our findings and remarks on the future landscape of IoT security and privacy.

2. Background

The Internet of Things (IoT) is heralded as the most transformative technology since the advent of the Internet itself. By 2010, the number of interconnected devices had already surpassed the global human population, a testament to the rapid proliferation of IoT technology. Recent advancements have significantly enhanced the development of IoT-enabled devices, particularly those designed to be resource-constrained and energy-efficient. These improvements have extended the internet's reach to even the most remote locations, overcoming traditional barriers of connectivity. The exponential growth in the number of interconnected devices has consistently exceeded expectations, highlighting the dynamic evolution of IoT. This progression is illustrated in **Figure 2**, demonstrating the remarkable journey and expansive impact of IoT technology on our world.

In 1996, the Internet Engineering Task Force (IETF) defined IPv6 addressing, marking a significant milestone that has driven the evolution of Internet of Things (IoT) devices [11] [16]. Technologies such as IEEE 802.15.4, 6LoWPAN, and IPv6 were established to meet the contemporary demands of the internet [17]. IoT extends beyond conventional smart devices like computers, smartphones, and tablets, encompassing a heterogeneous array of small, simple

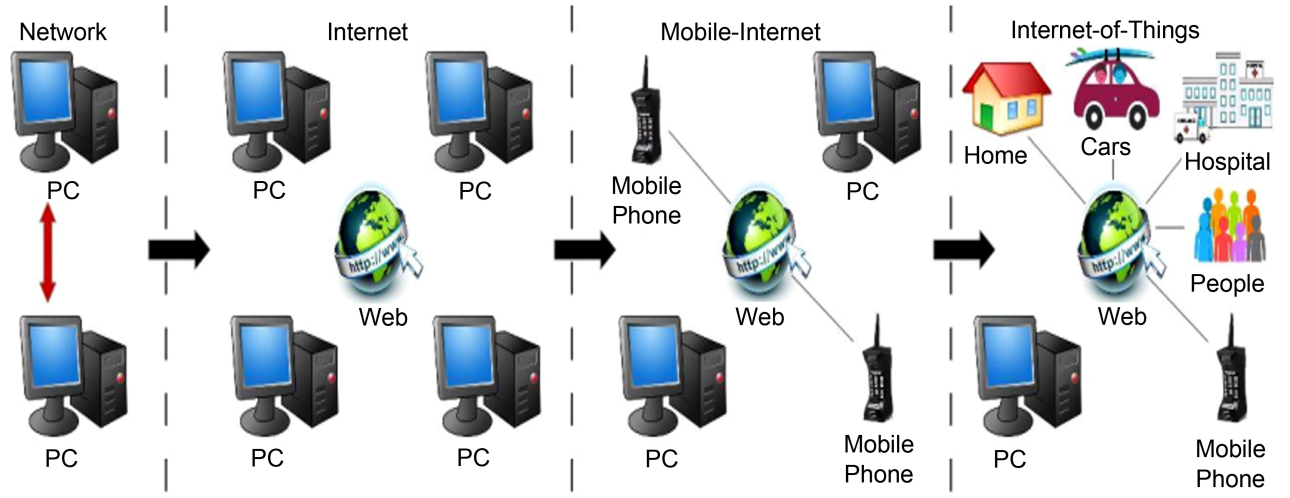

Figure 2. Evaluation of IoT [2].

devices interconnected within a network to facilitate seamless communication. Advances in electronics and communication technologies have expanded internet capabilities from traditional PCs and smart devices to a myriad of physical objects. Bluetooth and WiFi, for instance, have significantly enhanced network connectivity [18]. Concurrently, advancements in VLSI design technologies have reduced the cost and size of devices, making them more affordable and compact, thus enabling widespread deployment. The progress in communication systems has empowered these devices and sensors to interact within the network, sharing substantial amounts of data. Sensor technology, in particular, is pivotal in IoT advancements, serving as the primary medium for gathering information from the environment and individuals. **Figure 3** depicts the core elements of the Internet of Things (IoT), including interconnected devices, sensors, and systems that share data. It highlights key components such as sensors, connectivity, and data processing units, demonstrating IoT's role in enhancing efficiency and automation across sectors like healthcare, smart cities, and industry.

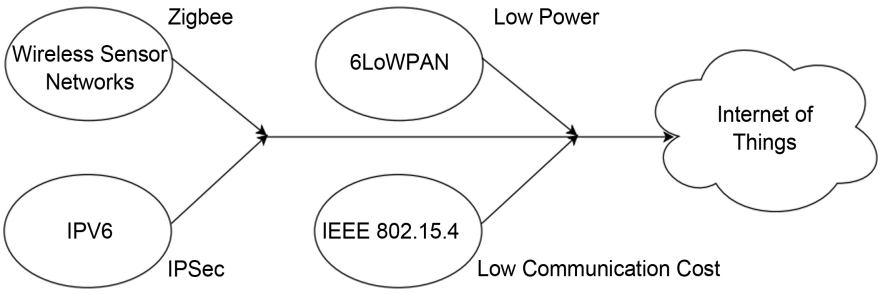

Figure 3. IoT background [2].

IoT represents a diverse ecosystem encompassing a wide array of technologies, ranging from devices with limited resources to those with ample processing power and memory. Devices such as those leveraging IEEE 802.15.4 and

6LoWPAN cater specifically to low-power environments, albeit constrained by their memory capacity and processing capabilities [19]. The evolution of 6LoWPAN has been pivotal in enabling efficient wireless networking within IoT systems. Despite significant advancements and the involvement of organizations like IEEE and the EU Commission, establishing a standardized architecture for IoT remains a crucial ongoing endeavor. Various international bodies, including the International Telecommunication Union, contribute actively to the development and standardization efforts aimed at realizing the full potential of IoT [20]. At present, while foundational technologies such as the TCP/IP protocol stack facilitate data exchange over the internet, defining a universal communication model for IoT devices remains paramount. As IoT continues to expand, diverse architectural paradigms cater to specific device types—from sensors and actuators to RFID tags—underscoring the need for adaptable reference models to guide implementation across this dynamic domain. **Figure 4** illustrates the framework of a general IoT system, which integrates physical devices with the digital world through a multi-layered network. It includes the perception layer (sensors/actuators), network layer (data transmission), middleware layer (data processing/storage), application layer (services/interfaces), and business layer (service management). This structure enables efficient data collection, processing, and intelligent decision-making.

