FMDB *Transactions on Sustainable Computing Systems*

Analysing Security and Privacy Threats in Next-Generation IoT Systems: A Review of Emerging Challenges and Mitigation Approaches

Dhina Suresh[1,*], M. Karthikeyan[2], V. Kalpana[3]

[1]Department of Computer Science, St. Joseph's College of Arts and Science for Women, Hosur, Tamil Nadu, India.
[2,3]Department of Computer Science, M.G.R. College, Hosur, Tamil Nadu, India.
dhinadulcy@gmail.com[1], mkeyan1990@gmail.com[2], msckalpana@gmail.com[3]

Abstract: The Internet of Things (IoT) is undergoing continual transformation, fundamentally reshaping industries by enabling seamless connectivity and autonomous interactions among smart devices. Emerging technologies, including Artificial Intelligence (AI), edge and fog computing, blockchain, and advanced 5G/6G communication networks, are driving the evolution of IoT systems. These innovations have improved the efficiency, scalability, and intelligence of IoT networks, supporting real-time data analytics, autonomous decision-making, and context-aware functionalities. This paper provides an in-depth review of the architectures, enabling technologies, and security strategies that characterise next-generation IoT ecosystems. It examines how intelligent systems facilitate adaptive control and resilience, with a focus on application areas like autonomous transportation, smart healthcare, and industrial automation. Additionally, the review discusses the increasing relevance of data-driven architectures, decentralised frameworks, and blockchain-based trust models in promoting self-organising and self-healing IoT environments. By synthesising the latest research trends and technological advances, this review offers a foundational resource for researchers and practitioners. It aims to inform the design and implementation of secure, efficient, and future-ready IoT ecosystems equipped to meet the evolving challenges of digital infrastructures. This revised version enhances your original content by improving precision and readability while preserving your main ideas.

Keywords: Next-Generation IoT; Smart Devices; Edge Computing; Artificial Intelligence; IoT Architecture; Security Mechanisms; Smart Cities; Industrial IoT; Machine Learning.

Received on: 03/11/2024, **Revised on:** 28/01/2025, **Accepted on:** 06/03/2025, **Published on:** 07/09/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCS

DOI: https://doi.org/10.69888/FTSCS.2025.000475

Cite as: D. Suresh, M. Karthikeyan, and V. Kalpana, "Analysing Security and Privacy Threats in Next-Generation IoT Systems: A Review of Emerging Challenges and Mitigation Approaches," *FMDB Transactions on Sustainable Computing Systems,* vol. 3, no. 3, pp. 166-175, 2025.

1. Introduction

The rapid evolution of technological fields such as wireless communications, embedded computing, broadband Internet access, and automated tracking and identification has significantly contributed to the integration of intelligent objects into everyday human life. The Internet of Things (IoT) refers to the concept of connecting physical objects to the Internet, enabling them to communicate, exchange data, and perform coordinated tasks across a wide range of applications [1]. These applications include

[*] Corresponding author.

smart homes, industrial operations, healthcare monitoring, transportation management, and environmental observation. Through this pervasive interconnection, IoT systems are transforming traditional infrastructures into intelligent, data-driven environments [2]. Within the IoT ecosystem, several emerging technologies play an essential role in enhancing functionality, scalability, and security. Among these, blockchain, artificial intelligence (AI), machine learning (ML), cloud computing, and humanitarian logistics have emerged as key enablers of next-generation IoT systems. Blockchain technology ensures secure, transparent, and tamper-resistant data transactions among interconnected devices, thereby improving trust and reliability in distributed environments [5].

Cloud computing offers scalable storage and processing capabilities, enabling real-time data analytics and facilitating the effective management of the massive data generated by IoT networks [6]. Similarly, AI and ML techniques empower IoT devices with intelligent decision-making, anomaly detection, and predictive maintenance capabilities, resulting in enhanced operational efficiency and automation. In addition, humanitarian logistics leverages IoT systems to optimise resource distribution, enhance situational awareness, and coordinate relief operations during crises and natural disasters. The convergence of these technologies not only enhances productivity and innovation but also addresses critical issues such as data privacy, interoperability, and system resilience [7]. Collectively, these advancements pave the way for secure, efficient, and intelligent IoT ecosystems that drive sustainable growth and improve quality of life across various sectors [18]. As technological innovation accelerates at an unprecedented pace, Internet of Things (IoT) devices have become deeply integrated into modern daily life [19]. From smart home appliances to industrial sensors, IoT gadgets now play a crucial role in enhancing convenience, automation, and connectivity. However, this growing dependence on IoT technology has also expanded the potential attack surface for cybercriminals, who increasingly view these devices as vulnerable entry points within digital ecosystems [9].

