Journal of Global Research in Electronics and Communication
Volume 1, No. 6, June 2025
Available Online at: www.jgrec.com
REVIEW ARTICLE

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

Mrs. Neha Upadhyay,
Assistant Professor, Department of Computer Applications
IIS University,Bhopal(M.P.)
neha.upadhyay887@gmail.com

***Abstract*—The Internet of Things (IoT) has quickly developed into a force that is revolutionizing several industries, enabling seamless interconnection and autonomous communication among smart devices. Artificial intelligence (AI), edge/fog computing, blockchain, as well as 5G/6G communication networks are some of the cutting-edge technologies that are combining to create next-generation IoT systems. The effectiveness, scalability, and intelligence of IoT networks have been greatly increased by these developments, enabling real-time data analytics as well as decision-making. This study offers a thorough examination of the architecture, key enabling technologies, and security mechanisms shaping next-generation IoT. It also looks at the integration of intelligent systems for adaptive control and highlights prominent use cases in domains like Autonomous transportation, smart healthcare, as well as industrial automation. In addition, the paper outlines the evolving role of data-driven architectures and decentralized frameworks in creating more autonomous and self-healing IoT systems. By synthesizing current trends and technological advancements, this paper provides academics and practitioners with a fundamental resource for creating resilient and future-ready IoT ecosystems.**

***Keywords*—Next-generation IoT, Smart devices, Edge computing, 5G/6G, Artificial intelligence, Blockchain, IoT architecture, Security mechanisms, Smart cities, Industrial IoT**

I. INTRODUCTION

The development of several technological fields, including wireless communications, embedded computing, broadband internet access, and automated tracking and identification, has led to the integration of intelligent objects into their daily life [1]. IoT describes the network connectivity of everyday objects in many different contexts, such as smart homes, industrial operations, health monitoring, and environmental monitoring [2]. Key components of the IoT ecosystem that contribute to increased efficiency, security, as well as innovation include blockchain technology, AI, ML, cloud computing, and humanitarian logistics. In the IoT, blockchain technology guarantees safe and transparent transactions [3], humanitarian logistics, on the other hand, makes use of the IoT to organize the supply of relief in times of crisis. With cloud computing, IoT data can be easily stored, accessed, and analyzed thanks to its scalable computational and storage capabilities.

The development of several technological fields in recent years, including wireless communications, embedded computing, broadband internet access, and automated tracking and identification, has led to the introduction of intelligent objects into their daily life [4]. The term IoT describes how the Internet is integrated with physical objects found in a variety of contexts, such as smart homes, industrial operations, health monitoring, and environmental monitoring. In the IoT ecosystem, blockchain, cloud computing, AI, ML, and humanitarian logistics are essential for increasing productivity, security, and creativity [2]. While humanitarian logistics makes use of IoT capabilities to manage assistance distribution during catastrophes, blockchain guarantees safe and transparent transactions between IoT devices [5]. For smooth communication and analysis of data produced by the Internet of Things, cloud computing offers scalable processing and storage resources.

IoT gadgets are becoming increasingly integral to their everyday lives as the technology that powers them advances at a dizzying rate. Cybercriminals see IoT devices as easy prey because of their inherent insecurity caused by their diminutive size. They only support tiny electronic components, including memory and storage, low-powered embedded microcontrollers, simple sensors, actuators, as well as power supply units [6]. Operating systems that are basic or simple, low power consumption requirements, and computational capacity limitations, in addition to this size restriction, often inhibit the adoption of sophisticated or even contemporary cryptographic algorithms, much less full security solutions [7]. Furthermore, the vast majority of IoT devices still only have basic protection built in, which surprises cybersecurity professionals and investigators. This is especially true for mass-produced, inexpensive, off-brand products that perform a few necessary functions for both individual and commercial sectors.

A. Structure of the Paper

The paper's outline is provided below: Section II outlines the evolution and architecture of next-generation IoT systems. Section III details key security challenges and privacy threats, while Section IV discusses mitigation techniques, including cryptographic and AI-based approaches. Section V reviews related literature, and Section VI ends with important takeaways and recommendations for the future.