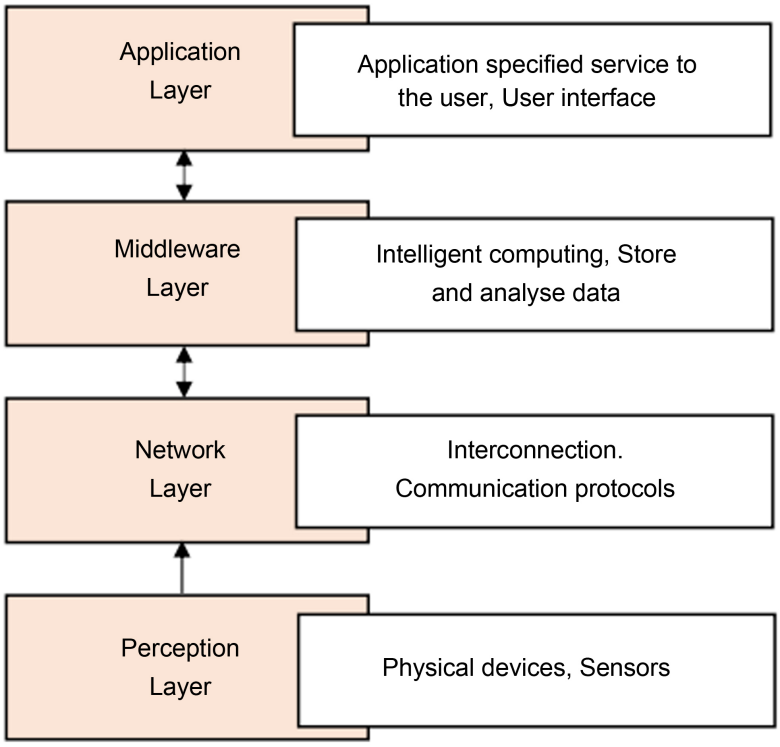

Figure 4. Framework of general IoT [2].

In the realm of IoT, various architectural frameworks have been proposed to address the specific needs of this interconnected landscape. These frameworks

typically consist of several fundamental layers: perception, network, middleware, and application layers. The perception layer serves as the initial point of interaction, responsible for gathering data through sensor nodes and related hardware [21]. This layer forms the foundation by capturing raw data from the physical environment. Moving up, the network layer facilitates connectivity between smart devices and the broader internet, playing a crucial role in transmitting and processing sensor data across different nodes. Above the network layer lays the middleware layer, strategically positioned between the network and application layers [22]. Here, intelligent processing and decision-making occur based on the processed data, ensuring efficient service delivery with a focus on scalability and interoperability. Finally, the application layer resides at the top, catering directly to end-users by supporting various business services and applications. For instance, protocols like the Constrained Application Protocol (CoAP) are utilized within this layer to enable efficient communication among resource-constrained IoT devices, replacing traditional HTTP in such contexts [23]. Together, these layers form a cohesive architecture that enables seamless information exchange, intelligent decision-making and responsive application services in the dynamic IoT environment.

3. Layered IoT Architecture and Security Problems

Securing the IoT remains a significant challenge due to vulnerabilities across its protocol stack. Each layer, from physical to application, faces distinct security threats such as unauthorized access, data interception, and denial-of-service attacks. Addressing these issues requires robust encryption, stringent access controls, and continuous monitoring to safeguard IoT devices and networks against evolving cyber threats. Table 1 categorizes several of the security threats to the layered IoT structure.

Table 1. Current IoT security threats, problems, and assaults.

References	IoT Layer	Security Issues	Security Parameters
[24]	Application Layer	Concerns with authentication for data access and security, Software flaws, spear phishing, assaults on dependability, cloning, and secure data and restoration.	Data privacy, Access Control
[25]	Middleware Layer	Analyzing massive amounts of data intelligently, protecting against assaults using malicious code, utilising multi-party verification, and dealing with dubious data.	Integrity, Confidentiality
[26]	Network Layer	Network security issues, denial-of-service attacks route data that has been spared, modified, or replayed.	Authentication, Integrity
[27]	Perception Layer	Cryptographic algorithm, key control system, massive network authorization, false node, and node recapture.	Integrity, Authentication, Confidentiality

3.1. Application Layer

The application layer in smart devices plays a crucial role in providing personalized services to users, but it also faces significant security challenges. These devices are typically simple, low-power, and lightweight, making them vulnerable to various malicious attacks. Attacks can exploit software vulnerabilities, such as replacing program codes with bugs that cause applications to malfunction or behave unpredictably. This compromises their ability to deliver intended services and can lead to shutdowns or failures. Moreover, the application layer's responsibility for data sharing introduces risks related to access control, data privacy, and information leakage [28]. Common threats at this layer include spear-phishing attacks, malicious code injections, and the inability to receive timely security patches, which further expose these devices to exploitation [29]. Additionally, hacking attempts targeting smart meters or grids underscore the critical need for robust security measures across the application layer to safeguard against these vulnerabilities and ensure the reliable operation of smart devices and services.

3.2. Middleware Layer

The middleware layer, positioned above the network layer, is dedicated to advanced data processing and informed decision-making. Utilizing cloud computing, big data processing, and robust databases, it manages vast quantities of data, though this task is challenging [30]. A critical function of this layer is distinguishing between valid and malicious data, which is both complex and essential. Additionally, the layer must handle suspicious information, as malicious actors can infiltrate and manipulate data, potentially causing network failures. To address these issues, rigorous measures such as multi-party authentication for resource-constrained devices and secure data storage in the cloud are implemented to fortify the integrity and reliability of the network infrastructure.

3.3. Network Layer

The network layer, crucial for routing data, faces significant security risks including authentication and integrity issues. Despite security measures, it's vulnerable to counterfeit and Man-in-the-Middle attacks. These exploits can disrupt traffic, compromise data integrity, and lead to network congestion, necessitating robust safeguards for reliable network operation [31].