One of the primary reasons for this vulnerability lies in the inherent limitations of IoT devices. Due to their compact size and cost-sensitive design, most IoT devices incorporate only minimal hardware components, such as low-power embedded microcontrollers, limited memory, basic sensors, actuators, and constrained power supply units [10]. These restrictions often prevent the implementation of advanced cryptographic protocols or comprehensive security frameworks [20]. Additionally, the use of lightweight or simplified operating systems, combined with restricted computational resources, further limits their ability to execute robust encryption or intrusion detection mechanisms [21]. Compounding this issue is the widespread deployment of mass-produced, low-cost IoT products that often lack standardised or well-maintained security measures [11]. Many of these off-brand or generic devices include only basic built-in protections, leaving them susceptible to exploitation through common attack vectors such as unauthorised access, malware injection, and data breaches [12]. The absence of regular firmware updates and weak authentication mechanisms further aggravates the problem, making IoT systems attractive targets for cyberattacks [22]. Thus, the convergence of limited device capability, inadequate security design, and rapid market expansion presents significant challenges to ensuring privacy and resilience in the IoT landscape [13].

2. Survey of Literature on IoT Security and Privacy

The literature on the Internet of Things (IoT) in healthcare and smart systems explores recent developments, potential applications, and security challenges. It emphasises privacy issues, security vulnerabilities, AI-based solutions, and future research avenues aimed at creating more resilient and secure IoT environments. Bollineni et al. [3] provide a comprehensive review of innovative healthcare solutions driven by these technologies. Their analysis covers the architecture, applications, benefits, and limitations of these solutions. The article categorises healthcare use cases into critical domains, including wearable health devices, intelligent diagnostics, telemedicine, and emergency response systems [14]. It also examines significant challenges, such as compatibility, power efficiency, data integrity, safety, and ethical considerations. To address these challenges, the authors discuss existing solutions and outline essential future research directions for scalable and sustainable healthcare innovation. Yalli et al. [4] describe the IoT as a concept that envisions all devices being interconnected via the Internet. The IoT offers new opportunities for innovative services and serves as a foundation for future growth. As computer processing power nearly doubles every two years, the IoT sector is experiencing rapid expansion.

Simultaneously, the size and power requirements of devices are halved during this period. This trend creates numerous new possibilities for data exchange and interaction, made feasible by increasingly compact and powerful devices. Adam et al. [8] discuss IoT security, privacy, and trust through a three-tiered IoT design framework. The study examines the security requirements of IoT architectures and the challenges they encounter in establishing a foundation for IoT privacy, safety, and trust [25]. Following this, the research examines current trends aimed at addressing trust, privacy, and safety issues related to IoT devices [26]. Furthermore, it covers the latest developments and strategies for protecting sensitive data and IoT systems from security breaches. The survey concludes with a summary of the current state of IoT safety and the ongoing challenges that still need to be addressed. Gautam et al. [17] highlight significant privacy and security risks associated with IoT connections. This research investigates these issues to identify the most common vulnerabilities and their implications for IoT systems. The research methodology includes risk assessment, data encryption techniques, and security measures [14]. The study identifies several key concerns, including unencrypted communication, insecure firmware, weak authentication, and a lack of security updates. These findings lay the groundwork for real-world improvements to the IoT security landscape by encouraging manufacturers to prioritise security measures, promoting the adoption of standards and regulations, and enhancing user awareness and education [15].

Promsuk [23] discusses a neural network model called the multi-layer perceptron (MLP), which is used to reduce interference from nearby channels within a 2.4 GHz IoT network. The study compares the effectiveness of traditional minimum mean square error (MMSE) methods with the interference mitigation techniques (IMTs) based on the MLP model. By utilising amplitude and fast Fourier transform data as input, the MLP model enhances the reduction of interference. The design of the Internet of Things (IoT) network also considers the effects of route loss and small-scale fading to reflect a more realistic system. The findings reveal that both IMTs employing the MLP model outperform the MMSE filter. Yu et al. [24] highlight the rapid advancements in IoT technologies and their applications in areas like smart homes, the Internet of Vehicles, and industrial IoT. Many emerging smart devices feature simplistic designs, which may leave the perception, transport, and application layers vulnerable to security flaws. As a result, most IoT security analysis frameworks now require additional high-performance devices. Moreover, there has been insufficient focus on new types of malware, such as "mining" attacks, which exploit the computing power of devices [16]. To address these concerns, this article develops and implements an analytical system designed to enhance smart home security. Table 1 summarises research on Next-Generation IoT Security and Privacy Challenges, detailing the methodology, key findings, difficulties encountered, and potential directions for future research.

