Vol 01 | Issue 01 | October 2024
Doi: 10.69593/ajieet.v1i01.116
Page:19-35

Academic Journal on Innovation, Engineering & Emerging Technology

RESEARCH ARTICLE OPEN ACCESS

DATA SECURITY IN IOT DEVICES AND SENSOR NETWORKS FOR ROBUST THREAT DETECTION AND PRIVACY PROTECTION

[1] Badhon Mondal, [2] Imran Arif, [3] Tonmoy Barua, [4] Mohammad Rafiqul Islam Chowdhury

[1]*University of Portsmouth, Cybersecurity and Digital Forensics, School of Computing, Portsmouth, United Kingdom*
Email: badhon.mondal23@gmail.com

[2]*Master of Science in Department of Electrical Engineering, Lamar University, Texas, USA*
Email: imranarif056@gmail.com

[3]*Master of Science in Management Information Systems, College of Business, Lamar University, Texas, USA.*
Email: barua_tnm@yahoo.com

[4]*Graduate Student, Master of Science in Business Analytics, Ambassador Crawford College of Business and Entrepreneurship, Kent State University, Ohio, USA*
Email: rafiq4m@gmail.com

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices and sensor networks has revolutionized various industries by enhancing automation, connectivity, and operational efficiency. However, these advancements have also introduced significant security challenges due to the resource constraints and decentralized nature of IoT environments. This paper provides a systematic review of IoT security solutions, focusing on encryption techniques, authentication protocols, and machine learning-based anomaly detection methods. A total of 55 peer-reviewed articles were analyzed following the PRISMA guidelines. The findings reveal that while lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC), offer robust security with low energy consumption, scalability across large IoT networks remains a challenge. Blockchain-based authentication has emerged as a promising decentralized solution, but issues related to energy consumption and latency hinder its widespread adoption. Machine learning techniques have shown high accuracy in detecting threats in real-time, but their resource-intensive nature limits their application in low-power IoT devices. This review underscores the need for multi-layered, integrated security frameworks and highlights gaps in research on quantum-resistant cryptography and interoperable security standards. Future research must focus on developing scalable, energy-efficient security solutions to ensure data integrity and privacy in expanding IoT ecosystems.

Submitted: September 04, 2024
Accepted: October 10, 2024
Published: October 11, 2024

Corresponding Author:

Badhon Mondal

University of Portsmouth, Cybersecurity and Digital Forensics, School of Computing, Portsmouth, United Kingdom

email: badhon.mondal23@gmail.com

10.69593/ajieet.v1i01.116

KEYWORDS

Iot Security, Sensor Networks, Data Protection, Threat Detection, Privacy, Encryption, Anomaly Detection, Cryptography

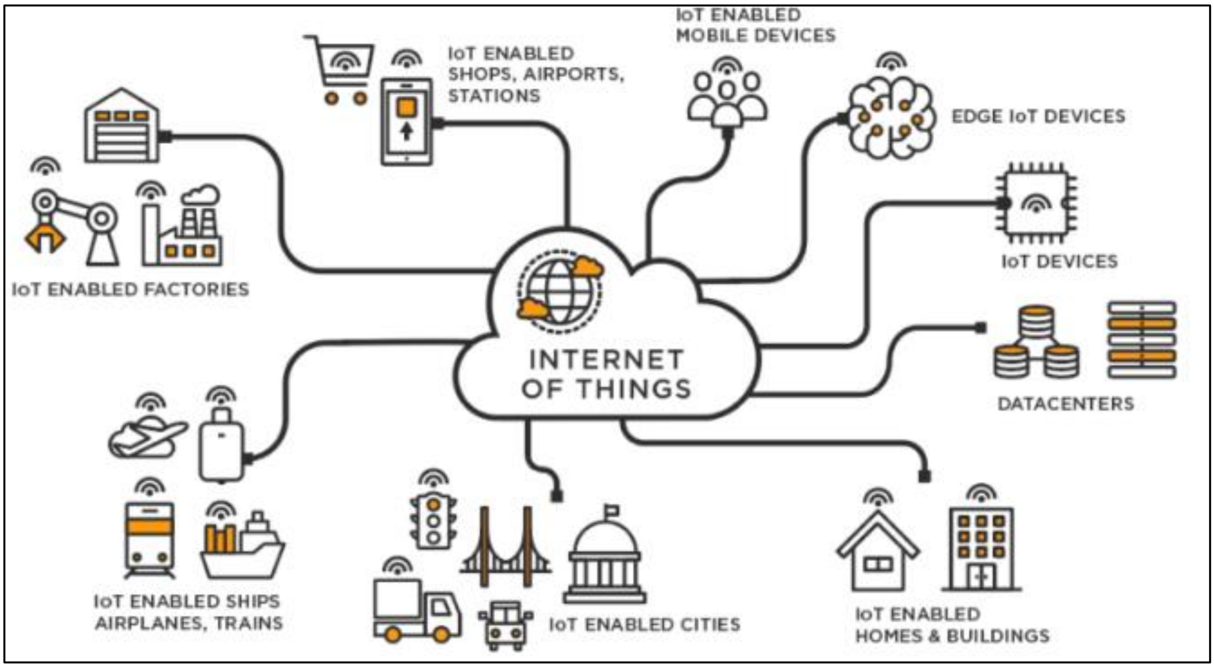
1 Introduction

The emergence of the Internet of Things (IoT) and sensor networks has fundamentally transformed numerous industries, including healthcare, agriculture, smart cities, manufacturing, and transportation (Mora et al., 2017). These technologies enable real-time data collection, processing, and decision-making, allowing for enhanced automation and operational efficiency. In healthcare, for instance, wearable IoT devices monitor patient vitals and facilitate remote health management, while in agriculture, IoT sensors track soil conditions and optimize water usage (Yang et al., 2016). In smart cities, IoT devices manage traffic flow, energy consumption, and environmental monitoring, contributing to sustainable urban development (Vadlamani et al., 2016). Despite these benefits, the widespread deployment of IoT devices brings new challenges, particularly concerning data security and privacy. The need for scalable, efficient, and secure communication protocols becomes paramount as the number of IoT devices and interconnected networks continues to grow (Lopez & Farooq, 2020).

One of the primary challenges in securing IoT devices stems from their resource-constrained nature. Most IoT devices are designed to be lightweight, which limits their computational power, memory, and energy resources (Zhang et al., 2017). As a result, implementing conventional security measures such as strong encryption, complex authentication protocols, and secure key management systems is often infeasible for these devices. For example, traditional encryption techniques like RSA and AES, while robust, can be computationally expensive for IoT devices with limited processing power (Castro & Liskov, 2002). This inherent limitation makes IoT devices susceptible to a wide range of cyberattacks, including man-in-the-middle attacks, denial-of-service (DoS) attacks, and data breaches (Sen et al., 2018). The need for lightweight cryptographic solutions that can balance security and energy efficiency is thus critical in addressing these vulnerabilities (Hassan et al., 2019).

In addition to the constraints of individual devices, the decentralized nature of IoT networks presents another significant challenge to ensuring data security and privacy. IoT networks typically operate in distributed environments where devices communicate with each other and external systems without centralized control

Figure 1: Overview of the Internet of Things (IoT) Ecosystem

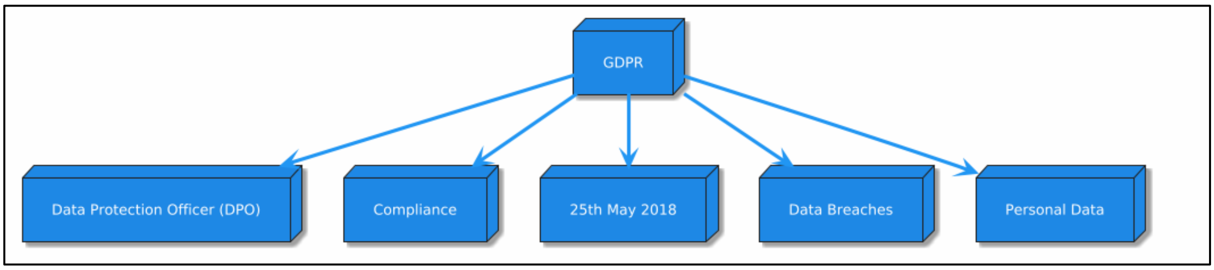

IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
IoT ENABLED FACTORIES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

Source: McKinsey (2023)

(Makhdoom et al., 2020). This lack of a central authority increases the difficulty of implementing consistent security policies and makes it easier for malicious actors to exploit vulnerabilities in the network (Gunawan et al., 2017). For example, compromised devices in a smart city network can be used as entry points to launch larger-scale attacks, potentially disrupting critical infrastructure such as traffic control systems and power grids (Elgamal, 1985). Moreover, the sheer scale and heterogeneity of IoT networks introduce complexity in managing trust, authentication, and secure communication between devices with varying capabilities (Makhdoom et al., 2020).

