Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

REVIEW IOT CYBERSECURITY: EMERGING RISKS AND MITIGATION APPROACHES – A COMPREHENSIVE SURVEY

Dilmurod Mirzaaxmedov
Tashkent State University of Economics,
Department of Digital economy, Uzbekistan
echo19_87@mail.ru

Abstract:
The Internet of Things (IoT) is increasingly integrated into everyday life, bringing with it serious cybersecurity concerns and a growing demand for robust protection mechanisms. This study presents a comprehensive systematic review of recent literature, examining the key challenges and types of cyberattacks that compromise IoT security. It evaluates existing frameworks and solutions while identifying emerging trends and notable research gaps. A distinguishing aspect of this work is its focused analysis of machine learning techniques employed to detect and mitigate IoT-related threats. Furthermore, the study highlights underexplored areas such as the economic implications of IoT vulnerabilities and specific security challenges within industrial IoT environments. The review synthesizes insights from relevant academic sources and outlines potential directions for future research. Findings suggest that privacy breaches and cybercrime remain the most critical concerns in IoT security. Although artificial intelligence shows significant promise in enhancing future defenses, certain threats—such as confidentiality violations, authentication failures, and insecure data server connections—are still insufficiently addressed by current approaches. This underscores the need for continued research and real-world validation of proposed solutions. As IoT technologies evolve rapidly, the importance of proactive cybersecurity strategies becomes increasingly evident. Greater international collaboration among cybersecurity stakeholders is essential to establish new standards and practices capable of addressing the unique vulnerabilities inherent in IoT systems. Such collective efforts are crucial for

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

strengthening the resilience of these systems against sophisticated and evolving cyber threats.

Keywords: Internet of Things (IoT); cybersecurity; cybersecurity frameworks; cybersecurity approaches.

1.Introduction

The Internet of Things (IoT) has expanded into numerous critical domains, including healthcare and the economic sector. Beyond these, its presence is rapidly growing in residential settings, smart cities, and various other aspects of daily life that are equally significant. IoT connects smart objects, applications, and cloud platforms—resulting in a massive network of devices, with an estimated 50 billion connected to the internet by 2020 [1]. This vast and growing source of data, combined with the increasing reliance on artificial intelligence, places significant pressure on IoT providers and developers to enhance security in order to meet future demands.

Trust in IoT devices fundamentally depends on their ability to ensure security—especially given their internet connectivity, which exposes them to a broad spectrum of threats and cyberattacks [2]. These threats range from cybercrime, software piracy, and malware [1], to other sophisticated and destructive attack vectors. However, due to the dynamic nature of the IoT ecosystem, existing security measures are no longer sufficient. Emerging risks necessitate the development of updated frameworks, solutions, and a continuous evolution of IoT-related disciplines [3]. It is therefore essential to regularly revise and enhance current security strategies and methodologies.

In this context, the present study provides an up-to-date assessment of recent advancements in IoT cybersecurity risk analysis, based on contemporary research publications. The study identifies various frameworks and methodologies developed to assess cybersecurity risks in IoT environments, shedding light on the primary challenges and threat vectors faced by connected devices. Furthermore, we examine specific algorithms and techniques, offering insights into their practical applications and effectiveness.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

A critical finding of this review is the presence of notable research gaps, particularly in understanding the economic consequences of IoT-related cybersecurity incidents. It also underscores the need for customized security solutions, particularly within the industrial IoT sector. To build a resilient and secure IoT ecosystem, collaboration among technology developers, regulatory authorities, and cybersecurity professionals is crucial. Strengthening partnerships among these stakeholders can pave the way for innovative and effective security strategies, ultimately contributing to a safer, more robust IoT infrastructure capable of withstanding emerging and advanced cyber threats.

2. Methodology

Eligibility sriteria:

This systematic review included studies selected based on clearly defined inclusion criteria. Specifically, the review considered research articles focused on Internet of Things (IoT) cybersecurity issues, those that analyzed current challenges in the field, and publications that proposed innovative frameworks or approaches for addressing cybersecurity threats. In addition, prior review papers that conducted assessments of IoT cybersecurity risks were also included to provide a comprehensive foundation for this study.