Table 1: Research on next-generation IoT security and privacy challenges

Author(s)	Focus / Area of Study	Methodology / Approach	Key Findings / Contributions	Challenges and Future Research Directions
Bollineni et al. [3]	IoT in Healthcare Systems	Comprehensive review of smart healthcare architecture and applications	Categorised IoT healthcare domains such as wearables, diagnostics, and telemedicine; identified benefits and limitations	Emphasised the need for scalable, secure, and power-efficient IoT healthcare frameworks
Yalli et al. [4]	IoT Development Trends	Conceptual study of IoT growth and device interconnectivity	Described IoT as the foundation for future digital services with enhanced processing efficiency	Future work should address interoperability and device standardisation
Adam et al. [8]	IoT Security, Privacy, and Trust	Analytical study using a three-tier IoT architecture	Identified privacy and trust challenges, and surveyed current security trends	Recommended: enhancing IoT resilience and developing advanced privacy-preserving mechanisms
Gautam et al. [17]	IoT Vulnerability Analysis	Risk assessment, encryption, and security testing	Highlighted vulnerabilities such as unencrypted communication, weak authentication, and insecure firmware	Suggested stronger legislation, encryption standards, and user security awareness programs
Promsuk [23]	AI-Based IoT Interference Mitigation	Used a Multi-Layer Perceptron (MLP) for interference reduction in 2.4 GHz IoT networks	Demonstrated MLP outperforms MMSE in mitigating interference	Proposed future AI-enhanced methods for real-time IoT signal optimisation
Yu et al. [24]	Smart Home and Industrial IoT Security	Developed an analytical framework for IoT malware detection	Addressed new malware types exploiting device computation (e.g., crypto-mining attacks)	Recommended lightweight yet robust IoT malware defence models

3. Conceptual Framework of Next-Generation IoT Systems

The traditional Internet of Things (IoT) has evolved into next-generation IoT systems, made possible by convergent technologies such as blockchain, edge and fog computing, 5G, and artificial intelligence (AI). These advanced IoT systems facilitate an unprecedented level of machine-to-machine connections, enabling ultra-low latency, real-time data processing, and the handling of massive data volumes. Next-generation IoT is being applied in complex fields, such as smart healthcare, autonomous flying vehicles, robotics for industrial automation, and integrated AI-driven urban transportation systems. Unlike earlier IoT architectures that relied on centralised cloud computing for processing and data interpretation, next-generation IoT systems utilise edge computing. This approach brings computational resources closer to the source of data production, thereby optimising efficiency and responsiveness.

3.1. Evolutionary Characteristics of Next-Generation IoT

The next-generation Internet of Things (IoT) encompasses common uses and needs that can be described using the following six characteristics, often referred to as the "six S's":

- **Syncretic:** This characteristic involves creating a highly dependable and high-performance data transmission system through the vertical and horizontal integration of heterogeneous networks, including both satellite and cellular networks.
- **Speedy:** It emphasises the rapid identification, management, and optimisation of various business services within the IoT landscape.
- **Synergistic:** This approach focuses on collaborative data processing, enabling accurate and real-time analysis of large datasets.
- **Security:** A crucial aspect that provides tailored and comprehensive privacy and security solutions for IoT business services.
- **Simplicity:** This ensures that the system is easy for users, developers, and operators to use, deploy, and manage.
- **Shared:** Utilising a common system architecture allows for the sharing of network resources and capabilities.

By integrating these six characteristics, next-generation IoT aims to enhance performance and usability across various applications.

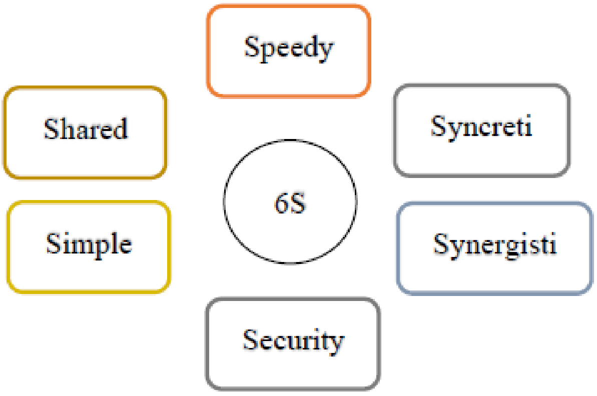

Figure 1: Characteristics of the generation IoT system based on 6S

Considering the next-generation IoT's 6S features, as seen in Figure 1, a new age of intelligent IoT is approaching.

