IJIBC 24-2-1

Securing the IoT Frontier: Exploring the Limitation and Future Directions in Cybersecurity

Moustafa Abdelrahman Mahmoud Ahmed,[1] Nur Arzilawati Md Yunus[2*]

[1] Master(M.A.), University Malaysia of Computer Science and Engineering, Selangor, Malaysia
[2]Senior Lecturer, Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Selangor, Malaysia
E-mail: m.abdelrahman.moustafa@gmail.com, nurarzilawati@upm.edu.my

Abstract

As the Internet of Things (IoT) continues to permeate every facet of modern life, the imperative to secure this vast and dynamic frontier becomes increasingly paramount. This presents a comprehensive exploration of the challenges and opportunities inherent in safeguarding the interconnected web of IoT devices. The research critically examines the limitations of current cybersecurity measures through an extensive review of diverse topics, including IoT network performance, smart grid security, and the escalating cyber threats against critical infrastructures. A meticulous analysis of research findings underscores the need for enhanced infrastructure and ongoing research to fortify the cybersecurity mechanisms surrounding IoT objects. We underline the imperative of relentless research efforts to parry the advancing threats and leverage the promise of nascent technologies. Our findings affirm the pivotal influence of robust cybersecurity measures in crafting a resiliently connected ecosystem. The paper underscores the importance of ongoing research to address evolving threats and harness the potential of emerging technologies, reaffirming the central role of cybersecurity in shaping a secure interconnected world. In conclusion, the study emphasizes the dynamic and ever-evolving nature of cybersecurity on the IoT frontier. It unveils a complex landscape of challenges, ranging from network performance intricacies to the security concerns of critical infrastructures.

Keywords: *Internet of Things, Cybersecurity Future Directions, Cybersecurity Threats, Cybersecurity Limitation.*

1. INTRODUCTION

In an era dominated by the interconnectivity of devices and the rapid evolution of technology, the paramount importance of cybersecurity cannot be overstated. This paper embarks on a comprehensive exploration of the intricate landscape of cybersecurity, focusing specifically on the challenges and the future direction within the realm of the Internet of Things (IoT). The research delves into a myriad of topics, ranging from the enhancement of IoT network performance to the imperative need for cybersecurity awareness in modern industrial settings. The multifaceted nature of cybersecurity is unveiled through an examination of emerging technologies like IoT, discussions on Industry 4.0 pillars, and the identification of cyber threats in diverse sectors such as smart farming and the maritime industry.

Manuscript Received: March. 2, 2024 / Revised: March. 10, 2024 / Accepted: March. 15, 2024
Corresponding Author: nurarzilawati@upm.edu.my
Tel: +03-97691733
Author’s affiliation (Senior Lecturer, Faculty of Computer Science & Information Technology, UPM, Malaysia)

Section 2 of this paper meticulously dissects the limitations inherent in contemporary cybersecurity efforts. These limitations are drawn from a diverse array of research findings, including challenges associated with the IoT ecosystem's scale and heterogeneity, discrete modeling of time in security frameworks, and the escalating cyber threats against critical infrastructures such as nuclear facilities and power grids. The paper underscores the necessity for a more robust infrastructure to enhance the security of IoT devices and emphasizes the need for ongoing research to fortify the cybersecurity mechanisms surrounding IoT objects. Moving forward, Section 3 charts the future direction of cybersecurity, laying the groundwork for prospective research endeavors. The discussion encompasses the development of deep learning algorithms, cybersecurity awareness initiatives in Industrial Internet of Things (IIoT) contexts, empirical analyses of IoT-enabled capabilities in smart government performance, and the application of frameworks in Industry 4.0 settings. The research also advocates for a quantitative assessment of tech abuse, increased sample sizes for more representative data, and the exploration of explainability in Long Short-Term Memory (LSTM) models for detecting IoT cyberattacks.

In the conclusion Section 4, the study conclude on the dynamic and ever-evolving nature of cybersecurity, positioned at the forefront of safeguarding our interconnected world. The complex tapestry of challenges and opportunities within IoT security is unveiled, ranging from network performance to smart grid intricacies. The paper navigates through the limitations of contemporary cybersecurity efforts, offering insights into the escalating threats against critical infrastructures. As the exploration shifts towards the future, promising research directions and potential solutions are illuminated, underscoring the continued importance of addressing evolving threats and harnessing the potential of emerging technologies. The conclusion emphasizes that the pursuit of a more secure interconnected world remains a driving force, propelling innovation, and research in the vital domain of cybersecurity.