II. OVERVIEW OF NEXT-GENERATION IOT SYSTEMS

The more conventional IoT has given way to next-generation IoT systems, which are made possible by convergent technologies like blockchain, edge as well as fog computing, 5G, as well as AI [8]. Next-generation IoT systems enable an unprecedented level of machine-to-machine connections while supporting ultra-low latency, real-time data processing, and massive data volume [9]. This

capability is being applied in complex areas such as smart healthcare, flying autonomous vehicles, autonomous wharf and factory robotics for industrial automation, and integrated artificial intelligent urban transportation systems; whereas earlier IoT architectures relied on centralized clouds to process and interpret objects and data in IoT ecosystems, next-generation IoT with edge computing provides computational resources closer to, or at, the source of the data production, and hence optimizes efficiency and responsiveness.

A. *Evolutional Characteristics of Next-generation IoT*

The common uses and needs of the next-generation Internet of Things, the future The following six S's can be used to describe IoT: (1) Syncretic: builds a highly dependable and high-performance data transmission system by vertically and horizontally integrating heterogeneous networks, including satellite and cellular networks; (2) Speedy: expeditiously realizes the identification, management, and optimization of the rich business services of IoT [10]; (3) Synergistic: Uses collaborative data processing to implement accurate and real-time analysis of large amounts of data; (4) security: enables tailored and all-encompassing privacy and security for IoT business services; as well as (5) simplicity: enables a system that is simple for users, developers, and operators to use, deploy, and administer [11]; (6) Shared: Utilizing a common system architecture, this approach enables the sharing of network resources and capabilities.

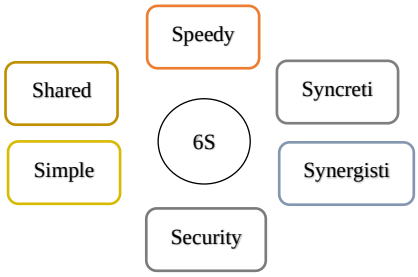

Fig. 1. Characteristics of next generation IoT system based on 6S

Considering the next-generation IoT's 6S features [12], As seen in Figure 1, a new age of intelligent IoT is approaching.

B. *Key Characteristics of Internet of Things (IoT)*

The IoT's most well-liked features include [13]:

- **Intelligence:** The IoT is intelligent due to its mix of hardware, software, and algorithms. In the IoT, ambient intelligence broadens its capabilities by allowing devices to respond intelligently to a situation and help them do certain tasks.
- **Connectivity:** Connectivity is what enables the IoT by bringing together everyday objects. Because basic object-level interactions in IoT networks contribute to collective intelligence, Connectivity between these items is crucial. It enables network compatibility as well as accessibility for the products.
- **Dynamic Nature:** The primary purpose of the Internet of Things is to collect data from its environment, which is achieved by the always-changing environment around the devices. The statuses of these devices vary dynamically, changing context (temperature, location, and speed), when they are connected or detached, as well as when they sleep or wake up.

C. *Architectural Trends and Objectives*

Numerous IoT designs have been created, each having the attributes required for the problem being solved. IoT designs based on hierarchical layers have generally been presented by various scientific organizations for certain application fields. "Tiers" is another name for these strata [14]. To illustrate different functional blocks, relationships, and integration, a reference model may be used. Figure 2 depicts the seven layers that make up Cisco's depiction of a reference model.

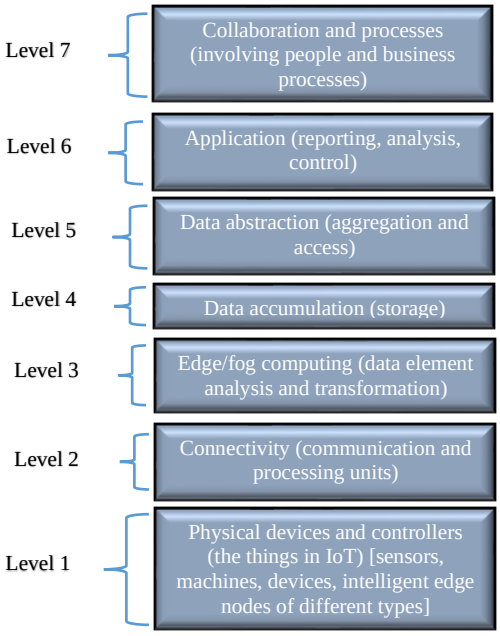

Fig. 2. Conceptual framework as reference model of an IoT system proposed by CISCO

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).

