RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI
2023
№4 (12),
oktabr-dekabr
http://dgeconomy.tsue.uz/
ILMIY ELEKTRON JURNAL

SYSTEMATIC ANALYSIS OF CYBERSECURITY THREATS IN IOT ENVIRONMENTS

Mirzaakhmedov Dilmurod
Senior teacher of Tashkent State University of Economics
mirzaakhmedovdilmurod@gmail.com

Abstract
The Internet of Things (IoT) is increasingly becoming a part of our daily routines. This integration raises significant concerns about potential cybersecurity threats and the need for reliable solutions. This study presents a comprehensive systematic review of the current literature, exploring the various challenges and attacks that threaten IoT cybersecurity. It also discusses proposed frameworks and solutions. Additionally, the study delves into emerging trends and identifies gaps in current knowledge. A distinctive feature of this research is its in-depth exploration of machine learning methods to identify and mitigate IoT risks. The study further contributes by highlighting research gaps in evaluating the economic impacts and security concerns specific to industrial IoT.

Annotatsiya
Buyumlar Interneti (IoT) bizning kundalik hayotimizga tobora chuqurroq kirib bormoqda. Bu integratsiya, kiberxavfsizlik tahdidlari va ishonchli yechimlarni topish zaruratini kuchli ravishda oshirmoqda. Bu tadqiqot, hozirgi adabiyotlarni keng qamrovli va sistemali tarzda ko'rib chiqish orqali, Buyumlar Interneti kiberxavfsizligiga qarshi turli xil muammolar va hujumlarni o'rganadi. U shuningdek, taklif etilgan yondashuvlar va yechimlarni muhokama qiladi. Tadqiqot yangi tendentsiyalarni o'rganish bilan birga, hozirgi bilimlardagi bo'shliqlarni aniqlaydi. Bu tadqiqotning noyob xususiyati Buyumlar Interneti xavflarini aniqlash va kamaytirishda mashinasozlik usullaridan chuqur foydalanishdir. Tadqiqot, shuningdek, sanoat Buyumlar Internetiga xos bo'lgan iqtisodiy ta'sirlar va xavfsizlik masalalarini baholashdagi tadqiqot bo'shliqlarini yoritib beradi.

Аннотация
Интернет вещей (IoT) все глубже входит в нашу повседневную жизнь. Эта интеграция значительно усиливает необходимость в надежных решениях по кибербезопасности и поднимает вопросы о потенциальных угрозах. Данное исследование представляет собой обширный и систематический обзор

существующей литературы, в котором рассматриваются различные вызовы и атаки, угрожающие кибербезопасности IoT. В нем также обсуждаются предлагаемые методологии и решения. Кроме того, исследование затрагивает новые тенденции и выявляет пробелы в текущих знаниях. Особенностью этой работы является подробное изучение методов машинного обучения для выявления и уменьшения рисков IoT. Исследование также вносит вклад, подчеркивая пробелы в исследованиях экономических последствий и проблем безопасности, специфичных для промышленного IoT.

Keywords
Internet of Things (IoT), cybersecurity, cybersecurity frameworks, cybersecurity approaches.

Kalit so'zlar
Buyumlar Interneti (IoT), kiberxavfsizlik, kiberxavfsizlik tizimlari, kiberxavfsizlik yondashuvlari.

Ключевые слова
Интернет вещей (IoT), кибербезопасность, рамки кибербезопасности, подходы к кибербезопасности.

Introduction

IoT has permeated numerous sensitive disciplines, including the health sector and the economic sector. However, the IoT is emerging at home, in large cities, and in other, different domains of life, which are not of less importance. In addition, the IoT provides connections to intelligent objects, applications, and cloud computing; 50 billion IoT devices were connected to the internet in 2020 [1]. This huge source of data, as well as the future trend of artificial intelligence, which the world has come to rely on, has put pressure on vendors and designers of IoT devices to secure this technology in order to enable it to meet upcoming demands. However, trusting a device starts with ensuring its security, which has become a necessity, especially when these devices are connected to the internet, exposing them to many threats and cyberattacks [2]. The security threats include cybercrimes, software piracy, and malware attacks [1], as well as various damaging attacks. However, this continuous field of improvement cannot adopt existing approaches to provide security. New risks keep on arising, which requires updates to new frameworks and solutions in parallel with updating IoT disciplines. [3] In addition, it is recommended to periodically update the methods and strategies used. To this end, the proposed study includes a current assessment of advances in cyber security risk analysis for the IoT presented in recent literature. This assessment also identifies the various frameworks and methodologies provided to analyze cybersecurity risks in IoT, identifying the various threats and barriers facing IoT devices. We will delve into individual algorithms and approaches, providing insight into their real-life applications and effectiveness. Furthermore, we identify significant gaps in research to assess the economic

consequences of IoT cybersecurity incidents and highlight the need for tailored security solutions in the industrial IoT sector.

