IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Impact Factor: 5.731

Volume 5, Issue 12, December 2025

A Comprehensive Review of Security and Privacy Challenges in the Internet of Things (IoT) Ecosystem

Kavitha A
Department of ECE
East Point College of Engineering and Technology, Bangalore
kavitha.ece@eastpoint.ac.in

Abstract: *The Internet of Things (IoT) has rapidly expanded, connecting a multitude of devices and transforming various sectors. However, this growth has introduced significant security and privacy challenges. This paper provides a comprehensive review of the current research landscape, focusing on authentication, security protocols, the Internet of Medical Things (IoMT), and blockchain-based security solutions. We analyze recent studies, highlighting the vulnerabilities, potential threats, and proposed solutions, while emphasizing the need for robust security frameworks to ensure the safe and reliable deployment of IoT technologies*

Keywords: *Internet of Things*

I. INTRODUCTION

The proliferation of IoT devices has revolutionized industries ranging from healthcare to industrial automation. However, the inherent vulnerabilities of these devices and the complex nature of IoT ecosystems have created substantial security and privacy concerns. This paper aims to synthesize recent research findings to provide a holistic overview of the security challenges and potential solutions in the IoT domain.

Authentication and Security Assessment in IoT

Saqib et al carried out a thorough evaluation of IoT authentication methods and security. Their research emphasizes how important it is to have strong authentication procedures in place to prevent data breaches and unwanted access. The difficulties posed by resource-constrained IoT devices and the need for thin authentication solutions are highlighted in the paper.

Key Findings from Saqib et al.

• Analysis of various authentication schemes, including password-based, biometric, and certificate-based methods.
• Identification of common vulnerabilities such as replay attacks, man-in-the-middle attacks, and denial-of-service attacks.
• Emphasis on the importance of key management and secure storage for authentication credentials.

Security Protocols in IoT

Mishra and Mishra \cite{mishra2025current} give an overview of recent studies on IoT security measures. Their research investigates several protocols intended to provide safe communication and data sharing in Internet of Things settings. In discussing the advantages and disadvantages of various protocols, the survey emphasizes the necessity of context-aware and adaptive security solutions.

Key Findings from Mishra and Mishra

• Review of protocols such as DTLS, IPSec, and MQTT-SN.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025
Impact Factor: 5.731

• Discussion of lightweight security protocols suitable for resource-constrained devices.
• Analysis of the challenges in implementing end-to-end security in diverse IoT networks.

Security Challenges in the Internet of Medical Things (IoMT)

Ahmed et al. \cite{ahmed2024insights} concentrate on the unique security issues facing the IoMT space. They stress how important data security and privacy are in medical applications that handle sensitive patient data. The study also looks at data fusion methods and possible ways to improve privacy and security.

Key Findings from Ahmed et al.

• Identification of unique security risks in IoMT, including data breaches and unauthorized access to medical devices.
• Discussion of data fusion techniques for aggregating and analyzing medical data.
• investigation of potential remedies to preserve patient privacy, such as federated learning and homomorphic encryption

Blockchain-Based Security Solutions for Industrial IoT (IIoT)

Sharma et al. \cite{sharma2023secure} investigate the use of blockchain technology to enhance security and privacy in the Industrial IoT (IIoT). They propose a secure authentication and privacy-preserving blockchain framework to address the challenges of data integrity and access control in industrial environments.

Key Findings from Sharma et al.

• Application of blockchain for secure authentication and data integrity in IIoT.
• Development of privacy-preserving mechanisms to protect sensitive industrial data.
• Analysis of the performance and scalability of blockchain-based security solutions.

Table 1: Comparative Analysis of Reviewed Research Contributions

Study	Focus Area	Key Contributions	Techniques/ Technologies Used	Challenges Addressed
Saqib et al. (2023)	IoT Authentication & Security	Evaluated authentication mechanisms; highlighted vulnerabilities like replay, DoS, and MitM attacks.	Password, biometric, certificate- based auth; key management	Light weight auth for resour ce-constr ained device s
Mishra & Mishra (2025)	IoT Security Protocols	Surveyed secure communication protocols; stressed need for context-aware security	DTLS, IPSec, MQTT-SN; lightweight security protocols	End- to-end security in diverse networks
Ah me d et al. (2024)	IoMT Security	Analyz ed privacy issues in medical IoT; discuss ed data fusion and privacy preserving solution s.	Federated learning, homomorphic encryption	Patient data privacy, unauthorized access
Sharma et al. (20 23)	Blockchain in Industri al IoT (IIoT)	Propose d blockchain-based secure authentic cation and privacy frameworks; evaluated performance and scalability.	Blockchain technology	Data integrity, access control, scalability in IIoT

Discussion

Together, the reviewed papers show how complex the security and privacy issues in the IoT ecosystem are. Customized solutions are needed for authentication, security protocols, and particular domains like IoMT and IIoT. There are encouraging opportunities to improve security and privacy through the use of blockchain technology.

Challenges and Future Directions

- Scalability: Developing security solutions that can scale with the growing number of IoT devices.
- Interoperability: Ensuring seamless integration of security protocols across diverse IoT platforms.
- Lightweight Security: Designing efficient and lightweight security mechanisms for resource- constrained devices.
- Privacy Preservation: Implementing robust privacy- preserving techniques to protect sensitive data.
- AI and Machine Learning: Using AI and Machine Learning to improve threat detection and security automation.
- Standardization: Developing uniform security standards and protocols for IoT.

II. CONCLUSION

There are serious security and privacy issues facing the IoT ecosystem that call for all-encompassing and flexible solutions. Numerous strategies have been investigated recently, including cutting-edge technologies like blockchain, strong security protocols, and sophisticated authentication methods. For IoT technologies to be widely adopted and deployed safely, these issues must be resolved. To guarantee the dependability and credibility of IoT systems, future research should concentrate on three key areas: creating scalable, interoperable, and privacy-preserving security solutions.

REFERENCES

[1] Manasha Saqib, Ayaz Hassan Moon, A Systematic Security Assessment of Internet of Things in the Context of Authentication,Computers & Security,Volume 125,2023,103053,ISSN 0167-4048,
https://doi.org/10.1016/j.cose.2022.103053}{ht tps://doi.org/10.1016/j.cose.2022.103053
[2] Raghavendra Mishra, Ankita Mishra,Current research on Internet of Things (IoT) security protocols: Computers & Security, Volume 151,2025,104310,ISSN 0167-4048
https://doi.org/10.1016/j.cose.2024.10431 0}{https://doi.org/10.1016/j.cose.2024.104310
[3] Shams Forruque Ahmed, Md. Sakib Bin Alam, Shaila Afrin, Sabiha Jannat Rafa, Nazifa Rafa, Amir H. Gandomi, Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions,Information Fusion,Volume 102,2024,102060,ISSN 1566-2535,
https://doi.org/10.1016/j.inffus.2023.102060}{ https://doi.org/10.1016/j.inffus.2023.102060
[4] Prakash Chandra Sharma, Md Rashid Mahmood, Hiral Raja, Narendra Singh Yadav, Brij B. Gupta, Varsha Arya, Secure authentication and privacy- preserving blockchain for industrial internet of things,Computers and Electrical Engineering, Volume 108,2023,108703,ISSN 0045-7906,
https://doi.org/10.1016/j.compeleceng.20 23.108703
https://doi.org/10.1016/j.compeleceng.2 023.108703