D. *Applications of IoT Systems*

IoT has found significant applications across multiple domains, each is using networked gadgets to increase productivity, automation, as well as decision-making shown in Table I. The following are examples of industrial applications of IOT systems:

TABLE I. APPLICATIONS OF IOT SYSTEMS WITH INDUSTRY AND CASES

Industry	Use case
Healthcare	IoT makes it possible to treat chronic diseases and remotely monitor patients with wearable technology and smartphone applications, while smart hospital systems use connected sensors for asset tracking[15], predictive maintenance, and EHR integration to enhance care and efficiency.
Smart Cities	In smart cities, IoT supports traffic management, smart waste collection, and environmental monitoring, while adaptive street lighting enhances energy efficiency.
Industrial IoT (IIoT)	IoT in industries enables predictive maintenance, real-time automation, enhanced supply chain visibility, and improved workplace safety through connected sensors and wearables.

Automotive	IoT in automotive systems enables V2V and V2I communication, ADAS, autonomous driving, fleet tracking, and diagnostics, enhancing safety, efficiency, and automation.

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

III. Security Challneges and Privacy Threats in Next-Generation in IoT

IoT-based apps' usefulness is evaluated based on their reliability in managing security and privacy concerns. The existing IoT's privacy and security problems might be a major factor in preventing the widespread adoption of the technology [16]. It is crucial to understand that gaining customers' trust in IoT apps, linked devices, and the associated services depends on security and privacy rights. IoT-based device privacy and security have been examined by several academics [17]. However, the ubiquitous AI-enabled frameworks, which have the ability to handle and analyze information from any location inside the network, are directly responsible for the trustworthiness issues. A crucial component that aids in their understanding of this problem is an AI-enabled network with Internet connectivity, as it makes it easier to acquire user information without an intelligent system design.

A. Privacy through Data Usage Control

The concept of access control may be extended to manage the usage of data. Going forward, data usage control systems will monitor as well as label data at every step of its processing lifetime, beyond the reach of conventional access control concepts [18]. It will develop fine-grained usage restrictions to guarantee that large data sets' privacy attributes are preserved when they are used for analytics and learning algorithms. Data usage control's main advantage is that it allows individuals to have control over how their data is used, even while it's being managed by a third party. Conforming to different national legislation (such the General Data Protection Regulation of the EU) would be made easier with this. Future IoT system implementations must provide end-to-end privacy guarantees, can control data exposure locally, and communicate with a variety of different systems.

B. Physical Security Systems based on IoT

Border regions use the most comprehensive and expensive systems, despite their lower frequency. Since access and monitoring are challenging in these regions due to the severe weather, A group of sensors, actuators, and controllers was used to build a smart safety system with intrusion detection capability using embedded technology as well as the IoT. The system is managed by a Raspberry Pi and an ESP8266 acting as controllers for the various devices. A motor, FLIR thermal cameras (Lepton), as well as a night camera were installed to provide 180° scanning. A torch and a laser gun were used in conjunction with the night camera to allow for monitoring in a range of scenarios [19]. Sensors for motion, sound, as well as photoelectric reticence were installed at the border to detect and trigger an electric barrier and alert system. In conclusion, it is worth noting that a dual-channel wired and wireless network guarantees communication with the control center. Benefits of this system include scanning the whole region and guaranteeing monitoring and detection in a variety of weather situations, including fog, rain, and darkness.