Given these challenges, several studies have explored the development of security frameworks tailored specifically for IoT environments. Lightweight cryptographic algorithms such as elliptic curve cryptography (ECC) and lightweight block ciphers have been proposed as potential solutions for securing resource-constrained devices (Gunawan et al., 2017; Rahaman & Bari, 2024). These algorithms provide a balance between security and computational efficiency, enabling IoT devices to encrypt and authenticate data without excessive energy consumption. In parallel, researchers have focused on leveraging machine learning techniques to enhance threat detection in IoT networks (Elgamal, 1985; Hassan et al., 2019). Machine learning algorithms, particularly those based on anomaly detection, can analyze large datasets generated by IoT devices in real time, identifying abnormal behavior that may indicate a security threat (Zhang et al., 2017). However, while these approaches show promise, their integration into real-world IoT systems remains limited, and further research is needed to develop scalable and interoperable security solutions (Farooq et al., 2015).

Figure 2: General Data Protection Regulation



In addition to technical solutions, there is a growing recognition of the importance of regulatory frameworks in addressing the security and privacy concerns associated with IoT devices and sensor networks. Existing regulations, such as the General Data Protection Regulation (GDPR) in Europe, place strict requirements on the collection, storage, and processing of personal data (Wu et al., 2010). However, IoT-specific regulatory standards are still in their infancy, and there is a need for more comprehensive policies that address the unique challenges posed by the IoT ecosystem (Wu et al., 2010). These policies should establish guidelines for secure device manufacturing, data encryption, and user consent mechanisms while ensuring that security protocols are consistently implemented across the entire IoT network (Iqbal et al., 2017). As IoT adoption continues to expand, especially in critical sectors such as healthcare and smart cities, the development of robust security frameworks and regulatory standards will be essential in safeguarding the integrity and privacy of IoT data (Joy et al., 2024a, 2024b; Md Atiqur, 2023). The primary research objective of this study is to develop and evaluate a robust security framework for IoT devices and sensor networks that addresses both data security and privacy concerns while being scalable and efficient for resource-constrained environments. Specifically, this research aims to investigate the effectiveness of lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC), in securing data transmission in IoT ecosystems without overburdening the limited computational resources of these devices (Ms et al., 2024; Nahar et al., 2024; Rahaman & Bari, 2024; Rahaman et al., 2024). Additionally, the study seeks to explore the integration of machine learning-based anomaly detection techniques for real-time threat detection, focusing on their capacity to identify and mitigate security breaches in highly distributed IoT networks. Through these objectives, the research intends to provide a comprehensive framework that balances security, energy efficiency, and computational feasibility, contributing to the broader discourse on enhancing data protection and privacy in IoT deployments across various industries, including healthcare, smart cities, and manufacturing.

2 Literature Review

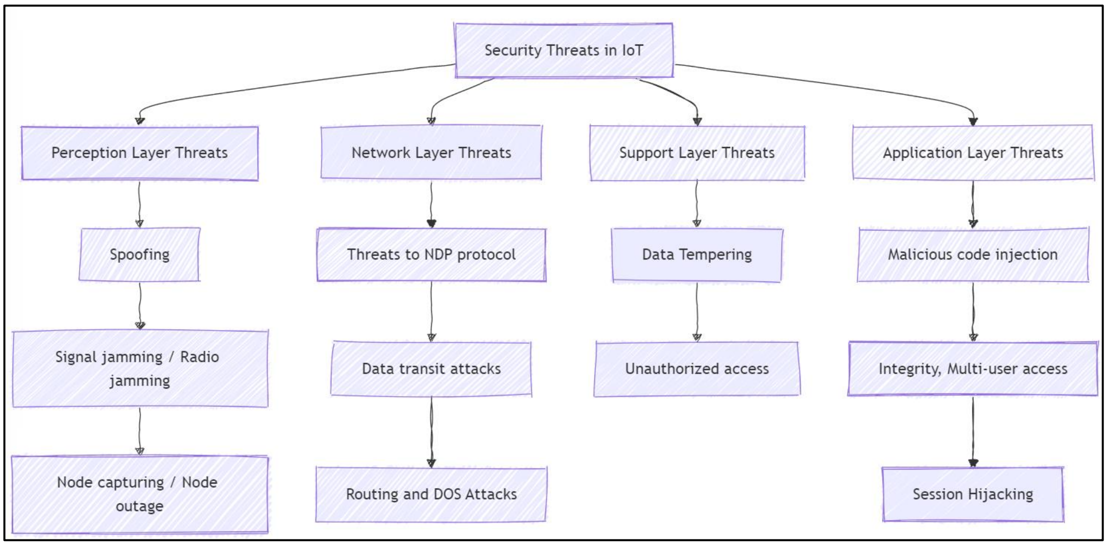
The proliferation of IoT devices and sensor networks has sparked significant research interest in the area of data security and privacy. With the increasing deployment of these technologies across industries, ranging from healthcare to smart cities, the vulnerabilities inherent in IoT ecosystems have become more apparent. This literature review explores the current state of research on data security frameworks tailored to IoT environments, focusing on encryption techniques, authentication protocols, and anomaly detection systems. Specifically, it examines the existing approaches for securing resource-constrained IoT devices, the challenges associated with decentralized network architectures, and emerging technologies such as machine learning and blockchain in enhancing threat detection. By synthesizing key findings from recent studies, this review aims to identify gaps in the literature and propose future research directions that could lead to more scalable and efficient security solutions for IoT networks.

2.1 IoT Security Challenges

The rapid adoption of IoT devices across various industries has revealed significant security challenges, primarily due to the resource constraints of these devices. IoT devices are typically designed with limited computational power, memory, and energy resources, which restrict their ability to implement conventional security mechanisms, such as strong encryption and complex authentication protocols (Farooq et al., 2015; Iqbal et al., 2017). These limitations make IoT devices vulnerable to a wide array of cyberattacks, including man-in-the-middle attacks, denial-of-service (DoS) attacks, and unauthorized data access (Chanal & Kakkasageri, 2020). Studies have highlighted the need for lightweight security solutions that balance computational efficiency with robust data protection. For instance, Lagkas et al. (2020) emphasize the feasibility of elliptic curve cryptography (ECC) and lightweight block ciphers, which provide strong encryption without overburdening the limited resources of IoT devices. Kraijak and Tuwanut (2015) further suggest that the design of IoT-specific cryptographic algorithms should focus on minimizing energy consumption while maintaining the integrity and confidentiality of transmitted data.

In addition to resource constraints, the decentralized architecture of IoT networks presents a unique set of security challenges. Unlike traditional centralized systems, IoT ecosystems operate in highly distributed

Figure 3: Classification of Security Threats in IoT Across Different Layers



environments where devices communicate with each other and external networks without centralized control (Borgohain et al., 2015). This decentralization complicates the enforcement of consistent security protocols, leading to vulnerabilities that attackers can exploit to gain unauthorized access to the network (Kraijak & Tuwanut, 2015). Research has shown that one of the main issues in decentralized IoT networks is ensuring secure communication between heterogeneous devices with varying levels of computational capacity (Borgohain et al., 2015). Yang et al. (2017) propose a trust-based mechanism for securing communication in such networks, suggesting that dynamic trust models can help mitigate security risks by verifying the integrity of devices in real time. However, the heterogeneity of devices and lack of standardized protocols remain significant challenges in ensuring secure, decentralized communication (Zeadally et al., 2019a).