Methodology

In this section, we describe the research methodology used in this study. It outlines a series of steps that begin with defining eligibility criteria for selecting research articles. It then goes on to outline the data sources, search strategy, and article selection process. In addition, this section explores the details of data analysis and synthesis. The review process followed the steps of systematic literature review as outlined in the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [6].

2.1 Eligibility Criteria

In this review, previous studies were selected based on specific eligibility criteria, which included research articles discussing IoT cybersecurity, studies addressing challenges related to IoT cybersecurity, and research proposing frameworks and novel approaches to address cybersecurity issues. Additionally, previous review papers focused on the risk assessment of IoT cybersecurity were considered.

2.2 Information Sources

The author relied on reputable databases like Science Direct and IEEE, as well as high-impact-factor international journals, to source papers and articles for this review.

2.3 Search Strategy and Selection Process

The authors employed certain keywords (IoT, cybersecurity, cybersecurity frameworks, cybersecurity approaches) within trusted research engines such as Google Scholar, Academia, Science Direct, and IEEE. Research articles meeting the inclusion criteria were then filtered by publication year, with a primary focus on papers published between 2015 and 2023, with particular emphasis on those from 2018 to 2023. The selected studies were also evaluated based on the depth of their analysis and their impact on the research field. Ultimately, this process led to the selection of articles that underwent systematic review, as shown in (see Fig. 1.)

2.4 Data analysis and synthesis

Each of the selected studies was classified according to type, such as empirical research, case study, survey or review paper. Additionally, the research objectives and issues addressed in each study were highlighted, and significant results and recommendations were extracted. To facilitate this process, the author used a table format to represent information related to threats, challenges, the impact of attacks, proposed frameworks and approaches, and noteworthy detection techniques. The findings encompassed a comprehensive summary of insights derived from the reviewed studies. Various types of attacks and challenges were thoroughly examined. Furthermore, the authors identified a research gap that had not been addressed in prior studies. Lastly, emerging trends in IoT cybersecurity were distilled from the literature and succinctly presented in the findings.