3.2. Key Characteristics of Internet of Things (IoT)

The IoT's most well-liked features include:

The Internet of Things (IoT) has several defining characteristics that make it a transformative technology:

- **Intelligence:** IoT systems exhibit intelligence through the integration of hardware, software, and algorithms. Ambient intelligence enhances this capability by allowing devices to interpret their surroundings, respond appropriately to various situations, and autonomously perform specific tasks.
- **Connectivity:** Connectivity is the backbone of IoT, linking everyday objects into a unified network. This interconnection facilitates seamless communication and data exchange among devices, fostering collective intelligence. Additionally, it ensures interoperability and accessibility across different platforms and systems.

- **Dynamic Nature:** IoT environments are inherently dynamic, as devices continuously collect and exchange data from their surroundings. The operational status of these devices frequently changes due to variations in environmental conditions such as temperature, location, and movement, as well as their connection states—whether they are active, idle, or offline.

3.3. Architectural Trends and Objectives

Numerous IoT designs have been developed, each possessing the attributes necessary to address a specific problem. IoT designs based on hierarchical layers have been generally presented by various scientific organisations for specific application fields. "Tiers" is another name for these strata.

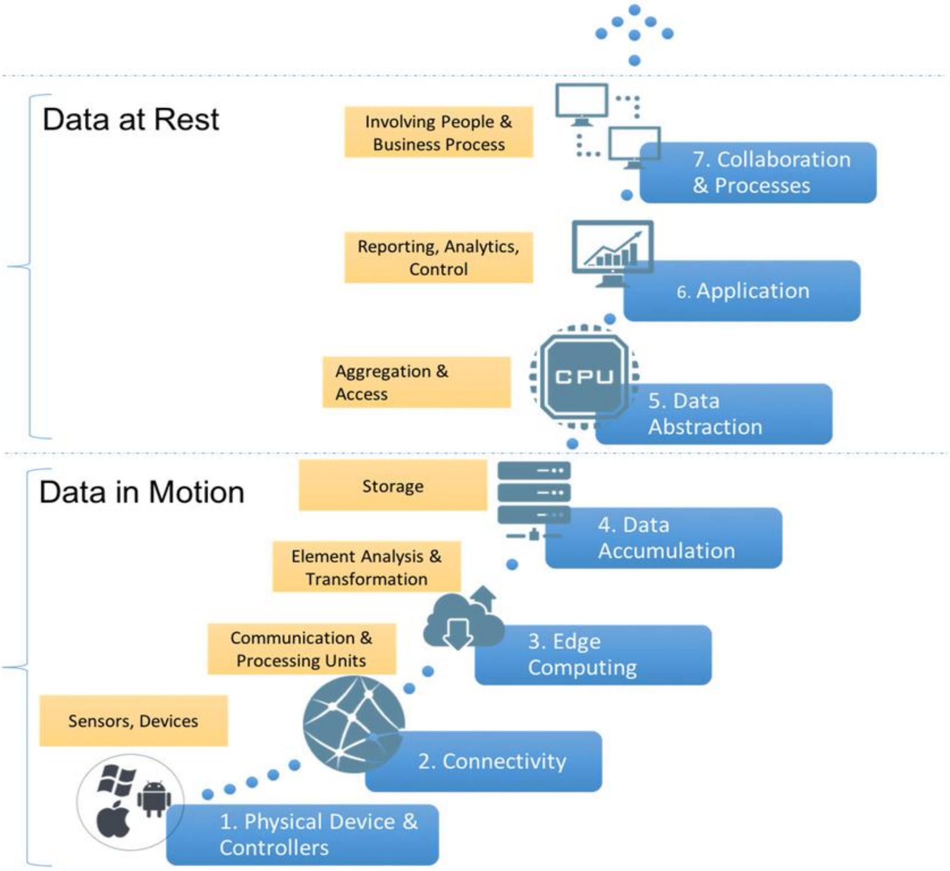
Data at Rest
Involving People & Business Process
7. Collaboration & Processes
Reporting, Analytics, Control
6. Application
Aggregation & Access
CPU
5. Data Abstraction
Data in Motion
Storage
4. Data Accumulation
Element Analysis & Transformation
3. Edge Computing
Communication & Processing Units
2. Connectivity
Sensors, Devices
1. Physical Device & Controllers

Figure 2: Conceptual framework as a reference model of an IoT system proposed by CISCO

To illustrate different functional blocks, relationships, and integration, a reference model may be used. Figure 2 illustrates the seven layers that comprise Cisco's reference model. The seven-level IoT architecture illustrates a layered approach from physical devices (Level 1) to business processes (Level 7). This diagram Figure 2 shows the seven levels of intelligent IoT operations, starting with data generation by sensors and controllers and progressing through connectivity (Level 2), processing at the edge or fog (Level 3), storage (Level 4), aggregation (Level 5), analysis at the application level (Level 6), as well as finally, integration of human and business processes (Level 7) (Table 2).

