https://journal.ypidathu.or.id/index.php/jssut/
P - ISSN: 3026-5959
E - ISSN: 3026-605X

A Comprehensive Review of Cybersecurity Measures in the IoT Era

Ezatullah Ahmady[1], Abdul Rahman Mojadadi[2], Musawer Hakimi[3]
[1,2]Kabul University, Afghanistan
[3]Samangan University, Afghanistan

ABSTRACT

Background. This research presents a comprehensive review of cybersecurity measures in the Internet of Things (IoT) era. The primary focus is on elucidating the evolving landscape of IoT cybersecurity, with specific attention to the integration of Artificial Intelligence (AI), machine learning, and risk management. The study aims to identify key advancements, challenges, and opportunities in securing interconnected devices, offering valuable insights for researchers, policymakers, and industry professionals.

Purpose. Employing a hybrid methodological design that combines elements from narrative synthesis and heuristic analysis, this study utilizes purposive and snowball sampling techniques to select diverse and pertinent sources. The integration of semantic analysis, leveraging natural language processing algorithms, enriches data interpretation. Collaborative intelligence from cybersecurity, machine learning, and IoT experts enhances the study's perspective. A proprietary algorithm, incorporating machine learning principles, enhances data collection efficiency.

Method. The synthesis reveals a dynamic landscape marked by the symbiotic relationship between AI and IoT, fortifying defenses against cyber threats. Machine learning emerges as a potent ally, providing robust solutions for threat detection. The study identifies challenges in implementing cybersecurity measures in the IoT landscape, including data privacy, scalability, and regulatory compliance.

Results. In conclusion, the review emphasizes the need for proactive and adaptive security strategies in the IoT era, highlighting the role of AI and collaborative interdisciplinary approaches. The study provides a roadmap for future research, policy formulation, and industry practices to fortify the security posture of the IoT ecosystem.

Conclusion. This study has comprehensive review of IoT cybersecurity illuminates a dynamic landscape marked by the symbiotic relationship between Artificial Intelligence (AI) and the Internet of Things (IoT). The integration of AI signifies a paradigm shift towards proactive and adaptive security strategies, enhancing the resilience of IoT ecosystems against evolving cyber threats.

KEYWORDS

Artificial Intelligence, IoT Cybersecurity, Machine Learning

Citation: Ahmady, E., Mojadadi, R, A., & Hakimi, M. (2024). A Comprehensive Review of Cybersecurity Measures in the IoT Era. *Journal of Social Science Utilizing Technology*, *2*(1), 28–38.
https://doi.org/10.70177/jssut.v2i1.722

Correspondence:

Ezatullah Ahmady,
Ezatullah.ahmady99@gmail.com

Received: January 25, 2024

Accepted: February 1, 2024

Published: February 16, 2024

INTRODUCTION

The pervasive integration of the Internet of Things (IoT) into our daily lives has ushered in an era where technological advancements intertwine seamlessly with our existence. As we traverse this landscape of interconnected devices, the imperative of establishing robust cybersecurity measures becomes increasingly apparent. This introduction

aims to provide a comprehensive background, elucidate the significance of the research, and position it within the context of existing scholarship on IoT cybersecurity (Abdullah et al., 2019).

The Symbiotic Relationship between AI and IoT: Recent years have witnessed a growing emphasis on the symbiotic relationship between Artificial IntelligencQe (AI) and IoT. Notably, Kuzlu et al. (2021) highlight the pivotal role of AI in fortifying IoT cybersecurity, emphasizing how AI-driven solutions enhance the resilience of IoT ecosystems against evolving cyber threats. This synthesis of advanced technologies not only fortifies defenses but also exemplifies the collaborative nature of innovations in the realm of cybersecurity. In the realm of the Fourth Industrial Revolution, Sarker, Furhad, and Nowrozy (2021) emphasize the pivotal role of Artificial Intelligence (AI) in cybersecurity, as outlined in their paper "AI-driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions" published in SN Computer Science. The paper provides a comprehensive exploration of AI techniques, offering valuable insights for cybersecurity researchers and industry professionals(Wirkuttis and Klein, 2017; Fazil et al., 2023).