Information sources:

The data for this review was sourced from well-established academic databases such as ScienceDirect and IEEE Xplore, as well as high-impact international journals. The use of these authoritative platforms ensured that the selected literature met rigorous academic standards and contributed diverse, high-quality perspectives. This methodologically sound selection process enhances the credibility and comprehensiveness of the review, establishing a strong foundation for analysis and interpretation.

Search strategy and selection process:

A strategic keyword-based search was employed using reliable academic engines such as Google Scholar, Academia.edu, ScienceDirect, and IEEE. Key search terms included: IoT, cybersecurity, cybersecurity frameworks, and cybersecurity

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

approaches. The inclusion criteria emphasized publications from 2015 to 2023, with a particular focus on studies published between 2018 and 2023. Selected articles were further assessed for analytical depth and their relevance to the current discourse in IoT cybersecurity. Only those works offering substantial insights and methodological rigor were included in the final review.

Data analysis and synthesis:

The selected literature was categorized according to publication type, such as empirical research, case studies, surveys, and review articles. Each study's objectives, research questions, significant findings, and recommendations were systematically identified and extracted. A tabular format was employed to streamline the presentation of key information, including cybersecurity threats, challenges, attack impacts, proposed solutions and frameworks, and effective detection methodologies.

The analysis yielded a rich synthesis of critical insights, offering a holistic understanding of prevailing challenges in IoT cybersecurity. Various categories of cyber threats were meticulously examined. Importantly, the review also identified key research gaps—especially concerning the economic impact of cyber incidents and the lack of tailored security solutions in the industrial IoT domain. Emerging trends were distilled and articulated to provide a forward-looking perspective.

This rigorous methodological approach ensures that the review delivers a well-rounded critique and a valuable academic contribution. The structured data synthesis positions the paper as a strategic resource for researchers, practitioners, and policymakers engaged in securing IoT infrastructures against evolving cyber threats.

Literature review

This section provides a critical overview of existing scholarly contributions related to IoT cybersecurity, with a strong emphasis on literature published over the last decade. It traces the evolution of cybersecurity concerns in tandem with the exponential growth of IoT networks. The review reveals how earlier works

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

laid the groundwork for current security frameworks, and how recent studies have responded to increasingly complex attack vectors and vulnerabilities.

Throughout the review, the effectiveness and limitations of various mitigation strategies are examined, alongside the theoretical and practical underpinnings of proposed solutions. Particular attention is paid to recent advancements in artificial intelligence, machine learning, and blockchain technologies as they relate to cybersecurity in the IoT ecosystem.

Moreover, the literature emphasizes the continuous need for innovative, scalable, and context-specific security mechanisms to safeguard interconnected devices. The findings underscore the importance of adaptive cybersecurity models capable of responding to dynamic threat landscapes and evolving user demands.

By synthesizing these insights, this literature review establishes a solid theoretical foundation for the study, enabling a deeper understanding of both the historical trajectory and the current state of IoT cybersecurity research.

IoT risk

The evaluation in Study [1] focused on addressing two major threats causing significant economic damage to IoT systems: software piracy and malware attacks. This empirical study employed an experimental methodology to assess a novel approach aimed at detecting pirated software and malware -infected files within the IoT network. The results of the experiments demonstrated the high effectiveness of this proposed approach compared to previous methods in improving IoT cybersecurity. Study [2], on the other hand, examined the increasingly pervasive role of IoT in our daily lives and the associated risks with its widespread adoption. This empirical investigation used the EBIOS methodology to conduct a comprehensive risk analysis to identify vulnerabilities within the IoT architecture. The primary objective was to determine the most critical security risks that developers should prioritize for mitigation. The findings highlighted that sensors, smart switches, and small actuators, in particular contexts, are the most vulnerable components in the IoT ecosystem. Study [3] focused on elucidating concepts related to IoT risk assessment. The primary goal was to uncover the underlying reasons for the inadequacy of existing risk

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

assessment approaches tailored to IoT. The study's results revealed that the main reasons for the limitations of current IoT risk assessment methodologies include:

- Deficiencies in regular evaluations.
- Evolving system boundaries with constrained system understanding.
- The complexity of comprehending interconnections.
- Neglecting the potential of assets as attack vectors.