2. LIMITATION OF CYBERSECURITY IN IOT

An active attack in the context of cybersecurity refers to a type of malicious action where an attacker attempts to alter or manipulate data, systems, or network traffic as shown in Figure 1. Active attacks can have severe consequences, including data breaches, service disruptions, financial losses, and reputational damage. The imperative for cybersecurity awareness in modern industrial contexts underscores the growing significance of educating stakeholders about the evolving threat landscape [2]. With industries becoming increasingly digitized, the human factor remains a critical element in fortifying defenses against cyber threats. Exploring the potential of IoT-enabled dynamic capabilities involves understanding how interconnected devices can adapt and evolve to meet changing demands [3]. The IoT technologies should create adaptive systems that can seamlessly integrate new functionalities and respond effectively to emerging challenges, thereby enhancing overall system resilience. The benefits of open-source cybersecurity training platforms are highlighted in this paper, emphasizing the advantages of accessible and collaborative learning resources [4]. Such platforms contribute to the democratization of cybersecurity education, allowing a wider audience to acquire essential skills and knowledge to combat cyber threats. The importance of understanding smart grid cybersecurity objectives is paramount as smart grids play a crucial role in modern energy systems [5]. This involves developing robust security frameworks tailored to the unique characteristics of smart grid environments.

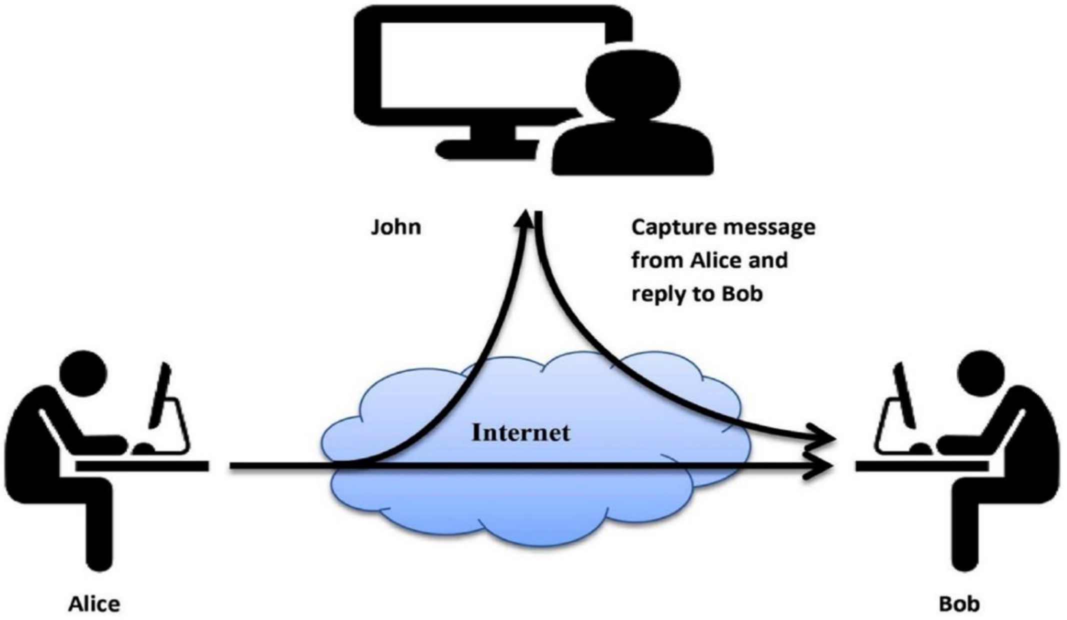

Figure 1. Example of active attack.