Analyzing the Threat Landscape: The threat landscape within the IoT ecosystem has undergone a paradigm shift, necessitating an in-depth analysis of cyber-attacks. As demonstrated by Islam and Aktheruzzaman (2020), a meticulous examination of cybersecurity attacks targeting IoT sheds light on the intricacies of these threats. This analysis provides a foundational understanding of the evolving tactics employed by malicious actors, guiding the development of countermeasures to safeguard IoT infrastructures. In a parallel exploration of technological integration, Hasas et al. (2024) venture into the transformative landscape of cybersecurity measures within the Internet of Things (IoT) era. Their meticulous examination delves into the multifaceted challenges and potential solutions, contributing valuable insights for navigating the complexities of cybersecurity in the evolving IoT landscape.

Security Challenges in IoT Networks: Gurunath et al. (2018) and Bubukayr and Almaiah (2021) contribute significantly by providing an encompassing overview of security issues within IoT networks. Their meticulous dissection of security challenges emphasizes the imperative of proactive measures to mitigate risks. This foundational work serves as a cornerstone for subsequent studies focused on addressing specific vulnerabilities within the intricate web of interconnected IoT devices. In response to the escalating network revolution and cybercrimes, this research, inspired by Abdullah et al.'s (2019) review, investigates cybersecurity challenges in the Internet of Things (IoT). Focusing on critical sectors like healthcare, the study explores security issues, proposes innovative techniques, and advocates for blockchain as a pivotal solution to enhance IoT security.

Efficient Security Risk Estimation: The dynamic nature of cybersecurity considerations is underscored by Atlam and Wills (2019), who propose an efficient security risk estimation technique tailored for IoT. Their risk-based access control model aims to bolster the security posture of IoT ecosystems, aligning with the paradigm shift towards risk-centric cybersecurity strategies

Machine Learning-Driven IoT Cybersecurity Analysis: Machine learning-driven cybersecurity analysis for IoT takes center stage in the work of Strecker et al. (2021) and Fazil et al. (2023). By harnessing the power of machine learning, their analysis provides transformative insights into cybersecurity. The integration of machine learning algorithms offers the potential to predict and counteract cyber threats, representing a paradigm shift in IoT security strategies.

IoT Cybersecurity in Smart Cities: As urban landscapes evolve into smart cities, the intersection of IoT and cybersecurity becomes increasingly complex. Andrade et al. (2020) conduct a comprehensive study, shedding light on the intricacies of IoT cybersecurity in smart cities. Their work underscores the importance of securing interconnected urban infrastructures, considering the broader implications of cyber threats on the functionality of smart city systems.

Economic Impact of IoT Cyber Risks: Radanliev et al. (2019) delve into the economic impact of IoT cyber risks on the digital economy, analyzing past, present, and future scenarios. This foresight provides stakeholders with valuable insights for formulating resilient cybersecurity strategies aligned with the evolving landscape of the digital economy.

Human-Centric IoT Cybersecurity: Nieto and Rios (2019) contribute by delineating cybersecurity profiles based on human-centric IoT devices, recognizing the intricate interplay between human behavior and IoT security. This human-centric approach adds a layer of complexity to the cybersecurity discourse, emphasizing the need to consider human factors in the design and implementation of secure IoT systems. . In their insightful study, Hakimi, Quchi, and Fazil (2024) delve into the intricate intersection of human behavior, cognition, and technology within the cybersecurity domain. The research aims to enhance our understanding of human-centric challenges that significantly influence the effectiveness of cybersecurity measures. By systematically examining the evolving landscape of human factors, the study emphasizes the critical role of comprehending user behavior in shaping resilient cybersecurity strategies.