C. Wireless Sensor Network (WSNs)

The building blocks of WSNs include actuators, which are computer parts, and sensor nodes, which are a lot of little cells [20]. Sensing, data processing, and transmission are the three primary functions of sensor nodes. Healthcare systems, logistics, habitat monitoring, military applications, environmental observation, and forecasting are just a few of the many IoT uses for WSNs [21]. The broadcasting transmission medium makes WSNs susceptible to assaults. The main dangers to WSNs are:

- **Physical Attacks:** Everything needs a sensor to function to its fullest. Physical access without authorization is difficult to stop. Hackers might change node or sensor information, endangering the functionality of the whole sensor networks.
- **Node Replication:** In this attack, a current node ID is copied to a network that has sensors. The network disconnects because of node duplication, packets are misrouted, or inaccurate sensor measurements are recorded. Consequently, a sensor network's ability to operate is disrupted.
- **Selective Forwarding:** Messages in WSN are forwarded to the appropriate recipient via the nodes. In this kind of assault, a rogue node selectively delivers packets. Not all emails need to be forwarded; others may be simply thrown away. After modifying the packets arriving from a select few nodes, the message is delivered to the remaining nodes. As a result, identifying the attacker is challenging.

D. AI/ML Techniques and Threat Detection

Machine Learning (ML) Techniques: The research identifies security flaws in IoT devices using supervised learning techniques, with an emphasis on lowering false positives and increasing accuracy in identifying known and undiscovered threats. Additionally, to find anomalies without labelled data, unsupervised learning methods like reconstruction-based models and clustering are used [22]. Additionally, reinforcement learning is being investigated to facilitate in-the-moment decision-making in intricate, dynamic settings.

AI-Based Threat Detection: The study looks on cyberattack detection and mitigation systems driven by AI. This involves using ML techniques to automate the identification of possible threats, especially via the use of real-world data sets in anomaly detection as well as IoT networks using intrusion detection systems.

E. Security Challenges in IOT

The IoT offers numerous benefits, but before it can be effectively used and broadly accepted, several problems must be resolved. The IoT presents many major issues, some of which are listed below [23]:

- **Security and privacy:** IoT devices' widespread usage and connection make them vulnerable to cybersecurity threats. To stop privacy violations, illegal access, and data breaches, robust security measures must be in place.
- **Interoperability and Standards:** The IoT uses a vast array of goods from several providers [24]. Interoperability issues and the absence of standardized protocols may make it more difficult to integrate and communicate devices and systems effectively.

- **Scalability and Network Management:** Managing the scalability and IoT system network design becomes challenging as the number of linked devices increases quickly.
- Massive amounts of data are produced by the IoT and must be managed efficiently, stored, processed, and evaluated. It is very difficult to manage real-time data streams, guarantee data quality, and derive actionable insights from the data gathered.
- **Power Consumption and Energy Efficiency:** Since many IoT devices run on batteries, reducing power consumption is essential to prolonging their life.
- **Ethical and Social Implications:** The IoT presents ethical and societal issues, including permission, data ownership, as well as surveillance danger.
- **Cost and Return on Investment:** Infrastructure setup, device deployment, and data management application installation may drive up the initial cost of implementing IoT solutions.
- **Regulatory and Legal Considerations:** IoT implementations must comply with a number of rules, including those pertaining to privacy, data protection, as well as industry-specific requirements.

Many stakeholders, including technology companies, legislators, standards organizations, and end users, must work together to address these issues. Through proactive resolution of these issues, the Internet of Things' full potential might be achieved while maintaining a safe, compatible, and socially acceptable IoT environment.

IV. Mitigation Techniques and Defence Mechanisms in IoT Solutions

Various legislative compliances, such as HIPAA, SOX, ISO27000, PCI, etc., must be satisfied to guarantee that organizations give information security the attention it needs [25]. Several compliance criteria must be fulfilled, including: Business compliance is covered by Sarbanes-Oxley (SOX), medical records and information are covered by HIPAA, credit card transactions and sales (used in retail chains, etc.) are covered by PCI, and corporate security requirements are covered by ISO27000. Network Access Control (NAC) is a notion that is increasingly crucial for verifying and enforcing security standards. NAC handles patch and antivirus administration, authentication integration, and endpoint security posture checks. Users may only access network resources if the intended security rules have been followed. NAC operates at the network layer and regularly assesses the security posture. Access controls (ABAC, RBAC), strong authentication (biometric, blockchain), lightweight cryptography, and AI-based intrusion detection all contribute to improved IoT security. Privacy is preserved via differential privacy and federated learning, while secure OTA updates and blockchain ensure trusted operations and transactions.