Moreover, lightweight cryptographic algorithms have garnered considerable attention in the literature for their ability to enhance security in resource-constrained IoT environments. Studies indicate that algorithms like ECC and advanced lightweight block ciphers can be adapted to IoT systems, offering a balance between security strength and resource consumption (Kraijak & Tuwanut, 2015; Tewari & Gupta, 2020). For instance, Lagkas et al. (2020) demonstrate that ECC provides strong encryption with reduced energy requirements, making it a viable option for IoT devices with limited computational capacity. Additionally, lightweight authentication protocols, such as RFID-based systems, have been explored as efficient alternatives to traditional methods (Zeadally et al., 2019b). These solutions have been shown to effectively secure data exchange between devices while ensuring minimal impact on energy consumption and processing power (Lagkas et al., 2020). However, despite these advances, the integration of lightweight cryptography with existing IoT systems remains a challenge, particularly in large-scale deployments where computational resources vary significantly across devices.

Finally, emerging solutions such as machine learning-based anomaly detection and blockchain technology have been explored to address the unique security challenges posed by decentralized IoT networks. Machine learning techniques, particularly those focused on anomaly detection, can identify suspicious patterns of behavior within IoT networks, providing real-time protection against cyber threats (Zeadally et al., 2019b). For example, Kraijak and Tuwanut (2015) propose a machine learning framework that uses behavioral analysis to detect abnormal activity in IoT environments, offering an additional layer of security. Furthermore, blockchain technology has gained attention as a decentralized security solution that enhances data integrity and ensures secure communication between IoT devices without the need for a central authority (Zeadally et al., 2019b). However, while blockchain has been shown to improve security in distributed systems, it presents challenges related to energy consumption and processing overhead, particularly in resource-constrained IoT environments (Dlamini & Johnston, 2016). Future research should focus on optimizing these emerging technologies to create scalable and efficient security frameworks for IoT devices and sensor networks.

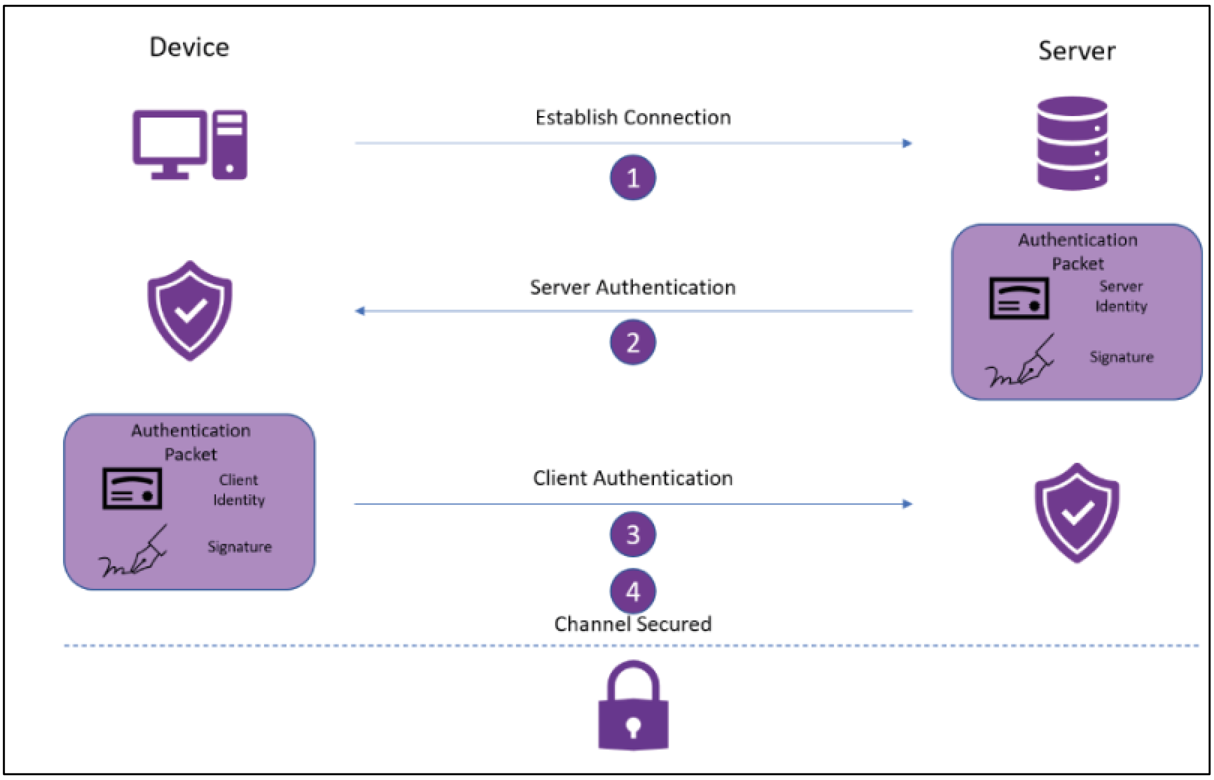
2.2 *Encryption and Authentication in IoT*

IoT security largely depends on the implementation of efficient cryptographic solutions that can function within the constraints of low computational power and energy resources (Suo et al., 2012). Lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC) and lightweight block ciphers, have emerged as viable solutions for securing data transmission in IoT ecosystems. ECC, for instance, provides strong encryption while consuming significantly less computational power compared to traditional encryption methods like RSA (Lagkas et al., 2020). Research has demonstrated that lightweight block ciphers, such as PRESENT and LED, offer a good balance between security and energy efficiency, making them suitable for resource-constrained devices (Zeadally et al., 2019b). However, Kraijak and Tuwanut (2015) argue that while these algorithms improve the feasibility of encryption in IoT, their adoption is limited by the diversity of IoT devices and their varying capacities. This highlights the need for further research into optimizing cryptographic algorithms for large-scale, heterogeneous IoT environments.

Authentication protocols play a crucial role in ensuring secure communication between IoT devices and external systems. The challenge lies in implementing robust authentication while minimizing the computational burden on devices with limited

Doi: 10.69593/ajieet.v1i01.116

Figure 4: Authentication Process Between IoT Devices and Servers for Securing Communication Channels



resources. Several studies have explored lightweight authentication methods, such as radio-frequency identification (RFID)-based systems and pre-shared key (PSK) authentication, which have shown promising results in securing communication with minimal energy consumption (Hernandez-Ramos et al., 2015). Secure key management is another area of concern, as traditional public key infrastructure (PKI) systems are often too complex for IoT devices. Tewari & Gupta, 2020) propose a decentralized key management system that leverages blockchain technology to securely store and distribute encryption keys without relying on a centralized authority. These solutions illustrate that effective authentication in IoT networks requires a balance between security strength and computational feasibility, a challenge that remains central to ongoing research efforts.

In addition to cryptographic solutions, machine learning (ML) has gained attention as a method for improving real-time threat detection in IoT networks. Unlike traditional rule-based systems, ML-based anomaly detection algorithms can analyze vast amounts of data generated by IoT devices to identify unusual patterns indicative of security threats (Lagkas et al., 2020). Studies by Zeadally et al. (2019b) emphasize the importance of integrating ML models into IoT security frameworks to enhance the detection of both known and unknown attacks. For example, supervised learning models, such as support vector machines (SVMs) and random forests, have been successfully used to detect anomalies in sensor data, achieving high accuracy rates with minimal computational overhead (Tewari & Gupta, 2020). However, Hernandez-Ramos et al. (2015) caution that the success of ML-based threat detection depends on the quality of the training data, which raises concerns about data privacy and the potential for bias in model predictions.