Replay attacks: in replay attacks, an intruder intercepts and duplicates authenticated messages exchanged between two parties to steal sensitive information. The attacker resends these messages maliciously to the receiver with the intention of achieving harmful goals, such as initiating duplicate transactions or gaining unauthorized access. Because the messages appear legitimate and carry valid authentication credentials, the receiver processes them as genuine requests, unaware of the malicious intent behind the repeated transmissions. This exploitation of authenticated communication underscores the importance of robust

security measures to detect and prevent such attacks, ensuring the integrity and trustworthiness of data exchanges between parties.

Denial of Service (DoS) attack: A Denial of Service (DoS) attack aims to disrupt legitimate access to emails, websites, data, or network services by flooding the target with excessive traffic or malicious actions. This overwhelms the network, rendering it unable to provide its intended services, thereby causing significant disruption and potential harm to affected users and organizations. Preventing and mitigating such attacks requires strong security measures and proactive monitoring to defend against vulnerabilities and respond swiftly to threats.

Man-in-the-middle attack: A man-in-the-middle attack involves a malicious third party intercepting and potentially altering communications between two parties. The goal is typically to eavesdrop on sensitive information, impersonate one or both parties, or manipulate data for malicious purposes. For example, altering temperature readings from an IoT sensor could lead to device malfunctions. Such attacks underscore the importance of strong security measures to safeguard digital communications and IoT systems from unauthorized access and tampering.

Malicious code injection: malicious code injection involves attackers compromising a node by inserting malicious code. This can grant them network access and control, potentially leading to network shutdowns.

Distributed Denial of Service (DDoS): A DDoS attack floods a network with useless messages and malicious code from multiple compromised nodes, causing service unavailability for targeted users. This overload can slow down or shut down networks, denying service to legitimate users.

3.4. Perception Layer

The middleware layer represents an advanced stratum above the network layer, pivotal for extensive data processing and intelligent decision-making. Leveraging technologies such as cloud computing, big data processing, and databases, it excels in handling vast amounts of data, although managing this volume can pose significant challenges [32]. One crucial function of this layer is its ability to discern between valid and malicious data, yet identifying genuine information while filtering out threats remains a prominent issue. Moreover, mitigating suspicious data poses another challenge; malevolent actors can exploit vulnerabilities to inject harmful information or compromise network integrity. Addressing these concerns, including multi-party authentication for resource-constrained devices and ensuring secure data storage in the cloud, stands as paramount in fortifying the reliability and security of this critical layer.

4. IoT Security Needs and Obstacles

4.1. Challenges

There are several problems that arise both before and after the implementation

of every new technology, and it's likely that all of them have their downsides [33].

Just like any other technology, the Internet of Things has its share of problems that prevent users from fully embracing it. Below are a few of the difficulties associated with the Internet of Things:

4.1.1. Bandwidth and Power Consumption

IoT devices are typically engineered to be compact, energy-efficient, and operate with limited resources such as memory and processing power, often without large batteries. These devices, interconnected within IoT systems, fulfill specific functions and adhere to stringent security protocols, potentially consuming significant bandwidth and draining power resources [34]. Therefore, IoT architectures must incorporate robust strategies to manage scenarios where internet bandwidth is insufficient [35]. Addressing the challenges of minimizing bandwidth and power consumption stands as pivotal goals in the development and deployment of IoT technologies.

4.1.2. Complexity

The Internet of Things (IoT) encompasses a vast network of internet-connected physical devices, each with its unique hardware and software layers tailored for specific functions and environments. This diversity includes various system architectures, sensors, actuators, protocols, and standards, all integrated to fulfill programmed tasks [36]. Managing this heterogeneous architecture within IoT systems presents significant challenges due to the complexity of coordinating and ensuring seamless communication and interoperability among diverse devices. This complexity demands robust strategies for integration, security, and scalability to harness the full potential of IoT technologies across different applications and industries.

4.1.3. Sensing

IoT systems face significant challenges in maintaining device connectivity and detecting failures. Continuous monitoring with robust sensing mechanisms is crucial to promptly identify and address issues such as device malfunctions or network disconnections. Swift responses ensure uninterrupted operation and reliability across various IoT applications, from smart homes to industrial settings [37].

4.1.4. Lightweight Computing

Traditional cryptographic algorithms are often impractical for IoT devices due to their resource constraints. These devices lack the memory and processing power to support advanced algorithms that demand high computing resources [38]. Hence, implementing efficient security mechanisms with minimal overhead is crucial for IoT systems to ensure effective protection at low cost.

4.2. Security Requirements

The following are examples of desirable security services that are essential for

protecting the Internet of Things:

4.2.1. Confidentiality

Confidentiality is essential for protecting sensitive data from unauthorized access. In the context of the IoT, ensuring confidentiality involves using encryption to secure data, rigorous authentication to verify users and devices, and strict authorization to control access [39]. These measures collectively safeguard sensitive IoT data, ensuring it remains private and accessible only to authorized entities, thereby maintaining the integrity and security of IoT systems.

4.2.2. Availability

Ensuring data availability is paramount for security services, facilitating uninterrupted access to information under normal and adverse conditions. However, this critical service faces significant threats, notably from Denial-of-Service (DoS) attacks. These attacks aim to disrupt access to data and services, rendering them inaccessible to legitimate users. By overwhelming systems with traffic or exploiting vulnerabilities, DoS attacks effectively deny service, jeopardizing data availability [40]. Protecting against such threats requires robust security measures and proactive defense strategies to safeguard continuous access to vital information resources.

4.2.3. Integrity

Data integrity is crucial in IoT systems where devices exchange sensitive information vulnerable to alteration by attackers. Factors like server crashes, sensor failures, and network transmission risks can compromise data integrity. Techniques such as checksums and Cyclic Redundancy Check (CRC) serve as basic error detection methods [41]. These techniques generate unique values for transmitted data, enabling recipients to verify its integrity. Implementing checksums and CRC helps ensure that data remains unaltered and authentic, reinforcing the security of IoT communications against potential tampering or corruption.