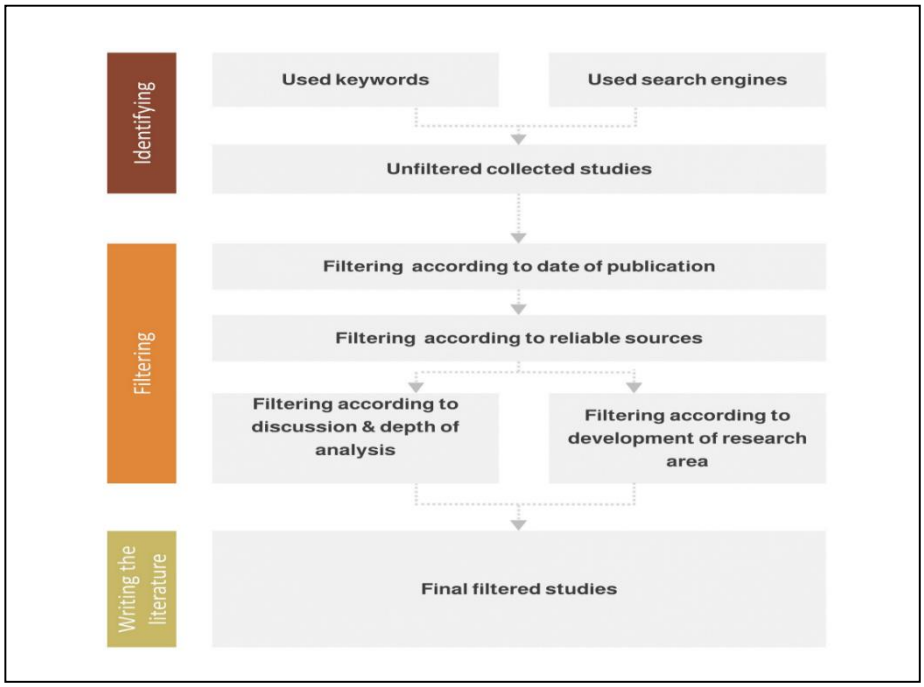

Fig. 1. Search strategy framework

IoT Risk

Evaluation in Study [1], the focus was on addressing two major threats causing substantial economic harm to IoT systems: software piracy and malware attacks. This empirical study employed an experimental methodology to assess a novel solution approach aimed at detecting pirated software and malware-infected files within the IoT network. The results of the experiments demonstrated the superior effectiveness of this proposed approach compared to previous methods in enhancing IoT cybersecurity. Study [2], on the other hand, delved into the increasingly pervasive role of IoT in our daily lives and the inherent risks associated with its widespread adoption. This empirical investigation utilized the EBIOS methodology to conduct a comprehensive risk analysis, with the goal of pinpointing vulnerabilities within the IoT architecture. Its primary objective was to identify the most critical security risks that developers should prioritize for mitigation. The findings highlighted those sensors, smart switches, and small actuators, in particular contexts, were the most vulnerable components in the IoT ecosystem. Study [3,4] concentrated on elucidating concepts related to IoT risk assessment. Its principal objective was to uncover the underlying causes for the inadequacy of current risk assessment approaches tailored to IoT. The study's results revealed that the primary reasons for the limitations of existing 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 was a need for automated and continuous risk assessment methods, along with the creation of innovative backup tools for simulating and forecasting capabilities.

Attacks and Challenges

Study [5], 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. 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 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.

Results and discussion

This section addresses the gap identified by the systematic review and outlines anticipated future trends in IoT cybersecurity.

Prevalent Attacks Targeting IoT

The outcomes reveal that the most frequently addressed issues and concerns regarding IoT cybersecurity primarily revolved around privacy-related matters [11,15]. Additionally, significant attention has been directed toward issues related to cybercrimes [12,17]. Another noteworthy concern discussed in the literature pertains to denial-of-access attacks [5,15]. Furthermore, data exploitation has emerged as a critical challenge in the realm of IoT security [6,11,13,16], closely followed by the detection of Man-in-the-Middle attacks as highlighted by [17].

Prominent Techniques Utilized for IoT Risk Detection

In terms of detection techniques, the present study has summarized a selection of methods identified in the literature. These techniques encompass artificial intelligence [1,4], cognitive security techniques [15], novel meta-heuristic approaches [18], cloud computing [17], and machine learning [14].

Conclusions

In conclusion, this systematic review has provided insights into the diverse and constantly changing landscape of IoT cybersecurity. The examination of the literature highlighted that IoT devices and systems are exposed to a wide array of cyber threats, with particular emphasis on privacy issues and cybercrimes. This reaffirms the urgent need for ongoing endeavors to address these pressing challenges.

Moreover, the review underscored the considerable potential of artificial intelligence as a promising approach to bolster IoT cybersecurity. With the IoT environment becoming increasingly complex and expansive, conventional security measures alone may prove insufficient in countering sophisticated attacks. The incorporation of artificial intelligence and machine learning holds promise for delivering adaptive, proactive, and more effective security solutions capable of mitigating evolving threats.

Nonetheless, while the review offered valuable insights from existing research, there remain critical areas warranting further investigation. Some attacks and vulnerabilities received limited coverage from the proposed solutions, underscoring the requirement for more tailored and precise countermeasures.

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. Kuzlu, M.; Fair, C.; Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discov. Internet Things 2021, 1, 7.
5. 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 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, 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. Furfaro, A.; Argento, L.; Parise, A.; Piccolo, A. Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. Simul. Model. Pract. Theory 2017, 73, 43–54.
13. Liao, B.; Ali, Y.; Nazir, S.; He, L.; Khan, H.U. Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. IEEE Access 2020, 8, 120331–120350.
14. Li, S.; Bi, F.; Chen, W.; Miao, X.; Liu, J.; Tang, C. An Improved Information Security Risk Assessments Method for Cyber-Physical- Social Computing and Networking. IEEE Access 2018, 6, 10311–10319.
15. Abidov, A., Mirzaaxmedov, D., Rasulev, D. Analytical Model for Assessing the Reliability of the Functioning of the Adaptive Switching Node. Lecture Notes in Computer Science, vol 13772. Springer, Cham., p. 46-56. https://doi.org/10.1007/978-3-031-30258-9_5.