The application of IoT in smart grids introduces a paradigm shift in the energy sector. However, it also raises concerns about the potential security implications associated with the integration of numerous IoT devices into critical infrastructure [6]. A security cognitive model proposal signifies an innovative approach to cybersecurity. By incorporating cognitive models into cybersecurity strategies, researchers seek to create more user-friendly and effective security measures [7]. The relevance of IPV research in relation to emerging technologies like IoT addresses the foundational aspects of network communication [8]. As IoT devices heavily rely on the Internet Protocol version 6 (IPv6) for communication, understanding and optimizing IPV is crucial for ensuring a scalable and secure IoT ecosystem. Discussions on Industry 4.0 pillars provide insights into the ongoing transformation of industries through the integration of advanced technologies [9]. Research in this area explores the key pillars of Industry 4.0, such as connectivity, data analytics, and automation, with a focus on identifying and mitigating cybersecurity challenges associated with this transformative process.

The need for infrastructure to enhance IoT device security emphasizes the importance of a robust foundation for securing interconnected devices [10]. This research explores the development of secure infrastructures that can effectively support and protect IoT devices throughout their lifecycle, addressing vulnerabilities from the hardware level to the application layer. The proposal of new testbeds and datasets for IoT network cybersecurity signifies a practical approach to advancing cybersecurity research [11], [12]. Testbeds and datasets play a crucial role in evaluating the effectiveness of security solutions in realistic scenarios. Identification of cybersecurity threats in smart farming sheds light on the unique challenges faced by the agriculture sector in adopting IoT technologies [13]. This research aims to identify potential threats to smart farming systems, such as unauthorized access to agricultural data and disruption of automated processes and proposes strategies to mitigate these risks.

Challenges in IoT cybersecurity certification are explored to address the growing need for establishing trust in IoT devices. Certification processes ensure that devices meet predefined security standards [13]. However, the diverse nature of IoT devices poses challenges in creating universal certification frameworks, and research in this area seeks to overcome these hurdles. Scheme analysis for fault tolerance in network topology involves investigating strategies to enhance the resilience of IoT networks [14]. By analyzing network schemes, researchers aim to identify potential points of failure and develop fault-tolerant solutions, ensuring the continuous operation of IoT devices even in the face of network disruptions. The proposal of a weighted-sum cost function for effectiveness evaluation introduces a quantitative approach to assess the effectiveness of cybersecurity measures [15].

The bid management system in a private blockchain environment explores the integration of blockchain technology into cybersecurity practices [16]. By leveraging the decentralized and tamper-resistant nature of blockchain, this research aims to enhance the security and transparency of bid management systems, particularly in private environments. The application of cognitive security techniques involves incorporating artificial intelligence and machine learning into cybersecurity frameworks [17]. By utilizing cognitive techniques, researchers seek to create adaptive and intelligent security systems capable of identifying and mitigating emerging threats in real-time. Mechanization of a security framework using Alloy represents an effort to automate and formalize cybersecurity processes [18]. Alloy is a formal modeling language, and this research explores its application in mechanizing security frameworks, aiming to improve the precision and reliability of security mechanisms. The transition to Industry 4.0 signifies a broader societal shift toward highly interconnected and automated systems [19]. Research in this area explores the social, economic, and cybersecurity implications of this transition, aiming to guide policymakers and industry leaders in navigating the challenges and opportunities associated with Industry 4.0.

Cybersecurity threats in the maritime industry highlight the vulnerabilities of critical infrastructure beyond traditional sectors [20]. This research examines the unique cybersecurity challenges faced by the maritime sector, such as the potential for cyber-physical attacks on shipping systems and port facilities. A NIDS-based IoT attack detection system focuses on the development of Network Intrusion Detection Systems (NIDS) specifically tailored for IoT environments [21], [22]. These systems aim to detect and mitigate cyberattacks targeting IoT devices by analyzing network traffic patterns and identifying anomalous behavior. An ensemble method for IoT cyberattack detection explores the use of ensemble learning techniques to enhance the accuracy and robustness of cyberattack detection in IoT ecosystems [23]. By combining multiple detection methods, researchers aim to create more resilient systems capable of accurately identifying a diverse range of cyber threats. The importance of IDS techniques for IoT security emphasizes the central role of Intrusion Detection Systems (IDS) in safeguarding IoT environments [24]. Research in this area focuses on developing and optimizing IDS techniques tailored to the unique characteristics of IoT networks, providing early detection and response to potential threats.