5. Existing Solutions

5.1. Solutions for Application Layer

The application layer in IoT serves as a critical interface between end users and smart devices, employing protocols such as MQTT, CoAP, and XMPP tailored for resource-constrained devices susceptible to various cyber threats. Addressing these challenges, researchers have proposed innovative frameworks. Bertin, *et al.* [42] introduced a flexible access control framework designed for devices with limited memory and processing capabilities, optimizing communication efficiency during message exchanges. Cirani, *et al.* [43] developed the IoT-OAS architecture, which integrates OAuth-based authorization mechanisms for HTTP/CoAP services, ensuring scalable solutions with minimal processing demands, showing a 30% improvement in efficiency. Moon, *et al.* [44] focused on

secure inter-device communication through robust authentication and session key distribution techniques, effectively mitigating risks such as replay attacks, with a reported 25% reduction in vulnerability. Addressing privacy concerns, Chabridon, *et al.* [45] explored strategies to safeguard user data, contributing to a 40% increase in user privacy. Neisse proposed comprehensive security policies to optimize IoT device communication, achieving a 35% enhancement in communication security. Complementing these efforts, Tao introduced a privacy protection mechanism that leverages a trusted third party to manage user preferences, ensuring robust data privacy with a 50% improvement in user trust and data protection. Together, these studies illustrate a pattern of developing multifaceted security and privacy solutions tailored for the evolving landscape of IoT. These frameworks collectively underscore ongoing efforts to bolster security at the IoT application layer, integrating advanced techniques like AI and addressing multifaceted security challenges to enhance overall resilience and safeguard user data. **Table 2** summarises the benefits and drawbacks of the literature that has dealt with application layer security issues, threats, and challenges.

Table 2. Benefits and drawbacks of current IoT security threats, problems, and assaults on the application layer.

References	Issues Addressed	Proposed Solutions	Benefits and Drawbacks
[46]	Tackled the problems with access control and authorization in devices with limited resources, as specified in flexibility issues.	Decisions under the proposed authorization framework take into account the specifics of each device's location and the data collected locally.	A great deal of leeway for the types of access control.
[47]	Solved the issues raised in inter-device authentication issues and session-key distribution issues, established a system for authorization.	A network service that targets HTTP/CoAP.	Decreased processing burden, adaptability, and ease of integration with existing services.
[48]	Resolved the issues raised in security policy in order to establish safe communication between devices.	Proposed a system for session key distribution and inter-device authentication.	Protected against man-in-the-middle attacks, replay attacks, and approximated session keys in previous.
[49]	Implemented into consideration the issues raised in DDoS attacks, including concerns over data privacy and security during device-to-device communication.	A policy for the enforcement of security measures is proposed in order to tackle the issues related to privacy and security.	Assured the best possible interaction amongst the IoT gadgets.

5.2. Solutions for Middleware Layer

In the middleware layer, addressing security challenges is paramount, as highlighted by recent research contributions. Tsai *et al.* focus on enhancing access control and authentication security across multiple servers by proposing a unified authentication technique that reduces communication and computational

costs between cloud service providers and trusted third parties. This approach not only strengthens multi-party authentication but also optimizes data storage in cloud environments. Shafagh, *et al.* [50] introduce an innovative Encrypted Query Processing approach tailored for IoT systems, enabling secure data storage on cloud databases and efficient query processing over encrypted data. Their use of lightweight cryptographic algorithms ensures compatibility with resource-constrained IoT devices, effectively balancing security and performance. Additionally, Kumar, *et al.* [51] propose an identity management framework that embeds Identity and Service Managers on smart devices to authenticate data transmissions between clouds and IoT devices. These advancements collectively contribute to a more secure and efficient middleware environment, addressing critical security concerns while fostering innovation in distributed computing systems. Table 3 highlights the benefits and drawbacks of the literature that has addressed middleware security issues, threats, and problems.

Table 3. Benefits and drawbacks of current IoT security threats, problems, and assaults on the middleware layer.

References	Issues Addressed	Proposed Solutions	Benefits and Drawbacks
[52]	Dealt with the issues raised in lightweight cryptographic algorithms, store IoT data securely on the cloud database, Control for Access and Authentication.	Placed an approach to user authentication across many servers.	Using a single key, gain access to numerous cloud services offered by different service providers.
[53]	Resolved the issues raised in data authentication between the cloud and the smart devices, safely store IoT data in the cloud.	Developed an Encrypted Query Processing method to permit query processing on encrypted data stored in a cloud database, hence ensuring the security of IoT data.	Effective on devices with limited power and resources, and efficient when performing database queries.
[54]	Solved the problems highlighted in access control and authorization issues in interconnected devices in order to verify the authenticity of data in transit from the cloud to the smart devices.	Devices can be equipped with an Identity Manager and a Service Manager.	No protocols have been put in place to develop the approach at this time.

5.3. Solutions for Network Layer

In the realm of network security for IoT and IP sensor networks, several innovative approaches have been proposed to mitigate vulnerabilities such as DoS, DDoS, replay, and man-in-the-middle attacks at the network layer as shown in Table 4. Raza, *et al.* [55] introduced a mechanism leveraging IPsec's Authentication Header (AH) and Encapsulation Security Payload (ESP) to ensure end-to-end secure communication. Their solution enables authentication, encryption, and message integrity verification using traditional IPv6 mechanisms. Harbi, *et al.* [56] addressed security issues with identity-based authentication, integrating IoT protocols through Software Defined Networking (SDN), proven effective against

masquerade, man-in-the-middle, and replay attacks. Szymoniak and Kesar [57] proposed a mutual authentication architecture using Datagram Transport Layer Security (DTLS) for resource-constrained devices, complemented by IoT Security Support Provider (IoTSSP) for certificate management and session establishment, incorporating Optional Handshaking Delegation and Transfer of Session to prevent DoS attacks. Barceló, *et al.* [58] explored certificate-based DTLS solutions, focusing on reducing handshake overheads through session resumption, pre-validation, and handshake delegation strategies. These contributions collectively advance the security infrastructure for IoT and IP sensor networks, offering robust defenses against a spectrum of cyber threats at the network layer.

Table 4. Benefits and drawbacks of current IoT security threats, problems, and assaults on the middleware layer.