A. Cryptographic Techniques

The problems of IoT devices make it difficult to protect them using cryptographic techniques. When building a cryptographic method to safeguard the data in the devices, IoT devices must have real-time reaction times and be compact in terms of memory, processing power, and physical space. While cryptographic techniques are used to safeguard data, some of them are insufficient to safeguard specialized devices, like the Internet of Things; this is where lightweight cryptography enters the picture. The approaches of lightweight cryptography are designed to be employed on ubiquitous devices with minimal resource requirements. For algorithms to be approved for use in safeguarding data on IoT devices, they must meet security and algorithmic requirements. For a cryptographic technique to be approved, it must provide secrecy, meaning that only the sender and the recipient may access the data. Integrity in which data transmission does not need modification. Both the client and the information may be verified, allowing for authentication. Non-repudiation prevents the user from contesting their interaction with the sent data [26].

B. Security Mechanisms in IoT Environments

The key agreement and authentication techniques appropriate for IoT situations are summarized in this section. These procedures are divided into three groups in this study. The authentication processes are carried out via the first group of protocols. Both the key agreement and authentication processes are carried out by the protocols in the second group. The protocols in the 3rd category only execute the primary agreement procedures:

1) Authentication Protocols for IoT Environments

A mutual authentication mechanism that establishes session keys for crowdsourcing. Both authenticated encryption and chaotic maps were used in their study. According to them, an informal security study as well as ROM validation make the protocol safe [27]. To guarantee the safety of the suggested protocol, they additionally used the Scythe tool. The aforementioned studies proved that the suggested protocol provides security services, including anonymity, untraceability, and information and message integrity. The Temporary parameter. Additionally, this protocol guards against impersonation, replay, leakage, as well as man-in-the-middle (MITM) attacks.

2) Authentication and Key Agreement Protocols for IoT Environments

A method of key agreement & authentication specifically designed for IoT as well as LTE devices that use DL. The protocol uses a technique for creating dynamic shared secret keys based on Deep Residual Networks [28]. The authors have verified that the suggested protocol safeguards against redirection, MITM, replay, as well as denial-of-service attacks in addition to preventing signaling congestion. Attack detection rates and response times might be enhanced with the use of DL methods. However, The scalability as well as resource availability of satellite-based technology might potentially be problematic, leading to potentially significant extra expenses.

3) Key Agreement Protocols for IoT Environments

An essential protocol for enhancing the security of communication in Decentralized Edge Computing Networks. The Diffie-Hellman method is a computational protocol. The ROM model as well as the Prove it tool were used by the authors to evaluate the protocol's security. Attacks like replay, denial of service, impersonation, stolen verification, and eavesdropping are all prevented by the protocol's architecture. The team concluded that their technique works well in IoT settings with limited power and resources.

4) Access Control Mechanisms with pricy preserving techniques

Access control mechanisms, privacy-preserving techniques, as well as safety firmware updates from the

cornerstone of robust IoT security frameworks. The Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) models are two examples of access control, and Capability-Based Models are vital for regulating user and device permissions based on attributes, roles, or explicitly granted capabilities, thereby ensuring fine-grained, scalable, and least-privilege access in dynamic IoT environments. To safeguard user privacy, techniques like differential privacy introduce noise into datasets for secure aggregate analysis, whereas federated learning ensures regulatory compliance and reduces exposure risks by allowing decentralized model training without sharing raw data. At the same time, authorized and tamper-resistant methods of providing security fixes and feature enhancements, secure firmware and over-the-air (OTA) updates are vital for maintaining device integrity. Collectively, these strategies enhance confidentiality, access control, and resilience across heterogeneous and large-scale IoT systems.