Table 2: Applications of IoT systems in industry and cases

Industry	Application Area	IoT Use Cases / Examples
Healthcare	Remote patient monitoring, smart diagnosis	Wearable sensors for heart rate and glucose monitoring; IoT-based telemedicine systems
Agriculture	Smart farming, precision agriculture	Soil moisture and crop monitoring using IoT sensors, along with automated irrigation systems.
Manufacturing	Industrial automation, predictive maintenance	Smart factories using IoT-enabled machines, monitoring equipment for fault detection

Transportation	Smart traffic management, fleet monitoring	Connected vehicles, real-time traffic monitoring, and route optimisation
Energy	Smart grids, energy optimisation	IoT-enabled power meters; real-time monitoring of energy consumption and renewable sources
Retail	Inventory management, customer analytics	Smart shelves; IoT-based point-of-sale (POS) systems and personalised marketing
Smart Cities	Infrastructure monitoring, public safety	IoT for street lighting control, waste management, and air quality monitoring
Home Automation	Smart appliances, home security	Connected thermostats; IoT-based surveillance and smart lighting systems
Logistics	Supply chain tracking, asset management	IoT sensors for shipment tracking; warehouse monitoring systems

In next-generation automotive systems, IoT enables intelligent communication, advanced driver assistance systems, autonomous driving, and real-time diagnostics, ultimately driving safer, smarter, and more efficient transportation.

4. Analysis of Security Challenges and Privacy Issues in Next-Generation IoT

The reliability of IoT-based applications primarily hinges on their ability to effectively address security and privacy issues. Existing vulnerabilities within IoT systems serve as significant obstacles to their widespread adoption. Establishing user trust in IoT applications, connected devices, and related services necessitates strong security and privacy mechanisms. While several studies have explored privacy and security concerns in IoT systems, the introduction of AI-enabled frameworks, which can analyse distributed data across networks, has brought about new challenges regarding trustworthiness. The integration of AI with Internet-connected systems enhances data accessibility, but without intelligent and secure system designs, this can further jeopardise user privacy and security.

4.1. Privacy Through Data Usage Control

The concept of access control can be expanded to include data usage management. Data usage control systems monitor and label data throughout its entire lifecycle, going beyond the limitations of traditional access control mechanisms. These systems enforce fine-grained restrictions to protect privacy in large datasets used for analytics and machine learning applications. The main advantage of data usage control is that it empowers individuals to decide how their data is used, even when third parties manage it. This approach also supports compliance with data protection regulations, such as the EU’s General Data Protection Regulation (GDPR). Future IoT architectures must ensure comprehensive privacy protection, enable local control over data exposure, and facilitate secure interoperability across diverse systems.

4.2. IoT-Based Physical Security Systems

IoT-enabled physical security systems are crucial for safeguarding remote and high-risk areas, such as border regions, where access and monitoring can be challenging due to harsh environmental conditions. An integrated safety system has been developed using embedded technology and IoT principles. This system employs a Raspberry Pi and ESP8266 as control units, managing components such as motors, FLIR thermal cameras, and night-vision modules to achieve a 180° scanning capability. Additional components, including torches and laser modules, enhance visibility under various conditions. Motion, sound, and photoelectric sensors are deployed to detect intrusions, triggering an automated electric barrier and alert system. A dual-channel wired and wireless communication network ensures real-time connectivity with the control centre, enabling comprehensive surveillance and reliable detection even in adverse weather conditions, such as fog, rain, and darkness.

4.3. Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSNs) are a fundamental component of the Internet of Things (IoT) architecture. They consist of numerous sensor nodes and actuators that enable sensing, data processing, and transmission functions. These networks support a variety of IoT applications, including healthcare, logistics, habitat monitoring, military systems, and environmental forecasting. However, the broadcast nature of wireless communication exposes WSNs to several security threats:

- **Physical Attacks:** Unauthorised physical access to sensor nodes can lead to data manipulation or tampering, thereby compromising the network's overall functionality.
- **Node Replication:** Attackers may duplicate a legitimate node ID and introduce it into the network, resulting in misrouting, inaccurate sensing data, and network disruption.

- **Selective Forwarding:** Malicious nodes may selectively drop or alter packets instead of forwarding them. This makes it difficult to detect the source of the attack and compromises data integrity.