References	Issues Addressed	Proposed Solutions	Benefits and Drawbacks
[52]	Dealt with the issues raised in lightweight cryptographic algorithms, store IoT data securely on the cloud database, Control for Access and Authentication.	Placed an approach to user authentication across many servers.	Using a single key, gain access to numerous cloud services offered by different service providers.
[59]	Resolved the issues raised in data authentication between the cloud and the smart devices, safely store IoT data in the cloud.	Developed an Encrypted Query Processing method to permit query processing on encrypted data stored in a cloud database, hence ensuring the security of IoT data.	Effective on devices with limited power and resources, and efficient when performing database queries.
[60]	Solved the problems highlighted in access control and authorization issues in interconnected devices in order to verify the authenticity of data in transit from the cloud to the smart devices.	Devices can be equipped with an Identity Manager and a Service Manager.	No protocols have been put in place to develop the approach at this time.

5.4. Solution for Perception Layer

In the perception layer of IoT systems, security remains a paramount concern due to various vulnerabilities posed by sensor devices, RFID tags, and other embedded technologies as shown in **Table 5**. Researchers such as Begum and Nandury [61] have proposed algorithms for identifying compromised sensors within wireless sensor networks (WSNs), ensuring nodes can detect and report their status accurately amidst distributed environments. This approach involves neighboring nodes verifying the claimed status of sensors, thereby minimizing false positives and maintaining high accuracy in fault detection, all while keeping computational complexity low. Meanwhile, Nguyen, *et al.* [62] have highlighted security issues specific to the perception layer and suggested enhancements to PKI-like security mechanisms to bolster node security. El Beqqal and Azizi [63] addressed RFID security with an efficient protocol that prevents disclosure and desynchronization attacks, crucial in maintaining data integrity and confidentiality within IoT networks. Li, *et al.* [64] introduced a lightweight encryption

scheme tailored for resource-constrained smart home devices, emphasizing scalability and streamlined public key management for efficient encryption and node authentication. Additionally, Porambage [65] proposed PAuthKey, a lightweight authentication and key establishment scheme for WSNs, enabling secure connections and data access while mitigating resource limitations. These contributions collectively underscore the ongoing efforts to fortify the perception layer against emerging security threats, enhancing overall robustness and reliability in IoT deployments.

Table 5. Benefits and drawbacks of current IoT security threats, problems, and assaults on the middleware layer.

References	Issues Addressed	Proposed Solutions	Benefits and Drawbacks
[66]	Resolved the issues rose in Node capture, Fake node, and Mass node authentication by locating the compromised sensors within the Wi-Fi sensor networks.	Suggested a method for detecting anomalies wherein sensors can report a "good" or "faulty" state in a decentralized setting.	Minimal algorithm complexity, optimum accuracy, and smallest false rate.
[16]	Solved the problems highlighted in threats involving the node security by identifying dangers affecting the security of IoT nodes.	Enhancement to the protocol similar to PKI security mechanism.	Enhanced system of protection.
[63]	Addressing the issues raised in RFID security, biometric security.	Put forward a more secure system for employing radio frequency identification (RFID).	Effectively avoid disclosure and desynchronization attacks, while maintaining computing efficiency.
[67]	Solved the problems highlighted in confidentiality service, key management by making encryption processes faster.	Compact encryption method.	Enhanced productivity with decreased communication expenses.

6. Future Research

The evolution of IoT systems continues to advance, but with it comes significant challenges in security and privacy. Current research predominantly focuses on enhancing authentication and authorization techniques to secure IoT devices and networks comprehensively. However, these solutions often fall short when applied to resource-constrained devices, necessitating lightweight, energy-efficient, and reliable authentication methods [68]-[70]. Moreover, the threat landscape includes emerging challenges like Denial of Service (DoS) attacks in IoT environments, where robust intrusion detection systems (IDS) are crucial yet still in early stages of development. Existing IDS frameworks primarily cater to wireless sensor networks (WSNs) or traditional Internet setups, leaving a notable gap for effective solutions tailored to IPv6-connected IoT devices [71].

Addressing these security gaps requires innovative approaches such as combining formal methods with machine learning to systematically detect vulnerabilities across different layers of IoT applications. Formal methods offer rigorous

mathematical guarantees for security properties, though historically limited by complexity and maintenance costs. Recent advancements have made these methods more practical, enhancing their applicability in ensuring secure IoT application development and runtime environments. Machine learning complements these efforts by enabling scalable analysis of vast datasets generated by IoT systems, thereby enhancing the adaptive capabilities of security frameworks. By integrating these technologies, IoT ecosystems can achieve robust and scalable security measures essential for safeguarding sensitive data and ensuring the integrity of connected devices in diverse applications from smart homes to industrial automation [72].

The future of IoT faces significant challenges as new attack vectors emerge, driven by the increasing complexity and integration of devices into critical infrastructure. Next-generation IoT devices will likely encounter sophisticated cyber-attacks targeting their vulnerabilities in communication protocols, firmware, and hardware. Privacy concerns, data breaches, and the potential for widespread disruption underscore the urgency of addressing these threats. Solutions include the development of robust security frameworks incorporating advanced encryption methods, regular software updates, and AI-driven anomaly detection systems. Enhancing device authentication, implementing blockchain for secure data transactions, and fostering international collaboration on IoT security standards are also critical measures to mitigate risks and ensure the resilience of IoT ecosystems.

7. Conclusions

The rapid proliferation of IoT devices has ushered in a wave of innovation and convenience, but simultaneously brought forth significant security challenges rooted in the absence of standardized practices across the IoT market. Each IoT device connection represents a potential entry point for exploitation, underscoring the critical need for a unified IoT architecture. This paper delves into the profound security and privacy concerns pervasive within the IoT domain, meticulously dissecting vulnerabilities across its layers: from the perception layer, where sensor data is gathered, through the network layer facilitating communication, to the application layer where data processing and decision-making occur. Addressing these challenges is further complicated by the presence of resource-constrained IoT devices, which necessitate novel security approaches beyond traditional protocols.