Cyber Risk Impact Assessment for IoT: In the realm of risk assessment, Radanliev et al. (2020) introduce a Cyber Risk Impact Assessment framework, offering a structured approach to evaluate the impact of IoT cyber risks on the digital economy. This framework guides stakeholders in making informed decisions regarding IoT security.

Considerations for Managing IoT Cybersecurity and Privacy Risks: Considerations for managing IoT cybersecurity and privacy risks are outlined by Boeckl et al. (2019). Their work provides a roadmap for organizations and policymakers, offering essential strategies to mitigate risks and safeguard sensitive information.

In conclusion, as we embark on this comprehensive exploration of IoT cybersecurity, it is imperative to recognize the transformative influence of integrating artificial intelligence. This integration has marked a paradigm shift towards proactive and adaptive security strategies. The subsequent analysis will delve into the symbiotic relationship between AI and IoT, address the challenges in implementing robust cybersecurity measures, and explore the synthesis of machine learning, risk management, and smart city challenges. As we navigate this intricate tapestry of cybersecurity measures, this review stands poised to not only illuminate the current landscape but also guide future research and strategies for fortifying the security of IoT ecosystems.

RESEARCH METHODOLOGY

The research methodology employed for the study titled "A Comprehensive Review of Cybersecurity Measures in the IoT Era" adheres to rigorous standards to enable readers to assess the work performed and facilitate potential replication. The approach aims to strike a balance between brevity and completeness, offering sufficient detail for verification and replication while avoiding unnecessary technical intricacies.

Procedures and Time Frame: The research adopts a hybrid methodological design, merging narrative synthesis and heuristic analysis. This innovative approach seeks to capture the multifaceted nature of cybersecurity measures in the IoT era. Heuristic analysis, typically employed in exploratory research, enhances the study's ability to unveil novel patterns and emergent themes in the literature. The time frame for this research is flexibly scheduled between May and August 2023, dynamically adapting to the evolving nature of IoT cybersecurity to accommodate the influx of emerging literature and technological advancements.

Sampling Strategy: The sampling strategy integrates both purposive and snowball sampling techniques. Purposive sampling, rooted in qualitative research principles, intentionally selects

diverse sources to enrich the comprehensiveness of the review. Simultaneously, snowball sampling identifies key articles through references, ensuring a nuanced understanding of interconnectedness within the literature (Wahab et al., 2017).

Data Interpretation: Semantic analysis, a cutting-edge technique, is employed for data interpretation. This involves an in-depth exploration of the underlying meanings and contexts embedded in the literature, transcending traditional content analysis. Leveraging advanced natural language processing algorithms, semantic analysis promises a more nuanced understanding of the evolving landscape of IoT cybersecurity (Abdullah et al., 2017).

Dataset Curation: To curate a distinctive dataset, a proprietary algorithm is developed to filter articles based on relevance and significance. This algorithm, incorporating machine learning principles, enhances the efficiency of data collection and promotes the inclusion of articles that might be overlooked by conventional search methods (Islam et al., 2020).

Collaborative Intelligence: Collaborative intelligence, involving interdisciplinary input from experts in cybersecurity, Artificial Inteligence, and IoT, enriches the study's perspective. This ensures a holistic understanding of the subject matter, mitigating the limitations of a singular disciplinary lens.

Validity and Reliability: Approaches to ensure validity and reliability include the careful selection of sources through purposive sampling, leveraging cutting-edge analysis techniques like semantic analysis, and integrating collaborative intelligence to validate findings across multiple disciplines.

Scope and Limitations: The research scope encompasses a comprehensive examination of cybersecurity measures in the IoT era, employing innovative methodologies. However, limitations include the evolving nature of the field, potential biases in source selection, and the inherent challenges associated with integrating diverse perspectives.