Furthermore, there is a need for automated and continuous risk assessment methods, as well as the creation of innovative backup tools for simulation and forecasting. These advancements would address the existing gaps and significantly strengthen the IoT security landscape. Implementing automated risk assessment and predictive modeling tools will provide a proactive approach to identifying and mitigating potential threats, thereby enhancing the overall resilience and reliability of IoT systems in an increasingly interconnected world.

2.1. Attacks and challenges

Attacks and Challenges. In Study [4], a survey-based research paper delved into the challenges and current state of IoT. The primary objective was to introduce security standards, prevalent issues, and forthcoming trends in IoT security. The methodology predominantly relied on a literature review. The findings indicated that recent IoT studies had been addressing authentication, access control, and protocols. Study [7] centered on cybersecurity threats to healthcare services, specifically in hospitals and clinics employing IoT technology. It introduced an adaptive cybersecurity framework designed to dynamically adapt to cyber threats. The research emphasized adaptive security measures that anticipate and respond to dynamic attacks targeting healthcare services and infrastructure [14]. The results demonstrated the framework's efficacy in providing robust defense against dynamic and adaptive attacks.

Study [8] underscored the significance of cyber risk within IoT systems and aimed to identify risks while defining relevant risk assessment techniques. It conducted an analysis of existing cyber risk assessment approaches through a review of relevant literature. This foundational study provided essential definitions in the context of IoT cybersecurity, offering an overview of studies on

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

IoT cyber risk quantification, as well as strategies for mitigating and transferring cyber risks.

Study [9] tackled privacy concerns in IoT and explored the role of computational intelligence (CI) in cybersecurity. The study sought to assess the relevance of CI technologies in addressing IoT cybersecurity issues. This survey-based research paper drew upon secondary data from a review of related literature, primarily highlighting the challenges faced by CI technologies in IoT cybersecurity.

Study [10] addressed the pressing need for novel solutions to combat global cybercrimes affecting IoT systems. The authors provided insights and solutions related to cybercrimes, offering a comprehensive overview of diverse cybersecurity challenges in IoT. These challenges were categorized based on IoT security features, and the study proposed blockchain as an ideal solution, offering integrity, authentication, and encryption.

Study [11] explored various concerns related to IoT devices, particularly data theft and data breach incidents. This review article aimed to identify IoT security challenges, requirements, and proposed solutions. The key findings emphasized that IoT security is influenced by factors such as the cost of cybersecurity solutions, data volume, and data sensitivity.

Study [12] delved into IoT's background and security, along with potential cybersecurity threats and available solutions. Additionally, the study introduced a novel three-layered solution model: lower (IoT), middle (edge), and upper (cloud). This empirical study assessed the proposed solution's effectiveness, revealing that the introduced model could mitigate certain potential vulnerabilities.

Study [13] aimed to create a taxonomy of threats impacting IoT devices and systems, accompanied by an analysis of attacks and intruders. The findings highlighted the paramount importance of issues like confidentiality, privacy, and organizational trust in IoT cybersecurity. Moreover, the paper paved the way for future research by shedding light on the consequences of these threats.

It is also worth noting that IoT cybersecurity is a rapidly evolving field, requiring continuous collaboration between researchers, developers, and regulators to devise and implement effective security measures. This collaboration is particularly crucial to stay ahead of constantly changing threats and to ensure the

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

protection of sensitive data and infrastructure. Furthermore, integrating multidisciplinary approaches and fostering international cooperation can enhance the development of robust security protocols. By sharing knowledge and best practices, stakeholders can address emerging vulnerabilities more effectively, ensuring that IoT ecosystems remain resilient against sophisticated cyber threats. This concerted effort is essential for safeguarding the integrity and reliability of IoT networks in the long term.