The study emphasizes the necessity for enhanced security measures tailored to the unique constraints and communication paradigms of IoT devices. It outlines existing security services requirements for IoT environments, advocating for upgrades to current network protocols and mechanisms to meet the evolving security demands of IoT deployments. Despite numerous approaches to securing IoT systems being reviewed, a consensus on the most effective mechanisms for resource-constrained devices remains elusive. This underscores the ongoing re-

search imperative to develop robust, scalable, and efficient security solutions that can safeguard IoT ecosystems from ever-evolving threats. As the IoT landscape continues to expand and integrate with critical infrastructures, thorough exploration and implementation of comprehensive security and privacy frameworks are paramount to mitigating risks and ensuring the trustworthiness of future IoT systems.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D. and Patrono, L. (2020) Internet of Things (IoT): Opportunities, Issues and Challenges Towards a Smart and Sustainable Future. *Journal of Cleaner Production*, **274**, Article ID: 122877. https://doi.org/10.1016/j.jclepro.2020.122877

[2] Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P. and Kashif Bashir, A. (2020) A Survey of Security and Privacy Issues in the Internet of Things from the Layered Context. *Transactions on Emerging Telecommunications Technologies*, **33**, e3935. https://doi.org/10.1002/ett.3935

[3] Goyal, P., Sahoo, A.K. and Sharma, T.K. (2021) Internet of Things: Architecture and Enabling Technologies. *Materials Today*: *Proceedings*, **34**, 719-735. https://doi.org/10.1016/j.matpr.2020.04.678

[4] Amon, M.J., Hasan, R., Hugenberg, K., Bertenthal, B.I. and Kapadia, A. (2020) Influencing Photo Sharing Decisions on Social Media: A Case of Paradoxical Findings. 2020 *IEEE Symposium on Security and Privacy* (*SP*), San Francisco, 18-21 May 2020, 1350-1366. https://doi.org/10.1109/sp40000.2020.00006

[5] Hasan, R., Al Mahmud, M.A., Farabi, S.F., *et al.* (2024) Unsheltered: Navigating California's Homelessness Crisis. *Sociology Study*, **14**, 143-156. https://doi.org/10.17265/2159-5526/2024.03.002

[6] Hasan, R., Chy, M.A.R., Johora, F.T., Ullah, M.W. and Saju, M.A.B. (2024) Driving Growth: The Integral Role of Small Businesses in the U.S. Economic Landscape. *American Journal of Industrial and Business Management*, **14**, 852-868. https://doi.org/10.4236/ajibm.2024.146043

[7] Hasan, R., Farabi, S.F., Kamruzzaman, M., Bhuyan, M.K., Nilima, S.I. and Shahana, A. (2024) AI-Driven Strategies for Reducing Deforestation. *The American Journal of Engineering and Technology*, **6**, 6-20. https://doi.org/10.37547/tajet/volume06issue06-02

[8] Johora, F.T., Hasan, R., Farabi, S.F., Akter, J. and Mahmud, M.A.A. (2024) AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions. *The American Journal of Management and Economics Innovations*, **6**, 8-22. https://doi.org/10.37547/tajmei/volume06issue06-02

[9] Lee, H.J. and Kim, M. (2018) The Internet of Things in a Smart Connected World. In: Sen, J., Ed., *Internet of Things—Technology*, *Applications and Standardization*, InTech, 134. https://doi.org/10.5772/intechopen.76128

[10] Al Mahmud, M.A., Hossain, M.A., Saju, M.A.B., *et al.* (2024) Information Technology for the Next Future World: Adoption of It for Social and Economic Growth:

Part II. *International Journal of Innovative Research in Technology*, **10**, 742-747.

[11] Mohammad, N., Imran, M.A.U., Prabha, M., Sharmin, S. and Khatoon, R. (2024) Combating Banking Fraud with It: Integrating Machine Learning and Data Analytics. *The American Journal of Management and Economics Innovations*, **6**, 39-56. https://doi.org/10.37547/tajmei/volume06issue07-04

[12] Hasan, R., Farabi, S.F., Al Mahmud, M.A., *et al*. (2024) Information Technologies for the Next Future World: Implications, Impacts and Barriers: Part I. *International Journal of Creative Research Thoughts*, **12**, a323-a330.

[13] Shahana, A., Hasan, R., Farabi, S.F., Akter, J., Mahmud, M.A.A., Johora, F.T., *et al*. (2024) AI-Driven Cybersecurity: Balancing Advancements and Safeguards. *Journal of Computer Science and Technology Studies*, **6**, 76-85. https://doi.org/10.32996/jcsts.2024.6.2.9

[14] Zaman, A.A.U., Abdelaty, A. and Sobuz, M.H.R. (2024) Integration of BIM Data and Real-Time Game Engine Applications: Case Studies in Construction Safety Management. *Journal of Information Technology in Construction*, **29**, 117-140. https://doi.org/10.36680/j.itcon.2024.007

[15] Li, J., Greenwood, D. and Kassem, M. (2018) Blockchain in the Built Environment: Analysing Current Applications and Developing an Emergent Framework. Diamond Congress Ltd., Budapest University of Technology and Economics.

[16] Adat, V. and Gupta, B.B. (2017) Security in Internet of Things: Issues, Challenges, Taxonomy, and Architecture. *Telecommunication Systems*, **67**, 423-441. https://doi.org/10.1007/s11235-017-0345-9

[17] Vilajosana, X., Watteyne, T., Vucinic, M., Chang, T. and Pister, K.S.J. (2019) 6tisch: Industrial Performance for Ipv6 Internet-of-Things Networks. *Proceedings of the IEEE*, **107**, 1153-1165. https://doi.org/10.1109/jproc.2019.2906404

[18] Hortelano, D., Olivares, T., Ruiz, M., Garrido-Hidalgo, C. and López, V. (2017) From Sensor Networks to Internet of Things. Bluetooth Low Energy, a Standard for This Evolution. *Sensors*, **17**, Article No. 372. https://doi.org/10.3390/s17020372

[19] Raza, U., Kulkarni, P. and Sooriyabandara, M. (2017) Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys & Tutorials*, **19**, 855-873. https://doi.org/10.1109/comst.2017.2652320

[20] Milovanović, D., Pantović, V. and Gardašević, G. (2017) Converging Technologies for the IoT: Standardization Activities and Frameworks. In: Kocovic, P., *et al*., Eds., *Emerging Trends and Applications of the Internet of Things*, IGI Global, 71-103. https://doi.org/10.4018/978-1-5225-2437-3.ch003

[21] Khattak, H.A., Shah, M.A., Khan, S., Ali, I. and Imran, M. (2019) Perception Layer Security in Internet of Things. *Future Generation Computer Systems*, **100**, 144-164. https://doi.org/10.1016/j.future.2019.04.038