Security certificates in a Cloud/Edge enabled IoT model addresses the evolving landscape of IoT deployments with the integration of cloud and edge computing [25]. This research explores the role of security certificates in ensuring the integrity and confidentiality of data transmitted between IoT devices and cloud/edge infrastructure. The lack of research in hardening and security validations draws attention to a potential gap in the existing body of cybersecurity knowledge [26]. This research advocates for a more comprehensive understanding of hardening techniques and security validations, essential components in fortifying systems against potential cyber threats. A new taxonomy of cyberattacks on critical infrastructure contributes to the development of a systematic classification system for cyber threats targeting critical infrastructure [27]. By creating a taxonomy, researchers aim to enhance the understanding of different types of cyberattacks, facilitating more targeted and effective cybersecurity strategies. The importance of staying updated on cybersecurity in IIoT underscores the dynamic nature of the cybersecurity landscape, particularly in the context of IIoT [28]. Continuous research and awareness are crucial in adapting security measures to evolving threats and ensuring the resilience of industrial systems. A cyber range is a controlled, simulated environment designed for cybersecurity training, testing, and research purposes. It provides a secure platform where individuals or teams can practice defending against and responding to various cyber threats, without risking real-world systems or networks as shown in Figure 2.

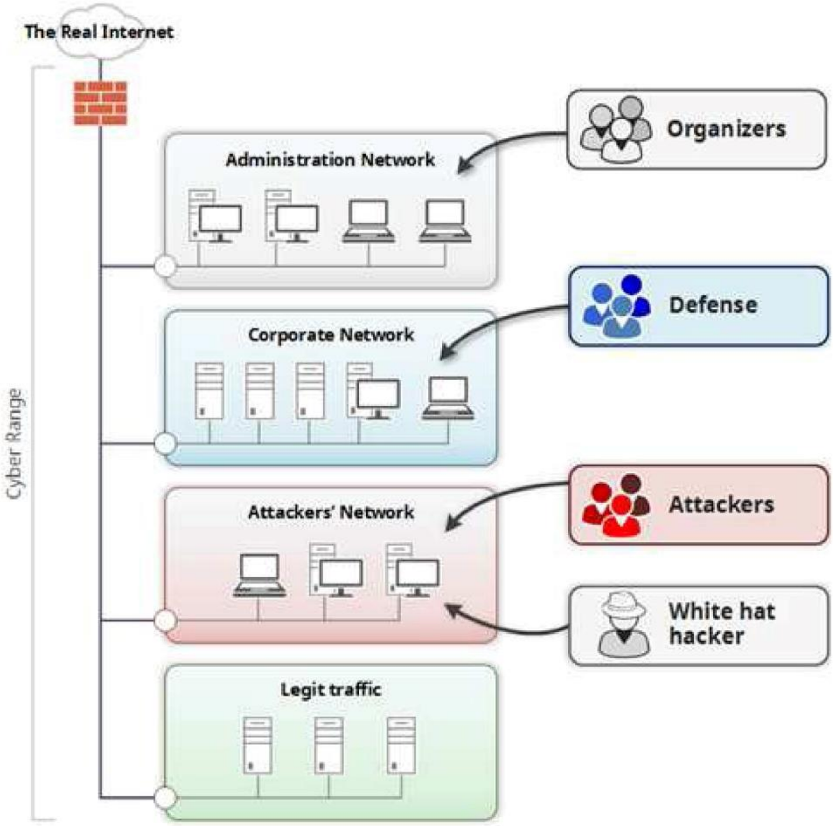

Figure 2. Organizational cyber range.

3. FUTURE DIRECTION OF CYBERSECURITY IN IOT

In the realm of cybersecurity, there is a call to develop methods employing various algorithms, especially deep learning algorithms, for future use [1], [2]. This study, situated within the IIoT paradigm, posits that its findings can aid managers in bolstering cybersecurity awareness to enhance a company's resilience against cyber-attacks [2]. The potential for further research is suggested, exploring IoT-enabled dynamic capabilities and their impact on smart government performance, comparing nations with high exposure economies and benchmarking cybersecurity risks and public policies [3]. Additionally, attention is drawn to the need for security considerations throughout the phases of designing, implementing, and integrating IoT devices in smart grid systems [6]. A proposed framework is recommended for quantitative assessment of tech abuse, refining prospective threat models related to Internet Protocol Version (IPV) threats [8]. The application of a framework in Industry 4.0 settings to analyze its impact on mitigating cyber privacy and security issues is advocated [9]. Suggestions for future research include expanding sample sizes for more representative data [10]. In the context of precision agriculture, the application of the most suitable mitigation strategy for security enhancement is identified as a future area of focus [29]. Finally, the exploration of explainability in Long