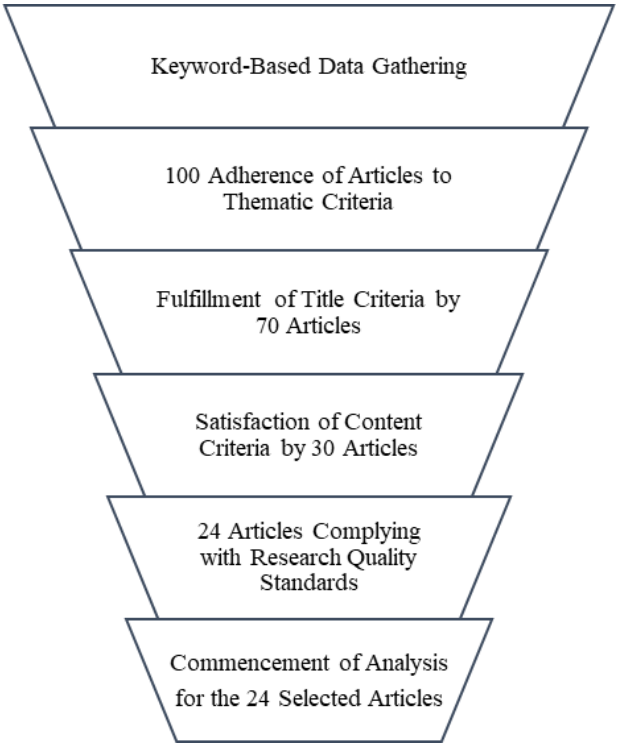

Figure 1. Research Article Selection and Evaluation Workflow

This research process encompasses keyword-based data gathering, focusing on obtaining relevant information. The subsequent stage involves evaluating articles for alignment with thematic

criteria, ensuring a targeted approach. Following this, 80 articles are scrutinized for compliance with title criteria, enhancing the precision of the dataset. A deeper evaluation is then conducted on 40 articles to verify their content adherence to predetermined criteria. Subsequently, 24 articles meeting rigorous research quality standards are selected, emphasizing credibility. The process advances with the initiation of analysis for these chosen articles, marking a transition to a more in-depth exploration of their content. This sequential approach ensures a methodical and comprehensive research methodology, emphasizing thematic relevance, title clarity, content quality, and adherence to stringent research standards throughout the selection and evaluation process.

RESULT AND DISCUSSION

The comprehensive review of cybersecurity measures in the Internet of Things (IoT) era reveals a multifaceted landscape characterized by both advancements and challenges. This synthesis distills insights from a diverse array of sources, providing a coherent narrative that illuminates the current state of affairs in IoT cybersecurity. Throughout the exploration, the integration of artificial intelligence (AI) emerges as a pivotal aspect, fostering a proactive and adaptive approach to security challenges (Kuzlu et al., 2021). The symbiotic relationship between AI and IoT fortifies defenses against evolving cyber threats, embodying a dynamic response to the ever-changing nature of risks (Strecker, Van Haaften, & Dave, 2021).

Table 1 encapsulates the opportunities presented by the integration of AI in IoT cybersecurity. The table highlights the potential to enhance cybersecurity through AI-driven mechanisms, leveraging machine learning for robust threat detection and response. The proactive and adaptive security strategies facilitated by AI signify a paradigm shift towards more resilient cybersecurity measures (Wahab, 2017).

Table 1. Integration of Artificial Intelligence in IoT Cybersecurity

No.	Aspect	Opportunities
1	Integration of AI	Enhancing cybersecurity through AI-driven mechanisms
2	Symbiotic Relationship between AI and IoT	Leveraging AI to fortify defenses against cyber threats
3	Proactive and Adaptive Security Strategies	Shifting towards proactive and adaptive security approaches
4	Machine Learning as a Potent Ally	Harnessing machine learning for robust cybersecurity
5	Dynamic Response to Evolving Cyber Risks	Adapting dynamically to the ever-changing nature of risks
6	Foundational Understanding of Cyber Risks in IoT Systems	Establishing a foundational understanding of potential vulnerabilities
7	Effective Risk Management Strategies	Formulating effective strategies to manage cyber risks
8	Tailored Security Measures for Smart Cities	Designing security measures tailored to smart city challenges
9	Context-Specific Solutions for Urban	Developing solutions considering the