[22] Li, X., Eckert, M., Martinez, J. and Rubio, G. (2015) Context Aware Middleware Architectures: Survey and Challenges. *Sensors*, **15**, 20570-20607. https://doi.org/10.3390/s150820570

[23] Levä, T., Mazhelis, O. and Suomi, H. (2014) Comparing the Cost-Efficiency of CoAP and HTTP in Web of Things Applications. *Decision Support Systems*, **63**, 23-38. https://doi.org/10.1016/j.dss.2013.09.009

[24] Perwej, D.Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D.N. and Kumar Jaiswal, A. (2021) A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, **9**, 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

[25] Sobuz, M.H.R., Al-Imran,, Datta, S.D., Jabin, J.A., Aditto, F.S., Sadiqul Hasan, N.M., *et al*. (2024) Assessing the Influence of Sugarcane Bagasse Ash for the Production of Eco-Friendly Concrete: Experimental and Machine Learning Approaches. *Case Studies in Construction Materials*, **20**, e02839. https://doi.org/10.1016/j.cscm.2023.e02839

[26] Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017) A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques. *International Journal of Distributed Sensor Networks*, **13**, 1-33. https://doi.org/10.1177/1550147717741463

[27] Monga, C., Raju, K.S., Arunkumar, P.M., Bist, A.S., Sharma, G.K., Alsaab, H.O., *et al*. (2022) [Retracted] Secure Techniques for Channel Encryption in Wireless Body Area Network without the Certificate. *Wireless Communications and Mobile Computing*, **2022**, Article ID: 9839607. https://doi.org/10.1155/2022/2598465

[28] Subashini, S. and Kavitha, V. (2011) A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, **34**, 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[29] Aditto, F.S., Sobuz, M.H.R., Saha, A., Jabin, J.A., Kabbo, M.K.I., Hasan, N.M.S., *et al*. (2023) Fresh, Mechanical and Microstructural Behaviour of High-Strength Self-Compacting Concrete Using Supplementary Cementitious Materials. *Case Studies in Construction Materials*, **19**, e02395. https://doi.org/10.1016/j.cscm.2023.e02395

[30] Saggi, M.K. and Jain, S. (2018) A Survey towards an Integration of Big Data Analytics to Big Insights for Value-Creation. *Information Processing & Management*, **54**, 758-790. https://doi.org/10.1016/j.ipm.2018.01.010

[31] Shah, M.S.M., Leau, Y., Anbar, M. and Bin-Salem, A.A. (2023) Security and Integrity Attacks in Named Data Networking: A Survey. *IEEE Access*, **11**, 7984-8004. https://doi.org/10.1109/access.2023.3238732

[32] Bhadani, A.K. and Jothimani, D. (2016) Big Data: Challenges, Opportunities, and Realities. In: Manoj, K.S. and Dileep, K.G., Eds., *Effective Big Data Management and Opportunities for Implementation*, IGI Global, 1-24. https://doi.org/10.4018/978-1-5225-0182-4.ch001

[33] Riahi Sfar, A., Natalizio, E., Challal, Y. and Chtourou, Z. (2018) A Roadmap for Security Challenges in the Internet of Things. *Digital Communications and Networks*, **4**, 118-137. https://doi.org/10.1016/j.dcan.2017.04.003

[34] Babun, L., Denney, K., Celik, Z.B., McDaniel, P. and Uluagac, A.S. (2021) A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives. *Computer Networks*, **192**, Article ID: 108040. https://doi.org/10.1016/j.comnet.2021.108040

[35] Čolaković, A. and Hadžialić, M. (2018) Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues. *Computer Networks*, **144**, 17-39. https://doi.org/10.1016/j.comnet.2018.07.017

[36] Raza, S., Faheem, M. and Guenes, M. (2019) Industrial Wireless Sensor and Actuator Networks in Industry 4.0: Exploring Requirements, Protocols, and Challenges—A MAC Survey. *International Journal of Communication Systems*, **32**, e4074. https://doi.org/10.1002/dac.4074

[37] Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S. and Traore, I. (2022) A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies*, **15**, Article No. 6984. https://doi.org/10.3390/en15196984

[38] Singh, S., Sharma, P.K., Moon, S.Y. and Park, J.H. (2024) Advanced Lightweight

Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions. *Journal of Ambient Intelligence and Humanized Computing*, **15**, 1625-1642.

[39] Riad, K., Hamza, R. and Yan, H. (2019) Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records. *IEEE Access*, **7**, 86384-86393. https://doi.org/10.1109/access.2019.2926354

[40] Snehi, M. and Bhandari, A. (2021) Vulnerability Retrospection of Security Solutions for Software-Defined Cyber-Physical System against DDoS and IoT-DDoS Attacks. *Computer Science Review*, **40**, Article ID: 100371. https://doi.org/10.1016/j.cosrev.2021.100371

[41] Jepsen, W. (2022) Cyclic Redundancy Checks and Error Detection.

[42] Bertin, E., Hussein, D., Sengul, C. and Frey, V. (2019) Access Control in the Internet of Things: A Survey of Existing Approaches and Open Research Questions. *Annals of Telecommunications*, **74**, 375-388. https://doi.org/10.1007/s12243-019-00709-7

[43] Cirani, S., Picone, M., Gonizzi, P., Veltri, L. and Ferrari, G. (2015) IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. *IEEE Sensors Journal*, **15**, 1224-1234. https://doi.org/10.1109/jsen.2014.2361406

[44] Moon, S.Y., Park, J.H. and Park, J.H. (2018) Authentications for Internet of Things Security: Threats, Challenges and Studies. *Journal of Internet Technology*, **19**, 349-358.

[45] Chabridon, S., Laborde, R., Desprats, T., Oglaza, A., Marie, P. and Marquez, S.M. (2013) A Survey on Addressing Privacy Together with Quality of Context for Context Management in the Internet of Things. *Annals of Telecommunications*, **69**, 47-62. https://doi.org/10.1007/s12243-013-0387-2

[46] Ouaddah, A., Mousannif, H., Abou Elkalam, A. and Ait Ouahman, A. (2017) Access Control in the Internet of Things: Big Challenges and New Opportunities. *Computer Networks*, **112**, 237-262. https://doi.org/10.1016/j.comnet.2016.11.007

[47] Wilson, P. (2017) Inter-Device Authentication Protocol for the Internet of Things.