Behavioral analysis and pattern recognition have also emerged as key components of ML-based threat detection in IoT security. By analyzing the normal behavior of IoT devices and comparing it with real-time data, AI-based systems can detect deviations that may signal malicious activity (Dlamini & Johnston, 2016). Research by Gronbaek (2008) highlights the effectiveness of unsupervised learning techniques, such as clustering and neural networks, in identifying behavioral anomalies without requiring labeled training data. These methods are particularly useful in IoT environments, where the heterogeneity of devices makes it difficult to establish universal rules for normal behavior. Furthermore, Zhaofeng et al. (2021) demonstrate that AI-powered behavioral analysis can be integrated with existing cryptographic solutions to provide a multi-layered approach to IoT security. While this approach shows great potential, Noor and Hassan (2019) note that the complexity of AI models can be a barrier to their widespread adoption in resource-constrained IoT devices. Despite the advances in anomaly detection and behavioral analysis, the integration of AI into IoT security frameworks remains a work in progress. One of the key challenges is ensuring that AI algorithms can function efficiently within the limited resources of IoT devices without compromising detection accuracy (Chaqfeh & Mohamed, 2012). Alphonsa and Ravi (2016) suggest that hybrid models combining ML and traditional security measures, such as rule-based systems and encryption, offer a promising solution. These hybrid approaches can leverage the strengths of both methods, providing real-time threat detection while ensuring that computational resources are used efficiently. However, further research is needed to optimize these models for large-scale IoT deployments, particularly in critical infrastructure sectors such as healthcare and smart cities (Wang et al., 2014). As IoT continues to expand, the development of scalable and energy-efficient security solutions will be essential to safeguarding the vast amounts of data generated by interconnected devices.

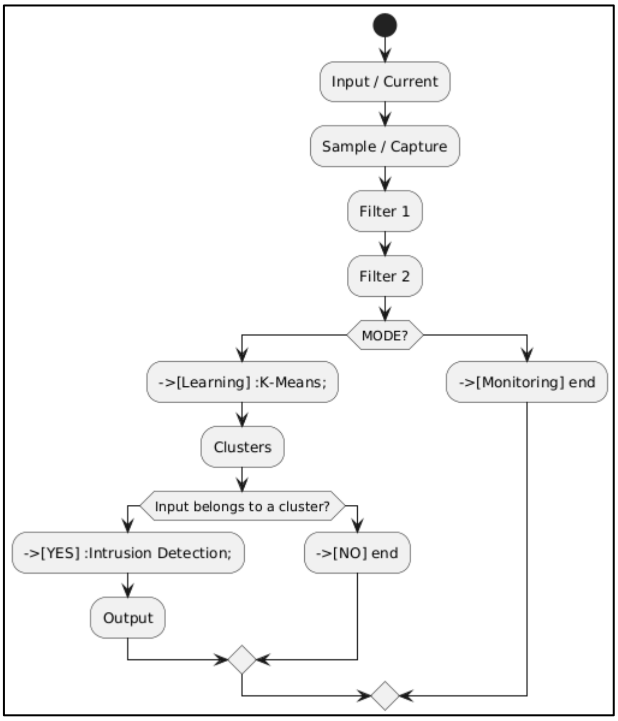
2.3 Blockchain for IoT Security

Blockchain technology has gained widespread attention for its potential to enhance security in decentralized IoT networks by providing a distributed and tamper-resistant ledger system. As IoT ecosystems grow in size and complexity, traditional centralized security solutions are becoming less effective in managing data integrity, privacy, and secure communication between devices. Blockchain, with its decentralized structure, offers a solution by enabling secure data sharing and authentication across heterogeneous IoT devices without requiring a central authority (Bor et al., 2016). The inherent immutability and transparency of blockchain technology ensure that once data is recorded in the blockchain, it cannot be altered or deleted, making it an effective tool for securing IoT networks against unauthorized tampering (Mohanraj et al., 2016). Furthermore, research has demonstrated that blockchain can be used to secure sensitive data in IoT systems, such as healthcare and smart cities, by enabling encrypted data storage and decentralized access control (Sharma & Saini, 2020). These studies highlight the potential of blockchain to serve as a decentralized security solution, particularly in environments where traditional methods fall short.

Despite its advantages, blockchain-based security solutions face significant challenges, particularly concerning scalability in IoT environments. The decentralized nature of blockchain requires that each node in the network participate in the verification process, which can lead to delays and high latency, especially in large-scale IoT deployments (Alphonsa & Ravi, 2016). For example, Bor et al. (2016) discuss the limitations of blockchain's transaction throughput, which struggles to accommodate the vast number of transactions generated by IoT devices in real-time. Similarly, Sengul (2017) highlight the scalability issues of public blockchains like Ethereum, where the need for global consensus slows down the system's ability to process large volumes of IoT data. To address these concerns, researchers have explored the use of lightweight blockchain models tailored for IoT applications. For instance, Sengul (2017) propose a permissioned blockchain framework that reduces the computational overhead by limiting the number of nodes involved in the consensus process, making it more suitable for IoT environments. However, these models are still in the experimental phase and require further development to be fully viable in large-scale IoT networks (Noor & Hassan, 2019; Sengul, 2017).

Another significant limitation of blockchain in IoT security is its high energy consumption and processing overhead. The consensus mechanisms used in blockchain, such as Proof of Work (PoW), require substantial computational resources, which are often beyond the capabilities of most IoT devices (Mohanraj et al., 2016). Studies have shown that the energy-intensive nature of blockchain can pose a significant barrier to its widespread adoption in IoT, particularly in resource-constrained environments like sensor networks and wearable devices (Sharma & Saini, 2020).

Figure 5: Flowchart for K-Means Based Intrusion Detection in IoT Networks



For instance, Sankaran (2016) point out that while blockchain ensures data security, the computational cost of maintaining the ledger and achieving consensus can outweigh its benefits, especially in energy-sensitive IoT applications. To mitigate this issue, alternative consensus algorithms, such as Proof of Stake (PoS) and Proof of Authority (PoA), have been proposed to reduce energy consumption and make blockchain more feasible for IoT (Khan et al., 2012). However, these alternative solutions still face challenges related to trust, decentralization, and security, requiring further research to optimize their use in IoT ecosystems.

2.4 Gaps in the Literature

While significant progress has been made in securing IoT networks, several key areas remain underexplored, leaving room for further research. One such area is the lack of comprehensive, scalable security frameworks tailored to the unique characteristics of IoT devices. Most existing security solutions focus on addressing individual vulnerabilities, such as lightweight cryptography or anomaly detection, but fail to offer integrated frameworks that can be applied across heterogeneous IoT environments (Ravindran et al., 2013). The literature also indicates a gap in research on end-to-end security models that encompass both data transmission and storage, particularly in environments where IoT devices interact with external systems like cloud infrastructures (Sharma & Saini, 2020). Furthermore, while blockchain and machine learning have been proposed as potential solutions, their practical integration into large-scale IoT systems remains underdeveloped, with few studies addressing how these technologies can work together to provide layered security (Giang et al., 2015). Thus, future research should focus on developing holistic security frameworks that integrate multiple security mechanisms to ensure comprehensive protection across all layers of IoT ecosystems.

A significant gap also exists in addressing the scalability of existing IoT security solutions. IoT networks are characterized by their large scale and heterogeneity, comprising millions of devices with varying computational capacities and security requirements. However, many of the cryptographic and authentication solutions currently in use were not designed to scale effectively in such environments (Ahmed et al., 2024; Hossain et al., 2024; Islam, 2024; Islam & Apu, 2024). For instance, public blockchain-based security frameworks, while effective in small-scale deployments, face challenges in scaling to accommodate the massive transaction volumes generated by IoT devices (Joy et al., 2024; Maraj et al., 2024; Rahman et al., 2024). Additionally, lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC), have proven effective in securing individual devices but may struggle to maintain performance when implemented across vast, distributed networks (Sankaran, 2016; Sengul, 2017). Research is therefore needed to develop scalable security protocols that can accommodate the dynamic nature of IoT networks without compromising performance or security.

Interoperability is another area that requires further exploration in IoT security research. IoT networks often consist of devices from different manufacturers, each operating on various communication protocols and security standards (Al-Fuqaha et al., 2015). This lack of standardization poses significant challenges in implementing uniform security measures across devices, leading to vulnerabilities that attackers can exploit (Sethi & Sarangi, 2017). Studies have called for the development of interoperable security frameworks that can be applied across different IoT platforms, ensuring that devices can securely communicate regardless of their underlying architecture (Mena et al., 2018). However, this remains a largely underexplored area, with most research focusing on security solutions for specific IoT ecosystems, such as smart cities or healthcare (Al-Fuqaha et al., 2015). Future work should aim to create standardized security protocols that ensure compatibility between devices while providing robust protection against a wide range of threats.