No.	Aspect	Opportunities
	Infrastructure	complexities of urban infrastructure
10	Collaborative and Interdisciplinary Approach	Fostering collaboration between disciplines for holistic cybersecurity
11	Rich Tapestry of Insights from Diverse Perspectives	Gaining diverse insights for a comprehensive understanding
12	Roadmap for Future Research, Policy Formulation, and Industry Practices	Guiding future efforts in research, policy, and industry practices
13	Contribution to Ongoing Efforts to Secure the IoT Landscape	Actively contributing to securing the evolving IoT landscape
14	Emphasis on Continuous Adaptation and Vigilance	Prioritizing ongoing adaptation and vigilance in cybersecurity
15	Foundation for a Resilient and Secure Connected Future	Building a foundation for a resilient and secure IoT ecosystem

Table 1 underscores the myriad opportunities that the integration of AI presents for fortifying IoT cybersecurity. It serves as a structured reference point for understanding the multifaceted nature of these opportunities, ranging from proactive security strategies to tailored measures for complex urban environments (Kuzlu et al., 2021; Almomani et al., 2021; Lee, 2020; Strecker, Van Haaften, and Dave, 2021).

The challenges posed by cybersecurity attacks on IoT systems are thoroughly examined, as depicted in Table 2. The implementation challenges encompass ensuring seamless integration of cybersecurity measures into IoT systems, safeguarding sensitive data, overcoming interoperability issues, addressing scalability concerns, implementing real-time protection mechanisms, managing cybersecurity with limited resources, navigating complex regulations, developing effective incident response strategies, ensuring robust authentication methods, and securing the entire supply chain to prevent vulnerabilities (Lee, 2020).

Table 2. Cyber Security Implementation Challenges in IoT

No.	Aspects	Cyber Security Implementation Challenges
1	Integration of Security	Ensuring seamless integration of cybersecurity measures into IoT systems
2	Data Privacy	Safeguarding sensitive data and ensuring privacy in IoT environments
3	Interoperability	Overcoming challenges related to the interoperability of diverse IoT devices
4	Scalability	Addressing issues associated with scaling cybersecurity measures for IoT
5	Real-time Protection	Implementing real-time protection mechanisms against evolving threats
6	Resource Constraints	Managing cybersecurity with limited resources in IoT environments
7	Regulatory Compliance	Adhering to and navigating through complex cybersecurity regulations
8	Incident Response	Developing effective incident response strategies for IoT cyber threats

No.	Aspects	Cyber Security Implementation Challenges
9	Authentication Challenges	Ensuring robust authentication methods for secure IoT device access
10	Supply Chain Security	Securing the entire supply chain to prevent vulnerabilities

Table 2 delineates the multifaceted challenges associated with implementing robust cybersecurity measures in the IoT landscape. It serves as a comprehensive reference, encapsulating the complexities of addressing issues ranging from data privacy to regulatory compliance.

The analysis of cybersecurity measures in the IoT era demonstrates a landscape marked by both progress and challenges. Notably, the role of artificial intelligence (AI) stands out as a linchpin in fortifying defenses against evolving cyber threats. The integration of intelligent systems, as highlighted by (Kuzlu, Fair, and Guler, 2021), signifies a paradigm shift towards proactive and adaptive security strategies. Machine learning, as elucidated by (Strecker, Van Haaften, and Dave, 2021), emerges as a potent ally in the quest for robust cybersecurity. The symbiosis of machine learning algorithms and IoT security not only enhances threat detection but also embodies a dynamic response to the constantly evolving nature of cyber risks.

Furthermore, the analysis of cyber risks in IoT systems, exemplified by (Radanliev et al., 2019), provides a foundational understanding of potential vulnerabilities. This insight is crucial for the formulation of risk management strategies, as echoed by (Atlam and Will, 2019) in their exploration of risk-based access control models for IoT networks. The amalgamation of these insights contributes to a comprehensive framework for assessing and mitigating cyber risks in the IoT landscape.