V. Literature Review

The literature on the IoT in healthcare and smart systems delves into recent developments, potential uses, and security issues, drawing attention to privacy concerns, security holes, AI-based remedies, and potential avenues for future study towards more resilient and protected IoT settings.

Bollineni et al. (2025) present a comprehensive review of smart and advanced healthcare solutions driven by these technologies, exploring their architecture, applications, benefits, and limitations. It categorizes healthcare use cases into critical domains, including wearable health devices, intelligent diagnostics, telemedicine, and emergency response systems. Furthermore, the article takes a close look at important obstacles like compatibility, power savings, data integrity, safety, and moral considerations. To address these issues, it discusses current solutions and highlights future research directions essential for scalable and sustainable healthcare innovation [29].

Yalli et al. (2025) The IoT is essentially an ideal that states all things should be linked together via the Internet. The IoT provides new possibilities for innovative services, making it the cornerstone for future growth. Since a computer's processing capacity almost doubles every two years, the IoT sector is booming. The size and power requirements, on the other hand, are cut in half throughout that time. This opens the door to a plethora of new possibilities for data interchange and interaction made possible by more compact and powerful devices [30].

Adam et al. (2024) IoT security, privacy, as well as trust studies based on a three-tiered IoT design. It explores the security requirements of IoT architectures and the challenges they encounter after establishing the foundation for IoT privacy, safety, as well as trust. Afterwards, the study delves into the current tendencies in studies that aim to resolve trust, Privacy and safety issues with IoT devices. In addition, the most recent developments and approaches to safeguarding sensitive data and IoT systems against security breaches are covered in this article. The survey ends with a summary of the status of IoT safety at the moment and the issues that still need to be resolved [31].

Gautam et al. (2023) This connection has significant privacy and security hazards. This research investigates these issues in order to identify the most prevalent vulnerabilities and their consequences for IoT systems. The research approach includes risk assessment, data encryption techniques, and security measures. This study of vulnerability frequency highlights many important issues, including unencrypted communication, insecure firmware, weak authentication, and a lack of security updates. These findings provide a foundation for advancing real-world enhancements to the IoT security environment by motivating manufacturers to prioritize security measures, promoting the adoption of standards and legislation, and enhancing user awareness and education [32].

Promsuk (2021) An AI neural network (ANN) model called the multi-layer perceptron (MLP) is used to lessen interference from nearby channels. The 2.4 GHz IoT network is examined using these suggested interference mitigation methods (IMTs). In this comparison, they look at the results obtained using the traditional minimum mean square error (MMSE) approach versus the MLP-based interference reduction. With amplitude and fast Fourier transform data as input, the MLP model can do its thing. The Internet of Things (IoT) network design also incorporates the consequences of route loss as well as small-scale fading to provide a more realistic system. It turns out that both IMTs can beat the MMSE filter when they use the MLP model [33].

Zhang et al. (2021) Technologies related to the IoT have advanced swiftly and find many uses in areas such as smart homes, Internet of vehicle, and the industrial IoT. Emerging smart gadgets often have simplistic designs, leaving the perception, transport, and application layers open to potential security flaws. Additional high-performance devices are now required by the majority of IoT security analysis frameworks. Additionally, there has been a lack of focus on new forms of malware, such as "mining" and additional methods of attack that directly take use of the computer power of the device. In light of these issues, this article develops and deploys an analytical system for smart home security [34].

Table II summarizes the research on Next-Generation IoT Security and Privacy Challenges, including the methodology, main results, difficulties, as well as potential future research paths

TABLE II. Literature Review on Security and Privacy Challenges in Next-Generation IoT Systems

Author	Study on	Approach	Key Findings	Challenges	Future Directions
Bollineni et al. (2025)	Smart and advanced healthcare solutions using emerging technologies	Comprehensive review of architectures, applications, benefits, and limitations across healthcare domains	Categorized healthcare applications into wearable devices, diagnostics, telemedicine, and emergency systems	Interoperability, energy efficiency, data quality, security, and ethical concerns	Proposes scalable, secure, and sustainable frameworks; emphasizes interdisciplinary research and standards
Yalli et al. (2025)	Growth and development of IoT devices	Analysis of IoT device evolution, computational power, and interconnectivity	Smaller, more powerful devices enable wide-ranging applications	Privacy and safety risks due to increased interconnectedness	Developing secure protocols and frameworks for future IoT development