4.4. AI/ML Techniques and Threat Detection

Machine Learning (ML) Techniques: ML algorithms play a crucial role in identifying vulnerabilities within IoT devices. Supervised learning techniques improve the accuracy of detecting known and unknown threats while minimising false positives. Unsupervised methods, such as clustering and reconstruction-based models, are employed to identify anomalies without labelled data. Reinforcement learning is also being explored for adaptive, real-time decision-making in complex and dynamic IoT environments. AI-Based Threat Detection: Artificial intelligence (AI) enhances IoT security by automating the detection and response to cyberattacks. AI-driven models integrate ML-based intrusion detection systems (IDS) and anomaly detection using real-world datasets. These systems enable proactive threat identification and mitigation, improving the resilience of IoT networks against evolving cyber threats.

4.5. Security Challenges in IoT

While IoT technologies provide significant advantages, several critical challenges must be addressed to enable secure and sustainable deployment:

- **Security and Privacy:** The vast interconnectivity of IoT devices increases their exposure to cyber threats. To prevent unauthorised access and data breaches, it is essential to implement strong authentication measures, encryption, and privacy-preserving mechanisms.
- **Interoperability and Standards:** The diversity of IoT devices and vendors can lead to compatibility issues. The lack of standardised communication protocols complicates the integration of devices and the exchange of data.
- **Scalability and Network Management:** As IoT ecosystems grow, managing large-scale networks and maintaining efficient connectivity become increasingly complex.
- **Big Data Management:** IoT generates enormous volumes of data that must be processed, stored, and analysed efficiently. Ensuring data quality and real-time analytics remains a major challenge.
- **Power Consumption and Energy Efficiency:** Many IoT devices are battery-powered; therefore, optimising energy consumption is crucial to extending their lifespan.
- **Ethical and Social Implications:** IoT raises ethical concerns regarding user consent, data ownership, and potential surveillance risks.
- **Cost and Return on Investment:** High infrastructure, deployment, and maintenance costs may impede the widespread adoption of IoT technology.
- **Regulatory and Legal Compliance:** IoT implementations must comply with data protection laws and industry-specific regulations to ensure lawful and ethical operations. Addressing these challenges requires collaboration among technology developers, policymakers, standardisation bodies, and end users. Through coordinated efforts, the full potential of IoT can be realised while maintaining security, interoperability, and societal trust.

5. Approaches for Mitigation and Defence in Next-Generation IoT Systems

Legislative Compliance and IoT Security Frameworks: Organisations must comply with various regulatory frameworks, such as HIPAA, SOX, ISO 27000, and PCI, to ensure effective information security practices. Each of these compliance standards targets specific areas: HIPAA focuses on the protection of healthcare data, SOX addresses business and financial reporting, PCI regulates payment card transactions, and ISO 27000 provides guidelines for organisational information security management. Network Access Control (NAC) has become a crucial tool for enforcing compliance. It does this by validating endpoint security, managing patches and antivirus updates, and integrating authentication systems. NAC continuously monitors devices at the network layer and allows access only when compliance criteria are met. To further enhance IoT security, multiple strategies are employed, including Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), and strong authentication techniques such as biometrics and blockchain. Lightweight cryptography and AI-driven intrusion detection enhance data protection, while privacy-preserving technologies, such as differential privacy and federated learning, help safeguard user information. Additionally, secure over-the-air (OTA) updates and blockchain-based trust models ensure the integrity of firmware and transactional operations.

5.1. Cryptographic Techniques

Securing Internet of Things (IoT) environments presents unique challenges due to constraints related to processing power, memory, and real-time performance. Traditional cryptographic algorithms are often too resource-intensive for these devices, which necessitates the adoption of lightweight cryptography. These methods are optimised to minimise computational and energy overhead while still maintaining essential security properties. Effective cryptographic mechanisms must ensure the following:

- **Confidentiality:** Only authorised entities can access the transmitted data.
- **Integrity:** Data remains unchanged during transmission.
- **Authentication:** The identities of both the sender and receiver are verified.
- **Non-repudiation:** Entities cannot deny their participation in communication. Lightweight cryptography meets these objectives while complying with efficiency and security requirements, making it highly suitable for widespread IoT deployments.