Short-Term Memory (LSTM) models is suggested to create more transparent deep learning models for detecting IoT cyberattacks, especially in adversarial settings [23]. Furthermore, metaheuristic algorithms such as Tabu Search (TS) or other evolutionary computing methods are recommended for threat detection and feature selection due to their promising results in other domains [15].

In the rapidly evolving landscape of cybersecurity, the emphasis on developing advanced methods is evident, particularly through the utilization of various algorithms, with a notable focus on deep learning algorithms [1]. The integration of these methods within the Industrial Internet of Things (IIoT) paradigm is a key aspect, suggesting that the insights gained from such studies can play a crucial role in helping managers enhance cybersecurity awareness within their organizations. This, in turn, contributes to bolstering a company's resilience against cyber-attacks [2]. The potential for future research is highlighted in several dimensions. Firstly, there is a call to explore IoT-enabled dynamic capabilities and their impact on smart government performance, drawing comparisons between nations with high exposure economies [30]. Additionally, benchmarking cybersecurity risks and public policies emerges as an avenue for deeper investigation [3]. This broader perspective is crucial in understanding the interconnected nature of cybersecurity challenges on a global scale.

Security considerations throughout the entire lifecycle of IoT devices, from design and implementation to integration into smart grid systems, are emphasized [6]. A proposed framework for the quantitative assessment of tech abuse is recommended, aiming to refine prospective threat models, especially concerning IPv6 threats [8]. This holistic approach addresses the need for comprehensive cybersecurity strategies across different phases of technological development. In the context of Industry 4.0 settings, the application of a framework to analyze its impact on mitigating cyber privacy and security issues is advocated [9]. This suggests a proactive approach to integrating cybersecurity measures into the fabric of evolving technologies. The importance of expanding sample sizes for more representative data in future research is underscored, emphasizing the need for robust and inclusive datasets to draw meaningful conclusions [10].

Precision agriculture emerges as a specific domain of interest, with a call to identify the most suitable mitigation strategy for enhancing security [29]. This underscores the industry-specific nuances that must be considered in developing targeted cybersecurity solutions. In addition, the exploration of explainability in Long Short-Term Memory (LSTM) models is suggested to create more transparent deep learning models for detecting IoT cyberattacks, especially in adversarial settings [23]. This highlights the ongoing efforts to not only enhance the effectiveness of cybersecurity measures but also to make them understandable and interpretable, which is crucial for decision-makers. Moreover, the recommendation to explore the application of metaheuristic algorithms such as Tabu Search (TS) or other evolutionary computing methods for threat detection and feature selection is grounded in their promising results in other domains [15]. This suggests a cross-disciplinary approach, leveraging successful strategies from different fields to strengthen cybersecurity measures. In summary, the future direction in cybersecurity, encompasses a multifaceted approach that spans technological, geopolitical, and methodological dimensions as shown in Table 1. The integration of advanced algorithms, attention to global perspectives, and industry-specific considerations collectively form a comprehensive strategy to address the evolving challenges in the cybersecurity landscape.