3. Conclusions

This systematic review has offered a detailed exploration of the evolving landscape of cybersecurity within the Internet of Things (IoT) ecosystem. The analysis of existing literature confirms that IoT devices are increasingly susceptible to a broad spectrum of cyber threats, with particular concern surrounding issues of privacy and cybercrime. These findings underscore the critical and ongoing need for robust, scalable, and adaptive security mechanisms tailored to the dynamic nature of IoT environments. One of the prominent themes emerging from this review is the potential role of artificial intelligence (AI) and machine learning (ML) in enhancing IoT cybersecurity. As conventional security approaches become insufficient in addressing complex and sophisticated cyberattacks, the adoption of AI-based solutions presents a promising pathway toward proactive threat detection and response. These intelligent systems can analyze vast amounts of data in real time, detect anomalies, and adapt to emerging threats, thereby offering significant improvements over static, rule-based systems.

Despite the advancements identified, the review also revealed notable research gaps, particularly regarding the limited coverage of specific types of attacks and vulnerabilities. This highlights the need for further investigation into more targeted and context-aware countermeasures, especially in high-risk domains such as industrial IoT. Moreover, the economic impacts of cybersecurity breaches within IoT networks remain underexplored, warranting more focused research in this area.

Overall, the study emphasizes that securing IoT ecosystems demands not only technological innovation but also interdisciplinary collaboration among

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

stakeholders, including developers, cybersecurity experts, policymakers, and regulatory bodies. Global cooperation and the exchange of best practices are essential to develop comprehensive strategies capable of addressing the multifaceted challenges associated with IoT security. This review serves as a foundational reference for future research and a strategic guide for shaping more resilient and secure IoT infrastructures.

References

1. Ullah, F.; Naeem, H.; Jabbar, S.; Khalid, S.; Latif, M.A.; Al-Turjman, F.; Mostarda, L. Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. IEEE Access 2019, 7, 124379–124389.
2. Zahra, B.F.; Abdelhamid, B. Risk Analysis in Internet of Things Using EBIOS. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Vegas, NV, USA, 9–11 January 2017; pp. 1–7.
3. Nurse, J.R.C.; Creese, S.; De Roure, D. Security Risk Assessment in Internet of Things Systems. IT Prof. 2017, 19, 20–26.
4. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In Proceedings of the 2015 10th
5. International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
6. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. Int. J. Surg. 2010, 8, 336–341
7. Radanliev, P.; De Roure, D.; Maple, C.; Nurse, J.R.; Nicolescu, R.; Ani, U. Cyber Risk in IoT Systems. Univ. Oxford Comb. Work. Pap. Proj. Rep. Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent. 2019, 169701, 1–27.
8. Zhao, S.; Li, S.; Qi, L.; Da Xu, L. Computational Intelligence Enabled Cybersecurity for the Internet of Things. IEEE Trans. Emerg. Top. Comput. Intell. 2020, 4, 666–674. [CrossRef]
9. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A Review of Internet of Things (IoT) Security Issues,

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 03, June, 2025
Website: usajournals.org

Challenges and Techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6.

10. Rizvi, S.; Kurtz, A.; Pfeffer, J.; Rizvi, M. Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy, New York, NY, USA, 31 July–3 August 2018; pp. 163–168.
11. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. Appl. Sci. 2020,10, 4102.
12. Abomhara, M.; Køien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88.
13. Strecker, S.; Van Haaften, W.; Dave, R. An Analysis of IoT Cyber Security Driven by Machine Learning. In Proceedings of the International Conference on Communication and Computational Technologies: ICCCT 2021; Springer: Singapore, 2021; pp. 725–753.
14. Mirzaaxmedov D. Analysis and classification of Permanent Denial-of-Service (PDoS) Attacks: Scientific Journal of Digital Transformation and Artificial Intelligence VOLUME 3, ISSUE 1, FEBRUARY 2025, pp162-170 IEEE Access 2020, 8, 228922–228941.
15. Abidov, A., Mirzaaxmedov, D., Rasulev, D. (2023). Analytical Model for Assessing the Reliability of the Functioning of the Adaptive Switching Node. In: Koucheryavy, Y., Aziz, A. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2022. Lecture Notes in Computer Science, vol 13772. Springer, Cham., p. 46-56. https://doi.org/10.1007/978-3-031-30258-9_5.