5.2. Security Mechanisms in IoT Environments

IoT environments employ a variety of authentication and key management mechanisms to ensure data confidentiality and establish trust among devices. These mechanisms can be classified into three major categories:

- Authentication Protocols for IoT Environments Mutual authentication schemes have been developed using chaotic maps and authenticated encryption to establish secure session keys for IoT-based crowdsourcing. Formal analyses, including Random Oracle Model (ROM) validation and evaluations using the Scyther tool, confirm that the protocols are resilient against impersonation, replay attacks, data leakage, and man-in-the-middle (MITM) attacks.
- Authentication and Key Agreement Protocols Deep learning (DL)-based techniques for key agreement and authentication have been introduced for Internet of Things (IoT) and Long-Term Evolution (LTE) devices. These systems dynamically generate shared secret keys using deep residual networks, protecting against redirection, replay, and denial-of-service attacks. While DL improves detection accuracy and response times, challenges such as scalability and resource overhead persist, particularly in satellite or large-scale networks.
- Key Agreement Protocols for IoT Environments Key agreement schemes, such as those based on Diffie–Hellman protocols, are designed to secure communication in decentralised edge computing environments. Evaluations using the Random Oracle Model (ROM) and the ProVerif tool have demonstrated that these protocols are resistant to replay, impersonation, eavesdropping, and stolen verification attacks. They demonstrate robust performance even under the resource constraints typical in IoT conditions.
- Access Control Mechanisms and Privacy-Preserving Techniques Effective IoT security frameworks depend on fine-grained access control, privacy preservation, and secure firmware management.

Access Control: Models such as Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), and Capability-Based Models manage user and device permissions by assigning roles, attributes, or capabilities. These models ensure scalable, least-privileged access within dynamic IoT networks.

Privacy-Preserving Techniques: Differential privacy introduces statistical noise to safeguard individual identities during data analysis. Additionally, federated learning enables decentralised model training without the need to share raw data, thereby supporting regulatory compliance and minimising exposure risks.

Secure Firmware Updates: Authorised and tamper-resistant over-the-air (OTA) update mechanisms protect device integrity and enhance resilience against firmware-based attacks. Collectively, these mechanisms strengthen confidentiality, integrity, and availability across extensive and heterogeneous IoT ecosystems.

6. Conclusion and Future Work

This study offers a thorough examination of next-generation Internet of Things (IoT) technologies, including their design principles and the evolving security landscape. Emerging technologies such as Artificial Intelligence (AI), blockchain, 5G, and edge computing have significantly transformed traditional IoT systems, improving operational efficiency, enabling intelligent automation, facilitating real-time data processing, and supporting autonomous decision-making. However, IoT environments still face ongoing challenges related to privacy, security, and trust due to their resource constraints and the diverse application domains. As a result, deploying advanced cryptographic techniques, AI-driven threat detection mechanisms, and privacy-preserving frameworks is essential for creating secure, reliable, and trustworthy IoT ecosystems. Nonetheless, this review has certain limitations, such as the absence of real-world implementation analysis and a lack of comparative performance evaluation across different IoT sectors. Additionally, the rapidly evolving nature of cyber threats requires security frameworks that are adaptive and continuously updated, which this study does not discuss in detail. Future research should focus on the practical development of secure, scalable, and interoperable next-generation IoT architectures, particularly in high-risk sectors such as healthcare, autonomous vehicles, and smart city infrastructures. Researchers should focus on designing lightweight yet robust encryption algorithms, establishing cross-layered security models, and standardising communication protocols to ensure interoperability and reliability. Moreover, it will be essential to integrate ethical governance frameworks that emphasise transparency, user consent, and data ownership. Finally, incorporating privacy-preserving learning models, such as federated learning, and adopting quantum-safe cryptographic solutions represent promising directions for enhancing the resilience, sustainability, and long-term trustworthiness of IoT ecosystems.

Acknowledgment: The authors collectively express their gratitude to all contributors whose insights and support strengthened the quality and completion of this research.

Data Availability Statement: The datasets generated and analyzed during this study are available from the corresponding authors upon reasonable request, ensuring transparency and academic integrity.

Funding Statement: This research was carried out solely through the collaborative efforts of the authors, without reliance on any external financial assistance.

Conflicts of Interest Statement: The authors jointly declare that they have no competing interests that could have influenced the design, analysis, or interpretation of the study.

Ethics and Consent Statement: All authors affirm that the research was conducted in accordance with ethical standards, and that informed consent was obtained from all participants involved.