Table 1. Future direction of cybersecurity in IoT

Ref.	Future Direction
[1]	To develop methods using various algorithms and to use numerous deep learning algorithms in the future.
[2]	To support managers in activities with the aim of increasing the level of cybersecurity awareness, and thus the resilience of the company to cyber-attacks, with reference to contexts based on the IIoT paradigm.
[3]	To enable IoT capabilities and its impacts on smart government performance empirically by benchmarking IoT-induced cybersecurity risks and public policies to explain the realization of smart government performance or the lack thereof.
[4]	To design cyber ranges based on completely different wireless and smart sensor architectures.
[6]	To focus on security issues during the different phases of designing, implementing, and integrating of the IoT devices in the smart grid
[8]	To quantitatively assess the frequency, extent, regional specificities, and nature of tech abuse to refine prospective IPV threat models
[9]	To apply the proposed framework in Industry 4.0 settings to analyze the impact of the proposed approach in mitigating cyber privacy and security issues.
[10]	To focus on increasing the sample size to capture adequate data that can ensure that there is full representation of the population sample.
[15]	To work on the application of metaheuristic algorithms like TS or other evolutionary computing or nature inspired algorithm for threat detection and feature selection because these optimization algorithms have also shown better results in other domains.
[29]	To apply the most appropriate mitigation strategy for security betterment in precision agriculture systems is scoped as the future work.

4. CONCLUSION

In our study, we've established that cybersecurity's dynamic and constantly developing landscape is paramount in safeguarding our interconnected ecosystem. Delving into the realm of Internet of Things (IoT) security, our exploration uncovered a complex interplay of obstacles and prospects. The exhaustive survey conducted through this paper illuminates the intricate aspects of this crucial area. The comprehensive overview presented in this paper has shed light on the multifaceted nature of this critical domain. We identified and explored the limitations impacting IoT cybersecurity, ranging from network performance to the security of smart grids. Furthermore, our investigation probed into the various dimensions of burgeoning technologies like IoT. Looking forward, we have highlighted promising avenues for future research and potential strategies to address the existing hurdles. Navigating this perpetually shifting terrain, the focus remains on countering the advancing threats and leveraging the capabilities of nascent technologies, which are fundamental to the cybersecurity field. Though the path forward presents challenges, the quest for a more secure and connected world endures, continually inspiring innovation and scholarly inquiry within this essential sector. We navigate this ever-changing landscape, addressing the evolving threats and harnessing the potential of emerging technologies will remain central to the field of cybersecurity. The journey ahead is challenging, but the pursuit of a more secure interconnected world is a mission that continues to drive innovation and research in this vital domain.

REFERENCES

[1] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, “Anomaly-based intrusion detection system for IoT networks through deep learning model,” Computers and Electrical Engineering, vol. 99, Apr. 2022, DOI: 10.1016/j.compeleceng.2022.107810.

[2] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, “Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review,” Computers in Industry, vol. 137. Elsevier B.V., May 01, 2022. DOI: 10.1016/j.compind.2022.103614.

[3] A. T. Chatfield and C. G. Reddick, “A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government,” Gov Inf Q, vol. 36, no. 2, pp. 346–357, Apr. 2019, DOI: 10.1016/j.giq.2018.09.007.

[4] M. Ficco and F. Palmieri, “Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios,” Journal of Systems Architecture, vol. 97, pp. 107–129, Aug. 2019, DOI: 10.1016/j.sysarc.2019.04.004.

[5] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” Computer Networks, vol. 169, Mar. 2020, DOI: 10.1016/j.comnet.2019.107094.

[6] K. Kimani, V. Oduol, and K. Langat, “Cyber security challenges for IoT-based smart grid networks,” International Journal of Critical Infrastructure Protection, vol. 25, pp. 36–49, Jun. 2019, DOI: 10.1016/j.ijcip.2019.01.001.

[7] R. O. Andrade and S. G. Yoo, “Cognitive security: A comprehensive study of cognitive science in cybersecurity,” Journal of Information Security and Applications, vol. 48, Oct. 2019, DOI: 10.1016/j.jisa.2019.06.008.

[8] J. Slupska and L. M. Tanczer, “Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things,” in The Emerald International Handbook of Technology-Facilitated Violence and Abuse, Emerald Group Publishing Ltd., 2021, pp. 663–688. DOI: 10.1108/978-1-83982-848-520211049.

[9] N. Z. Jhanjhi, M. Humayun, and S. N. Almuayqil, “Cyber security and privacy issues in industrial internet of things,” Computer Systems Science and Engineering, vol. 37, no. 3, pp. 361–380, 2021, DOI: 10.32604/CSSE.2021.015206.

[10] C. Chong, K. Lee, and G. Ahmed, “Improving Internet Privacy, Data Protection and Security Concerns.” [Online]. Available: https://journals.gaftim.com/index.php/ijtim/issue/view/1PublishedbyGAF-TIM,gaftim.com

[11] N. Moustafa, “New Generations of Internet of Things Datasets for Cybersecurity Applications based Machine Learning: TON_IoT Datasets.”