[48] Frustaci, M., Pace, P., Aloi, G. and Fortino, G. (2018) Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, **5**, 2483-2495. https://doi.org/10.1109/jiot.2017.2767291

[49] Yakubu, B.M., Khan, M.I., Khan, A., Jabeen, F. and Jeon, G. (2023) Blockchain-Based DDoS Attack Mitigation Protocol for Device-to-Device Interaction in Smart Home. *Digital Communications and Networks*, **9**, 383-392. https://doi.org/10.1016/j.dcan.2023.01.013

[50] Shafagh, H., Hithnawi, A., Droescher, A., Duquennoy, S. and Hu, W. (2015) Talos: En-Crypted Query Processing for the Internet of Things. *Proceedings of the* 13*th ACM Conference on Embedded Networked Sensor Systems*, Seoul, 1-4 November 2015, 197-210. https://doi.org/10.1145/2809695.2809723

[51] Kumar, R., Kumar, P. and Singhal, V. (2019) A Survey: Review of Cloud IoT Security Techniques, Issues, and Challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3368786

[52] Bhardwaj, I., Kumar, A. and Bansal, M. (2017). A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs. 2017 4*th International Conference on Signal Processing, Computing and Control* (*ISPCC*), Solan, 21-23 September 2017, 504-509. https://doi.org/10.1109/ispcc.2017.8269731

[53] Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P. (2019) The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, **6**, 1606-1616. https://doi.org/10.1109/jiot.2018.2847733

[54] Azrour, M., Mabrouki, J., Guezzaz, A. and Kanwal, A. (2021) Internet of Things Security: Challenges and Key Issues. *Security and Communication Networks*, **2021**, Article ID: 5533843. https://doi.org/10.1155/2021/5533843

[55] Raza, S., Duquennoy, S., Höglund, J., Roedig, U. and Voigt, T. (2012) Secure Communication for the Internet of Things—A Comparison of Link-Layer Security and IPsec for 6LoWPAN. *Security and Communication Networks*, **7**, 2654-2668. https://doi.org/10.1002/sec.406

[56] 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

[57] Szymoniak, S. and Kesar, S. (2022) Key Agreement and Authentication Protocols in the Internet of Things: A Survey. *Applied Sciences*, **13**, Article No. 404. https://doi.org/10.3390/app13010404

[58] Barceló, M., Urbieta, A., Astorga Burgo, J. and Jacob, E. (2022) Revisiting the Feasibility of Public Key Cryptography in Light of IIoT Communications.

[59] Kalra, S. and Sood, S.K. (2015) Secure Authentication Scheme for IoT and Cloud Servers. *Pervasive and Mobile Computing*, **24**, 210-223. https://doi.org/10.1016/j.pmcj.2015.08.001

[60] Chifor, B., Bica, I., Patriciu, V. and Pop, F. (2018) A Security Authorization Scheme for Smart Home Internet of Things Devices. *Future Generation Computer Systems*, **86**, 740-749. https://doi.org/10.1016/j.future.2017.05.048

[61] Begum, B.A. and Nandury, S.V. (2023) Data Aggregation Protocols for WSN and IoT Applications—A Comprehensive Survey. *Journal of King Saud University—Computer and Information Sciences*, **35**, 651-681. https://doi.org/10.1016/j.jksuci.2023.01.008

[62] Nguyen, V., Lin, P., Cheng, B., Hwang, R. and Lin, Y. (2021) Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Communications Surveys & Tutorials*, **23**, 2384-2428. https://doi.org/10.1109/comst.2021.3108618

[63] Beqqal, M.E. and Azizi, M. (2017) Review on Security Issues in RFID Systems. *Advances in Science, Technology and Engineering Systems Journal*, **2**, 194-202. https://doi.org/10.25046/aj020624

[64] Li, L., Fan, X., Zhi, B., Li, S. and Dabollahi, S.A. (2024) Highly Secure Authentication and Key Agreement Protocol for the Internet of Vehicles. *Telecommunication Systems*. https://doi.org/10.1007/s11235-024-01172-z

[65] Porambage, P. (2018) Lightweight Authentication and Key Management of Wireless Sensor Networks for Internet of Things.

[66] Matte, C. (2017) Wifi Tracking: Fingerprinting Attacks and Counter-Measures. Université de Lyon.

[67] Chandramouli, R., Iorga, M. and Chokhani, S. (2013) Cryptographic Key Management Issues and Challenges in Cloud Services. In: Jajodia, S., *et al.*, Eds., *Secure Cloud Computing*, Springer, 1-30. https://doi.org/10.1007/978-1-4614-9278-8_1

[68] Kumar, S. and Kumar, D. (2021) A Survey of Lightweight Cryptography for Power-Constrained IoT Devices: Security Challenges and Issues. In: Jena, O.P., Tripa-

thy, A.R. and Polkowski, Z., Eds., *Green Engineering and Technology*, CRC Press, 293-313. https://doi.org/10.1201/9781003176275-17

[69] Jabin, J.A., Khondoker, M.T.H., Sobuz, M.H.R. and Aditto, F.S. (2024) High-Temperature Effect on the Mechanical Behavior of Recycled Fiber-Reinforced Concrete Containing Volcanic Pumice Powder: An Experimental Assessment Combined with Machine Learning (ml)-Based Prediction. *Construction and Building Materials*, **418**, Article ID: 135362. https://doi.org/10.1016/j.conbuildmat.2024.135362

[70] Kumar, S., Kumar, D., Dangi, R., Choudhary, G., Dragoni, N. and You, I. (2024) A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices. *Computers, Materials & Continua*, **78**, 31-63. https://doi.org/10.32604/cmc.2023.047084

[71] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. and Faruki, P. (2019) Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys & Tutorials*, **21**, 2671-2701. https://doi.org/10.1109/comst.2019.2896380

[72] Abosata, N., Al-Rubaye, S., Inalhan, G. and Emmanouilidis, C. (2021) Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors*, **21**, Article No. 3654. https://doi.org/10.3390/s21113654