References

1. V. Prajapati, “Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability,” *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, pp. 1011–1020, 2025.
2. S. Szymoniak, J. Piątkowski, and M. Kurkowski, “Defense and Security Mechanisms in the Internet of Things: A Review,” *Appl. Sci.*, vol. 15, no. 2, p. 499, 2025.
3. C. Bollineni, M. Sharma, A. Hazra, P. Kumari, S. Manipriya, and A. Tomar, “IoT for Next-Generation Smart Healthcare: A Comprehensive Survey,” *IEEE Internet Things J.*, vol. 12, no. 16, pp. 32616 - 32639, 2025.
4. J. S. Yalli, M. H. Hasan, L. T. Jung, A. I. Yerima, D. A. Aliyu, and U. D. Maiwada, “A Systematic Review for Evaluating IoT Security: A Focus on Authentication, Protocols and Enabling Technologies,” *IEEE Internet Things J.*, vol. 12, no. 12, pp. 18908 - 18928, 2025.
5. V. Thangaraju, “Security Considerations in Multi-Cloud Environments with Seamless Integration: A Review of Best Practices and Emerging Threats,” *Trans. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 226–238, 2024.
6. H. S. Chandu, “Enhancing Manufacturing Efficiency: Predictive Maintenance Models Utilizing IoT Sensor Data,” *International Journal for Science and Advance Research In Technology*, vol. 10, no. 9, pp. 58–66, 2024.
7. S. Pandya, “Integrating Smart IoT and AI-Enhanced Systems for Predictive Diagnostics Disease in Healthcare,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 2093-2105, 2024.
8. M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, “A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems,” *IEEE Access*, vol. 12, no. 3, pp. 57128–57149, 2024.
9. S. M. Nadeem, D. D. Rao, A. Arora, Y. V. Dongre, R. K. Giri, and B. Jaison, “Design and Optimization of Adaptive Network Coding Algorithms for Wireless Networks,” *in 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kamand, India, 2024.
10. C. Gilbert and M. A. Gilbert, “AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities,” *International Journal of Research Publication and Reviews*, vol. 5, no. 11, pp. 219-236, 2024.
11. A. Amrita, C. P. Ekwueme, I. H. Adam, and A. Dwivedi, “Lightweight Cryptography for Internet of Things: A Review,” *EAI Endorsed Trans. Internet Things*, vol. 10, no. 3, pp. 1-9, 2024.
12. F. Stodt and C. Reich, “Bridge of Trust: Cross Domain Authentication for Industrial Internet of Things (IIoT) Blockchain over Transport Layer Security (TLS),” *Electron*, vol. 12, no. 11, p. 2401, 2023.
13. Y. Lu, “Security and Privacy of Internet of Things: A Review of Challenges and Solutions,” *J. Cyber Secur. Mobil.*, vol. 12, no. 6, pp. 813–844, 2023.
14. M. A. Al Kabir, W. Elmedany, and M. S. Sharif, “Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques,” *J. Cyber Secur. Technol.*, vol. 7, no. 4, pp. 199–223, 2023.
15. P. Chatterjee, “Real-Time Payment Systems and their Scalability Challenges,” *Iconic Res. Eng. Journals*, vol. 6, no. 12, pp. 1461–1470, 2023.
16. S. Kumar, K. Kanchan, A. Kumar, and P. Aggarwal, “Internet of Things (IoT) Applications and Challenges: A Review,” *Int. J. Eng. Sci. Emerg. Technol.*, vol. 11, no. 2, pp. 359–367, 2023.

17. K. K. S. Gautam, R. Kumar, R. Yadav, and P. Sharma, “Investigation of the Internet of Things (IoT) Security and Privacy Issues,” *in 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2023.
18. S. Garg, “Next-Gen Smart City Operations with AIOps and IoT: A Comprehensive look at Optimizing Urban Infrastructure,” *J. Adv. Dev. Res.*, vol. 12, no. 1, pp. 1-9, 2021.
19. A. Goyal, “Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration,” *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 396–402, 2021.
20. Y. Li, Y. Ding, Y. Qie, C. Zhang, W. Chen, and S. Ma, “Next-generation Internet of Things: Conception of Key Characteristics and Typical Applications,” *in 2021 International Conference on Education, Management, Economics, Law and Social Sciences (EMELS)*, Moscow, Russia, 2021.
21. S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, “Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review,” *IEEE Sens. J.*, vol. 21, no. 22, pp. 24920–24932, 2021.
22. M. C. Gómez, A. M. L. Echeverry, and P. A. V. Sánchez, “Review of the use of IoT technologies and devices in physical security systems,” *Ing. Y Compet.*, vol. 24, no. 1, pp. 1–19, 2021.
23. N. Promsuk, “Development of Interference Mitigation Techniques based Artificial Neural Network for IoT Network,” *in 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, Chiang Mai, Thailand, 2021.
24. R. Yu, X. Zhang, and M. Zhang, “Smart Home Security Analysis System Based on The Internet of Things,” *in 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Nanchang, China, 2021.
25. A. K. R. Ayyadapu, “Scalable machine learning approaches for real-time big data processing in IoT networks,” *AVE Trends Intell. Comput. Lett.*, vol. 1, no. 2, pp. 51–61, 2025.
26. A. R. P. Reddy, “AI-powered anomaly detection for cybersecurity threats in multi-cloud infrastructure,” *AVE Trends Intell. Comput. Syst.*, vol. 2, no. 2, pp. 77–86, 2025.