Adam et al. (2024)	Issues of trust, privacy, as well as safety in the IoTs	Survey based on 3-layer IoT architecture; review of security requirements, trends, and challenges	Identified core security and privacy requirements; outlined latest security methods	Complex multi-laysser security requirements; evolving threat landscape	Address unresolved security challenges; enhance privacy-preserving techniques
Gautam et al. (2023)	IoT vulnerabilities and risk assessment	Risk assessment focusing on vulnerabilities, encryption algorithms, and security practices	Weak authentication, unsecured firmware, unencrypted communication highlighted as major risks	Lack of security updates and user awareness	Promote manufacturer security standards; increase user education
Promsuk (2021)	Interference mitigation in IoT networks	AI-based interference mitigation using Multi-Layer Perceptron (MLP) compared with MMSE approach	MLP-based model outperforms traditional MMSE in reducing interference in 2.4 GHz networks	Realistic network modeling with path loss and fading	Further AI integration for network robustness
Zhang et al. (2021)	IoT smart home security analysis	Building a smart home protection system that takes into account the perception, transportation, and application levels	Identified vulnerabilities in multiple IoT layers; noted emerging threats like mining malware	Need for high-performance security frameworks; overlooked emerging malware	Develop lightweight, efficient security frameworks; focus on malware detection

VI. Conclusion And Future Work

The security landscape, next-generation IoT technologies, and their design, features, and development were all thoroughly examined in this assessment. AI, blockchain, 5G, as well as edge computing, are just a few of the new technologies that have greatly improved the conventional IoT, making it more efficient, smarter, and able to analyze data in real-time and make decisions on its own. Despite these advancements, IoT still faces critical privacy and safety challenges due to its resource-constrained devices and diverse application areas. Advanced cryptographic methods, AI-driven threat detection, and robust privacy-preserving mechanisms are vital for building trustworthy IoT ecosystems. However, this study is limited by the lack of real-world implementation analysis and performance benchmarking across diverse IoT domains. Furthermore, the evolving nature of IoT threats demands continuous updating of security frameworks, on which this study does not provide any coverage.

Future studies must to concentrate on the practical deployment of secure and scalable next-generation IoT architectures, especially in high-risk sectors like healthcare, autonomous transport, and smart cities. Emphasis should be placed on developing lightweight yet robust encryption techniques and cross-layer security models tailored for heterogeneous IoT networks. Additionally, efforts should aim to standardize protocols for interoperability and integrate ethical frameworks that address data ownership and user consent. Adding federated learning for privacy-preserving analytics and integrating quantum-safe cryptography systems are two more viable approaches to improving the robustness and reliability of IoT ecosystems.

References

[1] 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, Nov. 2023, doi: 10.13052/jcsm2245-1439.1261.

[2] S. Garg, “Next-Gen Smart City Operations with AIOps & IoT : A Comprehensive look at Optimizing Urban Infrastructure,” *J. Adv. Dev. Res.*, vol. 12, no. 1, 2021.

[3] 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, Mar. 2025, doi: 10.38124/ijisrt/25mar1062.

[4] E. Kesavan, “Internet of Things (IoT): A Review of Security Challenges and Solutions,” *Int. J. Innov. Sci. Eng. Manag.*, vol. 2, no. 4, pp. 65–71, Dec. 2023, doi: 10.69968/ijisem.2023v2i465-71.

[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, 2024.

[6] M. A. Al Kabir, W. Elmedany, and S. Sharif, “Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques,” *J. Cyber Secur. Technol.*, vol. 7, no. 4, pp. 199–223, Oct. 2023, doi: 10.1080/23742917.2023.2228053.

[7] P. Chatterjee, “Real-Time Payment Systems and their Scalability Challenges,” *Iconic Res. Eng. Journals*, vol. 6, no. 12, pp. 1461–1470, 2023.