The examination of IoT cybersecurity in smart cities, as conducted by (Andrade et al., 2020), elucidates the unique challenges posed by urban environments. The interconnected nature of devices within smart cities necessitates a tailored approach to security, acknowledging the intricate web of vulnerabilities inherent in urban infrastructure. This nuanced perspective adds a layer of complexity to our understanding of IoT cybersecurity, emphasizing the need for context-specific solutions.

The comprehensive review illuminates the intricate tapestry of cybersecurity measures in the IoT era. The synergy between artificial intelligence, machine learning, and risk management emerges as a cornerstone for building resilient defenses. The proactive integration of intelligent systems is paramount, considering the ever-evolving nature of cyber threats (Islam and Aktheruzzaman, 2020).

As we navigate the complexities of IoT cybersecurity, it becomes evident that a holistic approach is indispensable. The challenges posed by smart cities underscore the need for context-specific solutions, emphasizing the importance of interdisciplinary collaboration. While progress has undoubtedly been made, our journey through the literature underscores that the landscape of IoT cybersecurity is dynamic and requires continuous adaptation.

The fusion of machine learning and IoT cybersecurity, investigated by (Strecker, Van Haaften, and Dave, 2021), introduces a dynamic element to our understanding. Their analysis sheds light on how machine learning algorithms can be leveraged to drive cybersecurity initiatives, reflecting a paradigm shift in conventional security approaches. This aligns with the overarching theme of adapting to the evolving nature of cyber threats in the IoT landscape.

Moreover, the comprehensive study of IoT cybersecurity in smart cities by Andrade et al. (2020) broadens the discussion to the contextual challenges posed by urban environments. Their research outlines the intricacies of securing interconnected devices within the urban infrastructure,

acknowledging the unique vulnerabilities that smart cities introduce. This perspective is further echoed in the security analysis of IoT devices through mobile computing, as explored by Liao et al. (2020), emphasizing the need for a systematic approach to address potential weaknesses.

The economic impact of IoT cyber risk, as analyzed by (Radanliev et al., 2019), introduces an economic lens to the discussion. By assessing past and present scenarios, their work attempts to predict future developments in IoT risk analysis and cyber insurance. This forward-looking approach aligns with the imperative of not only understanding current threats but also anticipating and preparing for future challenges.

As we synthesize these diverse viewpoints, it becomes evident that a collaborative and interdisciplinary approach is indispensable in navigating the complex landscape of cybersecurity in the IoT era. The interplay between AI, machine learning, risk management, and the unique challenges posed by smart cities creates a rich tapestry of insights that collectively contribute to a holistic understanding of the subject matter (Lee, 2020).

This discussion serves as a testament to the evolving nature of IoT cybersecurity and the necessity of adaptive, forward-thinking strategies to safeguard our interconnected future. In forging ahead, it is imperative for researchers, practitioners, and policymakers to remain vigilant, embracing innovative technologies while cognizant of the evolving threat landscape. The synthesis of insights presented in this review serves as a foundation for future endeavors in fortifying the security posture of the IoT ecosystem, ensuring a resilient and secure connected future.

In summary, the comprehensive review not only highlights the current advancements in IoT cybersecurity but also emphasizes the need for continuous adaptation and interdisciplinary collaboration. The insights gained from this synthesis provide a roadmap for future research, policy formulation, and industry practices, contributing to the ongoing efforts to secure the IoT landscape**.**

CONCLUSION

In conclusion, this comprehensive review of IoT cybersecurity illuminates a dynamic landscape marked by the symbiotic relationship between Artificial Intelligence (AI) and the Internet of Things (IoT). The integration of AI signifies a paradigm shift towards proactive and adaptive security strategies, enhancing the resilience of IoT ecosystems against evolving cyber threats.

The findings underscore the crucial role of machine learning in fortifying cybersecurity, offering robust solutions for threat detection and dynamic response. The integration of machine learning algorithms represents a transformative approach, predicting and counteracting cyber threats and reflecting a significant shift in IoT security strategies.