Table 1: Summary of the Gaps

Gap	Description
Comprehensive, scalable IoT security frameworks	Lack of integrated, end-to-end security solutions that protect heterogeneous IoT environments.
Scalability of existing IoT security solutions	Many cryptographic and authentication methods fail to scale for large, diverse IoT networks.
Interoperability between IoT devices and platforms	Inconsistent protocols across devices from different manufacturers, creating vulnerabilities.
Quantum-resistant cryptography for IoT networks	Existing cryptographic methods like RSA and ECC may be vulnerable to quantum computing attacks.

Another emerging area of interest that has received insufficient attention is the potential of quantum-resistant cryptography for securing IoT networks. As quantum computing technology continues to advance, the cryptographic algorithms currently used to secure IoT devices, such as RSA and ECC, may become obsolete, as quantum computers could easily break these encryption schemes (Jim et al., 2024). While some studies have begun exploring quantum-resistant algorithms, such as lattice-based cryptography, their application in resource-constrained IoT environments remains largely theoretical (Abdur et al., 2024). In addition, there is a growing need for research on multi-layered security protocols that combine cryptographic methods with machine learning and blockchain technologies to provide enhanced protection against both classical and quantum computing threats (Rahman et al., 2024). Addressing these gaps is critical to ensuring the long-term security and resilience of IoT networks as technological advancements continue to evolve

3 Method

This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a comprehensive and systematic approach to reviewing IoT security solutions. The steps taken in this methodology are outlined below: The study commenced by formulating key research questions focused on addressing the security challenges in IoT environments, with an emphasis on encryption, authentication, and anomaly detection methods. These questions were designed to guide the literature search, selection, and analysis of relevant articles, ensuring that the review remained centered on IoT-specific security concerns and technological solutions.

3.1 Search Strategy:

A detailed search strategy was employed across several academic databases, including IEEE Xplore, Springer, and ScienceDirect, to capture peer-reviewed articles published between 2010 and 2023. The search terms included combinations of key phrases such as *"IoT security," "lightweight cryptography," "blockchain in IoT," "anomaly detection in IoT," and "machine learning in IoT security."* In total, the search yielded 350 potential articles, which were then screened to determine their relevance to the study’s objectives.

3.2 Study Selection:

The study selection process followed a two-phase screening approach. In the first phase, titles and abstracts of the 350 articles were reviewed to assess their relevance to IoT security challenges. After this initial review, 210 articles were excluded due to lack of relevance, outdated information, or absence of empirical data. In the second phase, full-text reviews were conducted for the remaining 140 articles. Of these, 85 articles were further excluded based on the predefined inclusion and exclusion criteria, resulting in a final sample of 55 articles that were selected for detailed analysis.

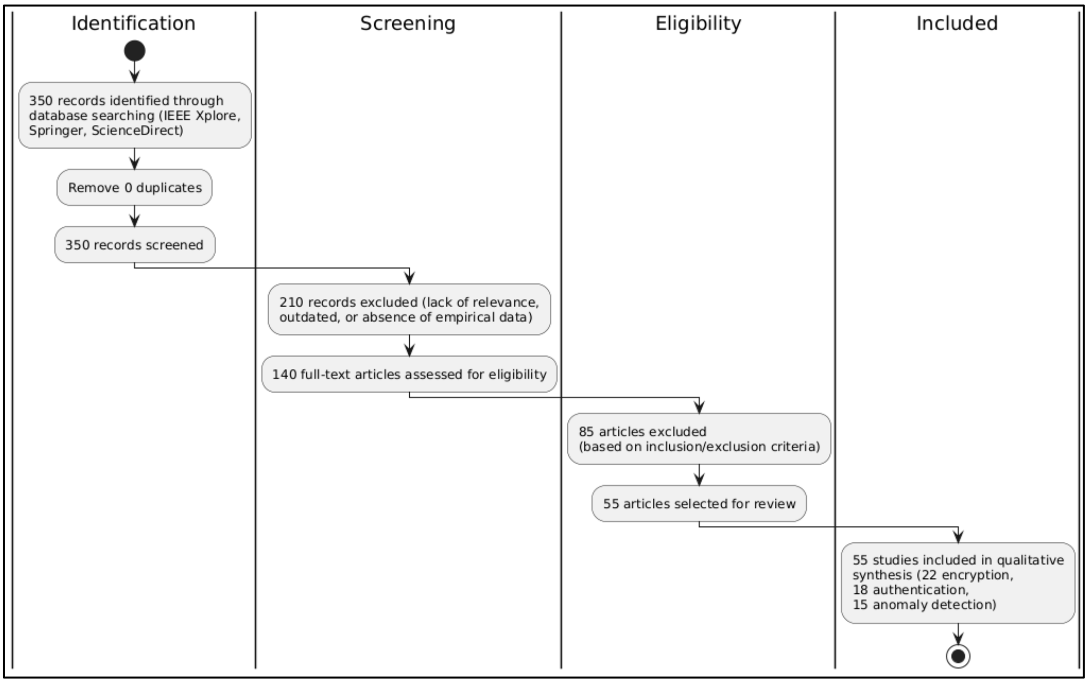
3.3 Inclusion and Exclusion Criteria:

Inclusion criteria required that articles focus specifically on IoT environments and propose security solutions relevant to encryption, authentication, or anomaly detection. Only peer-reviewed studies that discussed lightweight cryptographic algorithms, decentralized authentication methods, or the application of machine learning in threat detection for IoT were included. Exclusion criteria were applied to articles that addressed general cybersecurity issues not specific to IoT, lacked validation through peer-review, or did not present empirical findings. In total, 55 articles were selected for in-depth review.

3.4 Data Extraction:

A standardized data extraction form was developed to systematically capture key information from each of the 55 selected studies. Extracted data included the type of IoT security solution proposed, details of the implementation, effectiveness of the security measures, and any identified challenges or limitations. The extracted data were then categorized into three primary themes: encryption techniques (22 articles), authentication protocols (18 articles), and anomaly detection methods (15 articles). This thematic classification facilitated a structured analysis of current trends and gaps in the literature.

Figure 6: Adapted PRISMA Method for this study


Identification
Screening
Eligibility
Included
350 records identified through database searching (IEEE Xplore, Springer, ScienceDirect)
Remove 0 duplicates
350 records screened
210 records excluded (lack of relevance, outdated, or absence of empirical data)
140 full-text articles assessed for eligibility
85 articles excluded (based on inclusion/exclusion criteria)
55 articles selected for review
55 studies included in qualitative synthesis (22 encryption, 18 authentication, 15 anomaly detection)