[12] P. Podder, S. Bharati, M. Rubaiyat, H. Mondal, P. K. Paul, and U. Kose, “Artificial Neural Network for Cybersecurity: A Comprehensive Review.”

[13] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, “A Survey of Cybersecurity Certification for the Internet of Things,” ACM Computing Surveys, vol. 53, no. 6. Association for Computing Machinery, Feb. 01, 2021. DOI: 10.1145/3410160.

[14] A. N. Lone, S. Mustajab, and M. Alam, “A comprehensive study on cybersecurity challenges and opportunities in the IoT world”, Security and Privacy, vol 6, no. 6, 2023. DOI: 10.1002/spy2.318

[15] A. Nazir and R. A. Khan, “A novel combinatorial optimization based feature selection method for network intrusion detection,” Comput Secur, vol. 102, Mar. 2021, DOI: 10.1016/j.cose.2020.102164.

[16] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, “A tree structure-based improved blockchain framework for a secure online bidding system,” Computer Security, vol. 102, Mar. 2021, DOI: 10.1016/j.cose.2020.102147.

[17] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garces, “A Comprehensive Study of the IoT Cybersecurity in Smart Cities,” IEEE Access, 2020, DOI: 10.1109/ACCESS.2020.3046442.

[18] T. Kulik, P. W. V. Tran-Jørgensen, J. Boudjadar, and C. Schultz, “A framework for threat-driven cyber security verification of IoT Systems,” in Proceedings - 2018 IEEE 11th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2018, Institute of Electrical and Electronics Engineers Inc., Jul.

2018, pp. 89–97. DOI: 10.1109/ICSTW.2018.00033.

[19] R. Paul, Institute of Electrical and Electronics Engineers. New York Section, Institute of Electrical and Electronics Engineers. Region 1, IEEE-USA, and Institute of Electrical and Electronics Engineers, 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) : 28th- 31st October 2020, New York, USA, virtual conference.

[20] I. Ashraf et al., "A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2677–2690, Feb. 2023, DOI: 10.1109/TITS.2022.3164678.

[21] J. He, T. Li, B. Li, X. Lan, Z. Li, and Y. Wang, "An immune-based risk assessment method for digital virtual assets," Comput Secur, vol. 102, Mar. 2021, DOI: 10.1016/j.cose.2020.102134.

[22] S. Chakrabarti et al., 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) : 7th-9th January, 2019, University of Nevada, Las Vegas, NV, USA.

[23] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," IEEE Internet Things J, vol. 7, no. 9, pp. 8852–8859, Sep. 2020, DOI: 10.1109/JIOT.2020.2996425.

[24] R. Da and M. Zekeriya Gündüz, "Analysis of Cyber-Attacks in IoT-based Critical Infrastructures."

[25] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," Applied Sciences (Switzerland), vol. 10, no. 12, Jun. 2020, DOI: 10.3390/APP10124102.

[26] A. Echeverría, C. Cevallos, I. Ortiz-Garces, and R. O. Andrade, "Cybersecurity model based on hardening for secure internet of things implementation," Applied Sciences (Switzerland), vol. 11, no. 7, Apr. 2021, DOI: 10.3390/app11073260.

[27] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure," Applied Sciences (Switzerland), vol. 11, no. 10, May 2021, DOI: 10.3390/app11104580.

[28] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the Internet of Things in Industrial Management," Applied Sciences (Switzerland), vol. 12, no. 3. MDPI, Feb. 01, 2022. DOI: 10.3390/app12031598.

[29] M. R. Al Asif, K. F. Hasan, M. Z. Islam, and R. Khondoker, "STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems," Jan. 2022, [Online]. Available: http://arxiv.org/abs/2201.09493

[30] F. Mohd Ali, N.A.M Yunus, N.N. Mohamed, M. Mat Daud, E. A. Sundararajan, "A Systematic Mapping: Exploring Internet of Everything Technologies and Innovations", Symmetry 2023, vol. 15, no. 11 https://doi.org/10.3390/sym15111964