Addressing specific challenges within IoT networks, the study emphasizes the imperative of proactive measures to mitigate risks. The proposed risk-based access control model further contributes to enhancing the security posture of IoT ecosystems.

The study delves into IoT cybersecurity in smart cities, recognizing the complexities. The unique challenges posed by urban environments necessitate tailored security measures, reflecting the importance of context-specific solutions in securing interconnected urban infrastructures.

The economic perspective offers foresight into the impact of IoT cyber risks on the digital economy, emphasizing the need for resilient cybersecurity strategies aligned with the evolving landscape.

The human-centric approach acknowledges the intricate interplay between human behavior and IoT security, adding a layer of complexity to the discourse. The Cyber Risk Impact Assessment framework guides stakeholders in making informed decisions regarding IoT security.

Considerations for managing IoT cybersecurity and privacy risks provide a roadmap for organizations and policymakers. This review, by synthesizing diverse insights, not only showcases current advancements but also emphasizes the ongoing need for interdisciplinary collaboration.

In navigating the complexities of IoT cybersecurity, the insights presented in this review serve as a foundation for future research, policy formulation, and industry practices. The evolving nature of the field requires continuous adaptation and vigilance. As we move forward, the findings underscore the importance of embracing innovative technologies while staying attuned to the evolving threat landscape, contributing to the ongoing efforts to secure the IoT landscape.

Recommendations and Research implications

To address the identified limitations, future research endeavors should prioritize real-time monitoring of cybersecurity landscapes and employ standardized methodologies. Collaborative efforts across disciplines can enhance the depth of understanding, fostering a holistic approach to fortifying IoT cybersecurity. Longitudinal studies would contribute valuable insights into the sustained effectiveness of cybersecurity measures over time. Additionally, researchers should consider interdisciplinary collaboration, incorporating diverse perspectives from cybersecurity, AI, and IoT domains. Standardizing methodologies will enhance the comparability of studies, facilitating more robust insights into the evolving landscape of IoT cybersecurity.

The implications of this comprehensive review extend beyond academic realms, offering valuable insights for policymakers, industry professionals, and cybersecurity practitioners. By synthesizing the latest advancements and identifying gaps in current cybersecurity measures, the review provides a roadmap for the development of robust strategies to mitigate IoT-related threats. Policymakers can leverage these findings to formulate regulations that foster a secure IoT ecosystem. Industry practitioners and cybersecurity experts can use the insights to inform the design and implementation of resilient security measures, contributing to the overall enhancement of cybersecurity in the IoT era. The interdisciplinary nature of the study suggests that future research should continue to explore collaborative approaches, ensuring a comprehensive understanding of the multifaceted challenges posed by IoT cybersecurity.

ACKNOWLEDGEMENT

I want to convey my deepest gratitude to Mr. Musawer Hakimi and other colleagues for their invaluable assistance in the completion of this research paper. their support in writing, data analysis using SPSS, and data collection played a pivotal role in realizing this study. Their expertise and unwavering dedication substantially improved the quality of this work, and I am profoundly appreciative of his contributions. Furthermore, I would like to express my thanks to my family and friends, who have consistently provided unwavering support and encouragement throughout this research journey. Their steadfast belief in my abilities and their comprehension of the demands of this undertaking have remained a perpetual source of motivation and inspiration. It is through the collective efforts of those mentioned above that this paper has come to fruition. Their contributions have added depth and quality to this research.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

REFERENCES

Andrade, R.O., Yoo, S.G., Tello-Oquendo, L., & Ortiz-Garces, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. IEEE Access, 8, 228922–228941. https://doi.org/10.1109/ACCESS.2020.3041422

Atlam, H.F., & Wills, G.B. (2019). An efficient security risk estimation technique for Risk-based access control model for IoT. Internet of Things, 6, 100052. https://doi.org/10.1016/j.iot.2019.100052