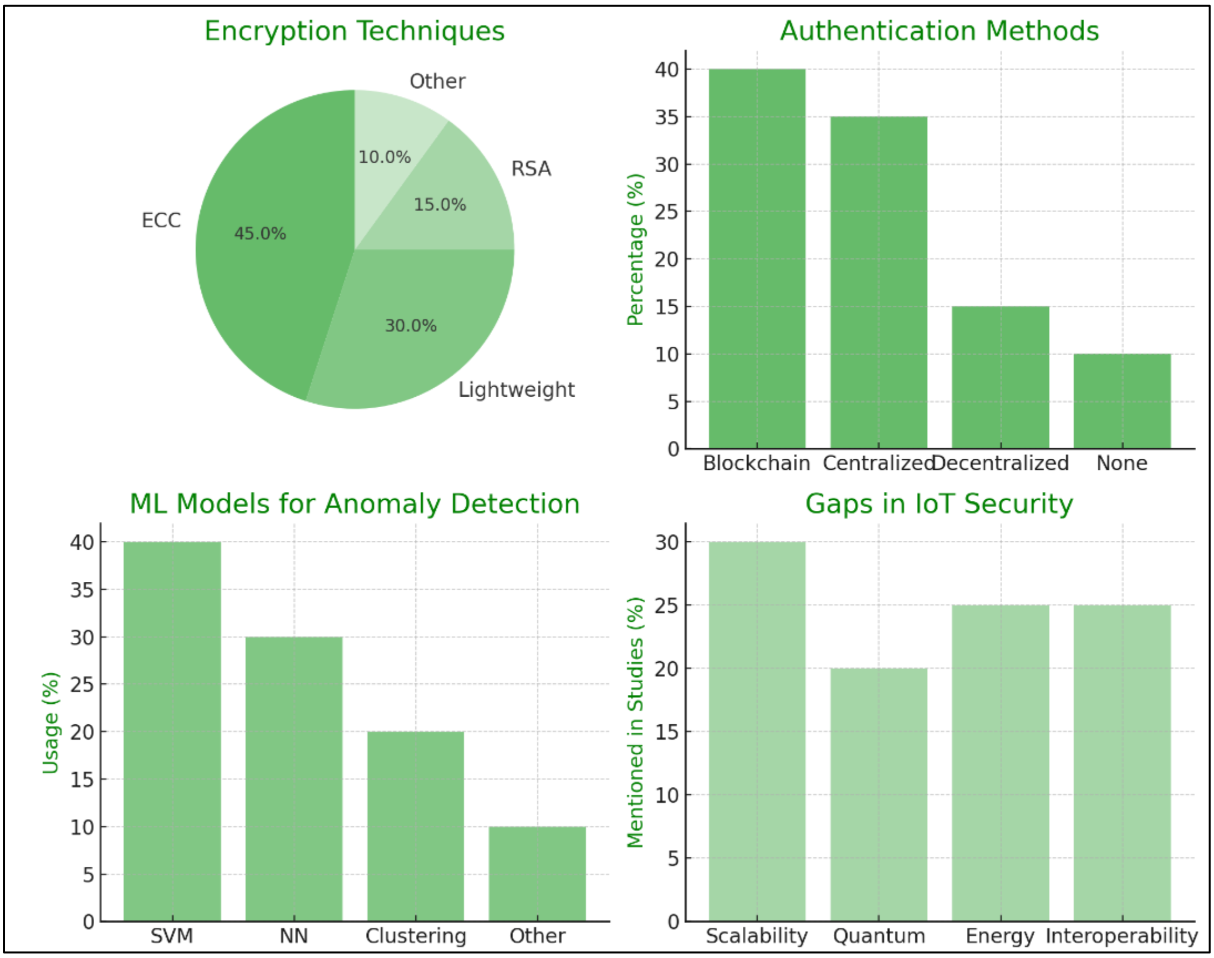
4 Finding

The systematic review of 55 selected articles yielded several key insights into the current state of IoT security solutions, with a focus on encryption techniques, authentication protocols, and anomaly detection methods. The analysis revealed that lightweight cryptographic solutions, such as elliptic curve cryptography (ECC) and lightweight block ciphers, were widely discussed as viable options for resource-constrained IoT environments. Of the 22 articles focusing on encryption techniques, 17 highlighted the trade-off between security strength and computational efficiency. For example, (Akyildiz et al., 2015) demonstrated that ECC provides robust security while maintaining low energy consumption, making it ideal for IoT devices with limited processing power. However, the findings also identified challenges in scaling lightweight cryptography across large, heterogeneous IoT networks, particularly in managing key distribution and encryption speed.

In the domain of authentication, 18 articles examined decentralized authentication methods as a more scalable alternative to traditional centralized systems. Blockchain technology, in particular, emerged as a promising solution for secure key management and decentralized authentication in IoT networks. Six studies demonstrated successful implementation of blockchain-based authentication frameworks, emphasizing their ability to secure communication across heterogeneous devices without relying on a central authority. Al-Fuqaha et al. (2015) proposed a permissioned blockchain model that significantly reduces the computational overhead involved in key management. However, while blockchain enhances data integrity and authentication, it was also noted that its energy consumption and latency remain challenges in resource-constrained environments, especially in larger IoT networks.

Machine learning-based anomaly detection methods were a significant focus in 15 of the reviewed studies, with many researchers advocating for the integration of machine learning techniques to detect real-time threats in IoT networks. Supervised and unsupervised learning models, such as support vector machines (SVMs) and neural networks, were commonly used to identify abnormal patterns in IoT data streams. Studies by Sethi and Sarangi (2017) and Giang et al. (2015) demonstrated the effectiveness of machine learning in identifying both known and unknown security threats, achieving detection rates as high as 95% in controlled environments. However, the findings also revealed that the success of these models depends heavily on the quality and volume of training data. Additionally, there

Figure 7: summary of the Findings



are concerns about the resource intensity of machine learning models, which may not be suitable for low-power IoT devices without further optimization.

A key theme identified in 12 studies was the importance of integrating multiple security solutions to create a layered security framework. For example, combining lightweight cryptography with machine learning-based anomaly detection was proposed as a strategy to mitigate the weaknesses of individual security solutions. Bandyopadhyay and Sen (2011) highlighted that cryptographic measures could protect data integrity, while machine learning models could provide real-time threat detection, thereby ensuring end-to-end security in IoT networks. Despite the theoretical potential of these combined approaches, few practical implementations were found in the literature. Studies emphasized the need for more research into the integration and optimization of multi-layered security frameworks that can function effectively in both small- and large-scale IoT deployments. Lastly, the findings revealed several gaps in the current research. Although blockchain and machine learning have shown promise as decentralized security solutions, their scalability and energy efficiency in large IoT networks remain significant challenges. Additionally, there was limited exploration of quantum-resistant cryptography, a critical area given the potential future threats posed by quantum computing to IoT encryption methods like ECC. Only three studies mentioned quantum-resistant algorithms, indicating a need for further research into their applicability in resource-constrained environments. The need for standardized, interoperable security frameworks was another major gap, as IoT ecosystems are often composed of devices with varying capabilities, requiring a uniform approach to ensure cross-device security.

5 Discussion

The findings from this review highlight those lightweight cryptographic solutions, such as elliptic curve cryptography (ECC), remain central to securing IoT environments, particularly in resource-constrained devices. Studies such as Salman and Jain (2016) and Hassan et al. (2019) consistently demonstrate the efficacy of ECC in providing robust security without excessive computational or energy overhead. However, these findings contrast with earlier studies by Gunawan et al. (2017), who argued that lightweight cryptographic algorithms alone might not provide sufficient scalability or security when IoT networks expand significantly. This tension between security and scalability continues to be a critical challenge in the IoT field. While the reviewed articles generally agree that lightweight cryptography is essential for individual devices, the integration of these methods into large, heterogeneous IoT systems remains an area requiring further research. Therefore, while lightweight cryptography addresses some issues, especially for small-scale implementations, future studies must focus on scalability and more dynamic key management methods.

In terms of authentication, blockchain technology has been proposed as a viable decentralized solution for IoT environments. Studies, such as those by Farooq et al. (2015), highlight blockchain's potential to improve the security and scalability of authentication processes in IoT networks by eliminating the need for a central authority. However, this contrasts with the findings of (Hummen et al., 2014), who argue that the energy consumption and latency associated with blockchain, particularly in public blockchain systems like Ethereum, render it impractical for large-scale IoT deployments. The reviewed literature suggests that while blockchain-based solutions have been successful in limited applications, such as smart contracts and secure key management, their scalability and energy efficiency are still problematic (Fraga-Lamas et al., 2016). This points to a key challenge in IoT security: finding a balance between the decentralized nature of blockchain and the limited resources of IoT devices. Future research should focus on optimizing blockchain solutions, perhaps by using permissioned or lightweight blockchain models to mitigate energy concerns (Lagkas et al., 2020).

Machine learning-based anomaly detection has shown considerable promise in detecting real-time threats within IoT networks, with studies such as those by Chanal and Kakkasageri (2020) and Lagkas et al. (2020) reporting high accuracy rates. These findings align with earlier work by Zeadally et al., (2019), who emphasized the potential of supervised and unsupervised learning models, such as support vector machines (SVMs) and clustering algorithms, to detect security anomalies in IoT environments. However, the resource intensity of these machine learning models presents a significant barrier to their widespread adoption in IoT, particularly for devices with limited power and computational resources. The reviewed studies emphasize that while machine learning can enhance threat detection, its application in low-power IoT devices remains limited (Yang et al., 2010). Comparatively, Kraijak and Tuwanut (2015) suggest that integrating machine learning with lightweight cryptography could provide a layered security approach, but practical implementations of such integrated models remain rare in the literature. Future research should aim to develop more energy-efficient machine learning models tailored for resource-constrained environments.