[8] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, “Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios,” *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[9] H. S. Chandu, “Enhancing Manufacturing Efficiency: Predictive Maintenance Models Utilizing IoT Sensor Data,” *IJSART*, vol. 10, no. 9, 2024.

[10] 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.

[11] N. Malali, “Next-Generation Augmented Data Science Platform for Autonomous Model Generation, Continuous Testing, Adaptive Deployment, and Real-Time Performance Optimization Using AI-Driven …,” 202521035177, 2025

[12] 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,” pp. 152–158, 2021.

[13] M. K. Saini and R. K. Saini, “Internet of Things (IoT) Applications and Security Challenges: A Review,” *Int. J. Eng. Res. Technol.*, vol. 7, no. 12, 2019, doi: 10.17577/IJERTCONV7IS12028.

[14] 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, Nov. 2021, doi: 10.1109/JSEN.2021.3055618.

[15] 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, Dec. 2024, doi: 10.32628/CSEIT2410612406.

[16] Y. Bin Zikria, R. Ali, M. K. Afzal, and S. W. Kim, “Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions,” *Sensors*, vol. 21, no. 4, p. 1174, Feb. 2021, doi: 10.3390/s21041174.

[17] M. Godavari and B. S. Prakash, “Next-Generation AI-Powered Automation for Streamlining Business Processes and Improving Operational Efficiency,” *J. Comput. Technol.*, vol. 12, no. 12, 2023.

[18] I. A. Thoker, “Safety in Next-Generation IoT Systems,” *IOSR J. Comput. Eng.*, vol. 25, no. 1, pp. 69–74, 2023, doi: 10.9790/0661-2501016974.

[19] M. Castaño Gómez, A. M. López Echeverry, and P. A. Villa Sánchez, “Revisión del uso de tecnologías y dispositivos IoT en los sistemas de seguridad física,” *Ing. Y Compet.*, vol. 24, no. 1, pp. 1–19, Oct. 2021, doi: 10.25100/iyc.v24i1.11034.

[20] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, IEEE, Mar. 2017, pp. 93–97. doi: 10.1109/Anti-Cybercrime.2017.7905270.

[21] 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)*, IEEE, Jun. 2024, pp. 1–5. doi: 10.1109/ICCCNT61001.2024.10725287.

[22] C. Gilbert and M. Gilbert, "AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities," *SSRN Electron. J.*, vol. 5, 2024, doi: 10.2139/ssrn.5259702.

[23] S. Kumar, 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.

[24] Z. Ali, H. Ali, and M. Badawy, "Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions," *Int. J. Comput. Appl.*, vol. 128, no. 1, pp. 975–8887, 2015.

[25] H. Gantla, "Threats and Mitigation Techniques in Network Security," *Int. J. Adv. Eng. Nano Technol.*, vol. 2, no. 2, pp. 266–273, 2014.

[26] 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, Mar. 2024, doi: 10.4108/eetiot.5565.

[27] 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, 2023, doi: 10.3390/electronics12112401.

[28] S. Szymoniak, J. Piątkowski, and M. Kurkowski, "Defense and Security Mechanisms in the Internet of Things: A Review," *Appl. Sci.*, vol. 15, p. 499, 2025, doi: 10.3390/app15020499.

[29] 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.*, pp. 1–1, 2025, doi: 10.1109/JIOT.2025.3570188.

[30] J. S. Yalli *et al.*, "A Systematic Review for Evaluating IoT Security: A Focus on Authentication, Protocols and Enabling Technologies," *IEEE Internet Things J.*, vol. PP, p. 1, 2025, doi: 10.1109/JIOT.2025.3545737.

[31] 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. April, pp. 57128–57149, 2024, doi: 10.1109/ACCESS.2024.3382709.

[32] 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)*, 2023, pp. 1489–1494. doi: 10.1109/ICIRCA57980.2023.10220814.

[33] 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)*, 2021, pp. 374–377. doi: 10.1109/ECTI-CON51831.2021.9454889.

[34] 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)*, 2021, pp. 596–599. doi: 10.1109/ICBAIE52039.2021.9389849.