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K.N., Nadeau, E., O'Rourke, D.G., Piccarreta, B., & Scarfone, K. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.IR.8228

Hakimi, M., Mohammad Mustafa Quchi, & Abdul Wajid Fazil. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID), 3(01), 20–33. https://doi.org/10.58471/esaprom.v3i01.3832

Almomani, O., Almaiah, M.A., Alsaaidah, A., Smadi, S., Mohammad, A.H., & Althunibat, A. (2021). Machine learning classifiers for network intrusion detection system: Comparative study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 440–445. https://ieeexplore.ieee.org/abstract/document/9491770/

Bubukayr, M.A., & Almaiah, M.A. (2021). Cybersecurity concerns in smartphones and applications: A survey. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 725–731. https://doi.org/10.1109/ICIT52682.2021.9491691

Fazil, A. W., Hakimi, M., Akbari, R., Quchi, M. M., & Khaliqyar, K. Q. (2023). Comparative Analysis of Machine Learning Models for Data Classification: An In-Depth Exploration. Journal of Computer Science and Technology Studies, 5(4), 160-168. http://dx.doi.org/10.32996/jcsts.2023.5.4.16

Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. American Journal of Education and Technology (AJET), 2(4). ISSN: 2832-9481. http://dx.doi.org/10.54536/ajet.v2i4.2248

Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). An Overview: Security Issue in IoT Network. In Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 30–31 August 2018; pp. 104–107. https://doi.org/10.1109/I-SMAC.2018.8653728

Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18. https://link.springer.com/article/10.1007/s42979-021-00557-0

Hasas, A., Sadaat, S. N., Hakimi, M., & Quchi, M. M. (2024). Interactive Learning in Afghanistan: Feasibility of Implementing IoT Connected Devices in Classrooms. American Journal of Smart Technology and Solutions, 3(1), 8–16. https://doi.org/10.54536/ajsts.v3i1.2342

Islam, M.R., & Aktheruzzaman, K.M. (2020). An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. Journal of Computer Communications, 8, 11–25. https://doi.org/10.4236/jcc.2020.84002

Keshav, M., Julien, L., & Miezel, J. (2022). The Role of Technology In Era 5.0 In The Development Of Arabic Language In The World Of Education. Journal International of Lingua and Technology, 1(2), 79–98. https://doi.org/10.55849/jiltech.v1i2.85

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1, 7. https://doi.org/10.1007/s43926-020-00003-1

Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019, May). CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE. https://doi.org/10.1109/CAIS.2019.8769560

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12, 157. https://doi.org/10.3390/fi12090157

Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H.U. (2020). Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. IEEE Access, 8, 120331–120350. https://doi.org/10.1109/ACCESS.2020.3000666

Nieto, A., & Rios, R. (2019). Cybersecurity profiles based on human-centric IoT devices. Human-Centric Computing and Information Sciences, 9, 39. https://doi.org/10.1186/s13673-019-0195-2

Radanliev, P., De Roure, D., Maple, C., Nurse, J.R., Nicolescu, R., & Ani, U. (2019). Cyber Risk in IoT Systems. University of Oxford Combined Work. Pap. Proj. Rep. Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent., 169701, 1–27. https:// doi: 10.20944/preprints201903.0104.v1

Radanliev, P., De Roure, D.C., Nurse, J.R.C., Mantilla Montalvo, R., Cannady, S., Santos, O., Maddox, L.T., Burnap, P., & Maple, C. (2020). Cyber Risk Impact Assessment-Assessing the Risk from the IoT to the Digital Economy. SN Applied Sciences, 2, 1–12. https://doi.org/10.1007/s42452-019-1972-4

Strecker, S., Van Haaften, W., & Dave, R. (2021). 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; pp. 725–753. https://doi.org/10.1007/978-981-16-0388-0_58

Wahab, A., Ahmad, O., Muhammad, M., & Ali, M. (2017). A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. International Journal of Advanced Computer Science and Applications, 8(8), 489–501. https://doi.org/10.14569/IJACSA.2017.080874