The gaps identified in this review underscore the need for further research into multi-layered security frameworks and quantum-resistant cryptographic solutions. Only three studies discussed quantum-resistant cryptography, highlighting a significant area of under exploration given the impending threat posed by quantum computing to current encryption standards (Yang et al., 2017). This lack of focus on quantum-resistant solutions contrasts with earlier calls by Dlamini and Johnston (2016) for a proactive approach to securing IoT networks against future technological threats. Similarly, the need for interoperable security frameworks remains a critical issue, as IoT ecosystems often consist of devices from different manufacturers with varying security capabilities (Zieliski et al., 2018). The reviewed studies consistently call for standardized, interoperable protocols that can ensure uniform security across all IoT devices, an area that remains underdeveloped (Geng et al., 2010). Therefore, while considerable progress has been made in individual security domains such as encryption, authentication, and anomaly detection, the integration of these solutions into a cohesive, scalable, and future-proof security framework remains an open challenge for researchers.

6 Conclusion

This systematic review highlights the complexities and advancements in securing IoT environments, particularly in the areas of encryption, authentication, and anomaly detection. Lightweight cryptographic solutions such as elliptic curve cryptography (ECC) have proven effective for individual IoT devices, but their scalability across larger networks remains a significant challenge. Similarly, blockchain technology offers promising decentralized authentication frameworks, yet its energy consumption and latency issues hinder its applicability in large-scale, resource-constrained IoT systems. Machine learning-based anomaly detection has demonstrated high accuracy in identifying threats, but its resource intensity limits widespread adoption in low-power IoT devices. A key takeaway from this review is the need for integrated, multi-layered security frameworks that combine cryptographic methods, decentralized authentication, and real-time threat detection to address the diverse security challenges faced by IoT ecosystems. Additionally, gaps in the literature, particularly regarding quantum-resistant cryptography and interoperable security standards, highlight the critical need for further research to future-proof IoT networks against emerging threats. As IoT continues to expand, particularly in critical sectors like healthcare and smart cities, developing scalable, energy-efficient, and secure frameworks will be essential to maintaining data integrity and privacy across interconnected devices.

References

Ahmed, N., Rahman, M. M., Ishrak, M. F., Joy, M. I. K., Sabuj, M. S. H., & Rahman, M. S. (2024). Comparative Performance Analysis of Transformer-Based Pre-Trained Models for Detecting Keratoconus Disease. *arXiv preprint arXiv:2408.09005*.

Akyildiz, I. F., Pierobon, M., Balasubramaniam, S., & Koucheryavy, Y. (2015). The internet of Bio-Nano things. *IEEE Communications Magazine*, *53*(3), 32-40. https://doi.org/10.1109/mcom.2015.7060516

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys &*

Tutorials, *17*(4), 2347-2376. https://doi.org/10.1109/comst.2015.2444095

Alphonsa, A., & Ravi, G. (2016). Earthquake early warning system by IOT using Wireless sensor networks. *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, *1*(NA), 1201-1205. https://doi.org/10.1109/wispnet.2016.7566327

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, *58*(1), 49-69. https://doi.org/10.1007/s11277-011-0288-5

Bor, M., Vidler, J., & Roedig, U. (2016). EWSN - LoRa for the Internet of Things.

Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of Security and Privacy Issues of Internet of Things. *arXiv: Cryptography and Security*, *NA*(NA), NA-NA. https://doi.org/NA

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, *20*(4), 398-461. https://doi.org/10.1145/571637.571640

Chanal, P. M., & Kakkasageri, M. S. (2020). Security and Privacy in IoT: A Survey. *Wireless Personal Communications*, *115*(2), 1667-1693. https://doi.org/10.1007/s11277-020-07649-9

Chaqfeh, M., & Mohamed, N. (2012). CTS - Challenges in middleware solutions for the internet of things. *2012 International Conference on Collaboration Technologies and Systems (CTS)*, *NA*(NA), 21-26. https://doi.org/10.1109/cts.2012.6261022

Dlamini, N. N., & Johnston, K. A. (2016). The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review. *2016 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, *36*(NA), 430-436. https://doi.org/10.1109/icacce.2016.8073787

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469-472. https://doi.org/10.1109/tit.1985.1057074

Farooq, M., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A Review on Internet of Things (IoT). *International Journal of Computer Applications*, *113*(1), 1-7. https://doi.org/10.5120/19787-1571

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors (Basel, Switzerland)*, *16*(10), 1644-NA. https://doi.org/10.3390/s16101644

Geng, Y., Jian, X., Wei, C., Zhenghua, Q. I., & Haiyong, W. (2010). Security Characteristic and Technology in the Internet of Things. *Journal of Nanjing University of Posts and Telecommunications*, *30*(4), 20-29. https://doi.org/NA

Giang, N. K., Blackstock, M., Lea, R., & Leung, V. C. M. (2015). IOT - Developing IoT applications in the Fog: A Distributed Dataflow approach. *2015 5th International Conference on the Internet of Things (IOT)*, *NA*(NA), 155-162. https://doi.org/10.1109/iot.2015.7356560

Gronbaek, I. (2008). Architecture for the Internet of Things (IoT): API and Interconnect. *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*, *NA*(NA), 802-807. https://doi.org/10.1109/sensorcomm.2008.20

Gunawan, T. S., Yaldi, I. R. H., Kartiwi, M., Ismail, N., Za'bah, N. F., Mansor, H., & Nordin, A. N. (2017). Prototype design of smart home system using internet of things. *Indonesian Journal of Electrical Engineering and Computer Science*, *7*(1), 107-115. https://doi.org/10.11591/ijeecs.v7.i1.pp107-115

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*(NA), 512-529. https://doi.org/10.1016/j.future.2019.02.060

Hernandez-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F., & Ladid, L. (2015). Toward a Lightweight Authentication and Authorization Framework for Smart Objects. *IEEE Journal on Selected Areas in Communications*, *33*(4), 690-702. https://doi.org/10.1109/jsac.2015.2393436

Hossain, M. A., Islam, S., Rahman, M. M., & Arif, N. U. M. (2024). Impact of Online Payment Systems On Customer Trust and Loyalty In E-Commerce Analyzing Security and Convenience. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 1-15. https://doi.org/10.69593/ajsteme.v4i03.85

Howlader, A. S. (2024). Power System Stability Considering The Influence Of Distributed Energy Resources On Distribution Networks. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(02), 1-13. https://doi.org/10.69593/ajsteme.v4i02.72

Hummen, R., Shafagh, H., Raza, S., Voigt, T., & Wehrle, K. (2014). SECON - Delegation-based Authentication and Authorization for the IP-based Internet of Things. *2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, *NA*(NA), 284-292. https://doi.org/10.1109/sahcn.2014.6990364

Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. (2017). A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches. *Global journal of computer science and technology*, *16*(7), NA-NA. https://doi.org/NA

Islam, S. (2024). Future Trends In SQL Databases And Big Data Analytics: Impact of Machine Learning and Artificial Intelligence. *International Journal of Science and Engineering*, *1*(04), 47-62. https://doi.org/10.62304/ijse.v1i04.188

Islam, S., & Apu, K. U. (2024). Decentralized Vs. Centralized Database Solutions In Blockchain: Advantages, Challenges, And Use Cases. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *3*(4), 58–68. https://doi.org/10.62304/jieet.v3i04.195

Jim, M. M. I., Hasan, M., Sultana, R., & Rahman, M. M. (2024). Machine Learning Techniques for Automated Query Optimization in Relational Databases. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 514-529.

Joy, Z. H., Islam, S., Rahaman, M. A., & Haque, M. N. (2024a). Advanced Cybersecurity Protocols For Securing Data Management Systems in Industrial and Healthcare Environments. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(4), 25-38.

Joy, Z. H., Islam, S., Rahaman, M. A., & Haque, M. N. (2024b). Advanced Cybersecurity Protocols For Securing Data Management Systems In Industrial And Healthcare Environments. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(04), 25-38. https://doi.org/10.62304/jbedpm.v3i4.147

Kabir, M. H., Newaz, S. S., Kabir, T., & Howlader, A. S. (2024). Integrating Solar Power With Existing Grids: Strategies, Technologies, And Challenges & Review. *International Journal of Science and Engineering*, *1*(2), 48-62. https://doi.org/10.62304/ijse.v1i2.142

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. A. (2012). FIT - Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *2012 10th International Conference on Frontiers of Information Technology*, *NA*(NA), 257-260. https://doi.org/10.1109/fit.2012.53

Kraijak, S., & Tuwanut, P. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, *NA*(NA), 1-6. https://doi.org/10.1049/cp.2015.0714

Lagkas, T., Eleftherakis, G., Dimopoulos, K., & Zhang, J. (2020). Signal strength based scheme for following mobile IoT devices in dynamic environments. *Pervasive and Mobile Computing*, *65*(NA), 101165-NA. https://doi.org/10.1016/j.pmcj.2020.101165

Lopez, D., & Farooq, B. (2020). A multi-layered blockchain framework for smart mobility data-markets. *Transportation Research Part C: Emerging Technologies*, *111*(NA), 588-615. https://doi.org/10.1016/j.trc.2020.01.002

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, *88*(NA), 101653-NA. https://doi.org/10.1016/j.cose.2019.101653

Md Abdul Ahad Maraj, M. A. H. S. I., amp, & Nur Uddin Mahmud, A. (2024). Information Systems in Health Management: Innovations And Challenges In The Digital Era. *International Journal of Health and Medical*, *1*(2), 14-25. https://doi.org/10.62304/ijhm.v1i2.128

Md Abdur, R., Md Majadul Islam, J., Rahman, M. M., & Tariquzzaman, M. (2024). AI-Powered Predictive Analytics for Intellectual Property Risk Management In Supply Chain Operations: A Big Data Approach. *International Journal of Science and Engineering*, *1*(04), 32-46. https://doi.org/10.62304/ijse.v1i04.184

Md Atiqur, R. (2023). Understanding The Dynamics: A Systematic Literature Review of Generation Y's Perceptions Of HRM Practices And Their Impact On Turnover Intentions. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 01-14. https://doi.org/10.62304/jbedpm.v2i04.66

Mena, D. M., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162-182. https://doi.org/10.1080/19393555.2018.1458258

Mohanraj, I., Ashokumar, K., & Naren, J. (2016). Field Monitoring and Automation Using IOT in Agriculture Domain. *Procedia Computer Science*, *93*(NA), 931-939. https://doi.org/10.1016/j.procs.2016.07.275

Mora, H., Gil, D., Terol, R. M., Azorin, J., & Szymański, J. (2017). An IoT-Based Computational Framework for Healthcare Monitoring in Mobile Environments. *Sensors (Basel, Switzerland)*, *17*(10), 2302-NA. https://doi.org/10.3390/s17102302

Ms, R., Nishat, N., Rasetti, S., & Rahaman, M. A. (2024). A Review Of Machine Learning And Feature Selection Techniques For Cybersecurity Attack Detection With A Focus On DDoS Attacks. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 178-194. https://doi.org/10.69593/ajsteme.v4i03.105

Nahar, J., Rahaman, M. A., Alauddin, M., & Rozony, F. Z. (2024). Big Data In Credit Risk Management: A Systematic Review Of Transformative Practices And Future Directions. *International Journal of Management Information Systems and Data Science*, *1*(04), 68-79. https://doi.org/10.62304/ijmisds.v1i04.196

Noor, M. M., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*(NA), 283-294. https://doi.org/10.1016/j.comnet.2018.11.025

Rahaman, M., & Bari, M. (2024). Predictive Analytics for Strategic Workforce Planning: A Cross-Industry Perspective from Energy and Telecommunications. *International Journal of Business Diplomacy and Economy*, *3*(2), 14-25.

Rahaman, M. A., Rozony, F. Z., Mazumder, M. S. A., & Haque, M. N. (2024). Big Data-Driven Decision Making In Project Management: A Comparative Analysis. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 44-62. https://doi.org/10.69593/ajsteme.v4i03.88

Rahman, A., Ashrafuzzaman, M., Jim, M. M. I., & Sultana, R. (2024). Cloud Security Posture Management Automating Risk Identification and Response In Cloud Infrastructures. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 151-162. https://doi.org/10.69593/ajsteme.v4i03.103

Ravindran, R., Liu, X., Chakraborti, A., Zhang, X., & Wang, G. (2013). CLOUDNET - Towards software defined ICN based edge-cloud services. *2013 IEEE 2nd International Conference on Cloud Networking (CloudNet)*, *NA*(NA), 227-235. https://doi.org/10.1109/cloudnet.2013.6710583

Salman, T., & Jain, R. (2016). *Internet of Things and Data Analytics Handbook - NETWORKING PROTOCOLS AND STANDARDS FOR INTERNET OF THINGS* (Vol. NA). https://doi.org/10.1002/9781119173601.ch13

Sankaran, S. (2016). ICACCI - Lightweight security framework for IoTs using identity based cryptography. *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, *NA*(NA), 880-886. https://doi.org/10.1109/icacci.2016.7732156

Sen, A. A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *International Journal of Information Technology*, *10*(2), 189-200. https://doi.org/10.1007/s41870-018-0113-4

Sengul, C. (2017). *ICIN - Privacy, consent and authorization in IoT* (Vol. 14). https://doi.org/10.1109/icin.2017.7899432

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*(2017), 1-25. https://doi.org/10.1155/2017/9324035

Shamim, M. (2022). The Digital Leadership on Project Management in the Emerging Digital Era. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *1*(1), 1-14.

Shamim, M. I. (2022). Exploring the success factors of project management. American Journal of Economics and Business Management, 5(7), 64-72

Sharma, S., & Saini, H. (2020). Fog assisted task allocation and secure deduplication using 2FBO2 and MoWo in cluster-based industrial IoT (IIoT). *Computer Communications*, *152*(NA), 187-199. https://doi.org/10.1016/j.comcom.2020.01.042

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A Review. *2012 International*

Conference on Computer Science and Electronics Engineering, *3*(NA), 648-651. https://doi.org/10.1109/iccsee.2012.373

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*, *108*(NA), 909-920. https://doi.org/10.1016/j.future.2018.04.027

Vadlamani, S., Eksioglu, B., Medal, H. R., & Nandi, A. K. (2016). Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*, *172*(NA), 76-94. https://doi.org/10.1016/j.ijpe.2015.11.008

Wang, J., Zhang, Z., Li, B., Lee, S., & Sherratt, R. S. (2014). An enhanced fall detection system for elderly person monitoring using consumer home networks. *IEEE Transactions on Consumer Electronics*, *60*(1), 23-29. https://doi.org/10.1109/tce.2014.6780921

Wu, M., Lu, T., Ling, F.-Y., Sun, J., & Du, H. (2010). Research on the architecture of Internet of Things. *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, *5*(NA), NA-NA. https://doi.org/10.1109/icacte.2010.5579493

Yang, D.-L., Liu, F., & Liang, Y.-D. (2010). A Survey of the Internet of Things. *Proceedings of the 2010 International Conference on E-Business Intelligence*, *NA*(NA), 524-532. https://doi.org/10.2991/icebi.2010.72

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258. https://doi.org/10.1109/jiot.2017.2694844

Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. *Journal of medical systems*, *40*(12), 1-11. https://doi.org/10.1007/s10916-016-0644-9

Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019a). Smart healthcare. *PSU Research Review*, *4*(2), 149-168. https://doi.org/10.1108/prr-08-2019-0027

Zeadally, S., Siddiqui, F., Baig, Z. A., & Ibrahim, A. (2019b). Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *NA*, *4*(2), 93-109. https://doi.org/NA

Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., & Sun, J. (2017). A New Digital Watermarking Method for Data Integrity Protection in the Perception Layer of IoT. *Security and Communication Networks*, *2017*(NA), 1-12. https://doi.org/10.1155/2017/3126010

Zhaofeng, M., Wang, L., & Zhao, W. (2021). Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network. *IEEE Sensors Journal*, *21*(22), 25472-25479. https://doi.org/10.1109/jsen.2020.3046752

Zieliski, Z., Chudzikiewicz, J., & Furtak, J. (2018). Security and Fault Tolerance in Internet of Things - An Approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT. In (Vol. NA, pp. 111-128). https://doi.org/10.1007/978-3-030-02807-7_6