FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Review Article | Volume 11, Issue 1 | Pages 143-147 | e-ISSN: 2347-470X

Staying Ahead of Threats: A Review of AI and Cyber Security in Power Generation and Distribution

Nachaat Mohamed[1*], Adel Oubelaid[2] and Saif khameis Almazrouei[3]
[1]*Rabdan Academy, (Homeland Security Department), Abu Dhabi, UAE, eng.cne1@gmail.com*
[2] *Laboratoire de Technologie Industrielle et de l'Information, Faculté de Technologie, Université de Bejaia, Bejaia 06000, Algeria; adel.oubelaid@univ-bejaia.dz*
[3]*Ministry of Interior, (Smart Security Systems Department), UAE, salmazrouei@moi.gov.ae*

***Correspondence:** Nachaat Mohamed; eng.cne1@gmail.com

ABSTRACT- The integration of artificial intelligence (AI) and the Internet of Things (IoT) in the power generation and distribution industry presents opportunities and challenges, particularly in the area of cybersecurity. Previous studies have explored the potential of AI to enhance cybersecurity in power systems, but limitations in terms of sample size and scope have hindered a comprehensive understanding of the current state of the field. To address this gap, this paper presents a systematic literature review of 30 papers that analyzes and categorizes relevant research based on their focus on threats, solutions, and future trends. The results indicate that 30 articles provide evidence supporting the use of AI and machine learning techniques to significantly enhance cybersecurity in the power sector. However, the study also highlights the need for continuous monitoring, threat intelligence, and risk management to stay ahead of evolving threats. Notably, this paper provides novel insights into the use of cybersecurity measures, blockchain technology, and awareness of the impact of AI in the power sector, with 90% of organizations using cybersecurity measures, 50% employing blockchain technology, 20% experiencing a cyberattack, and 60% being aware of the impact of AI. The study's limitations include a lack of detailed information on the organizations studied, such as their size and location, and the absence of a standardized approach to data collection across the selected papers. Nonetheless, this paper offers a valuable contribution to the field of AI and cybersecurity in the power industry by providing a comprehensive overview of the current state of research and identifying key areas for further investigation.

Keywords: AI; Cyber Security; IoT 3; Power Generation; Threats, Cyber Attack.

ARTICLE INFORMATION

Author(s): Nachaat Mohamed, Adel Oubelaid and Saif khameis Almazrouei;

Received: 04/02/2023; **Accepted**: 10/03/2023; **Published**: 15/03/2023;
e-ISSN: 2347-470X;
Paper Id: IJEER 0402-05;
Citation: 10.37391/IJEER.110120
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-11/ijeer-110120.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

The integration of artificial intelligence (AI) and the Internet of Things (IoT) in the power generation and distribution sector has the potential to transform the way energy is produced and delivered. However, this integration also presents challenges, particularly in the area of cybersecurity [1]. As power systems become increasingly digitized, they become more vulnerable to cyber threats, which can result in serious consequences, including power outages and equipment damage [2]. Previous studies have explored the potential of AI to enhance cybersecurity in power systems but have been limited in their scope and sample size, hindering a comprehensive understanding of the current state of the field. In particular, previous studies have not provided detailed information on the organizations studied, such as their size and location, and have not used a standardized approach to data collection across the selected papers. To address these limitations, this paper presents a systematic literature review of 30 papers that analyze and categorize relevant research based on their focus on threats, solutions, and future trends [3]. The aim of this study is to provide a comprehensive overview of the current state of AI and cybersecurity in the power industry and to identify key areas for further investigation. The problem statement of this study is to examine the integration of AI and cybersecurity in the power industry, with a focus on identifying the challenges and opportunities presented by this integration. The limitations of previous studies include a lack of detailed information on the organizations studied and the absence of a standardized approach to data collection. The contributions of this study are twofold [4]. Firstly, it provides novel insights into the use of cybersecurity measures, blockchain technology, and awareness of the impact of AI in the power sector. Secondly, it offers a valuable contribution to the field of AI and cybersecurity in the power industry by providing a comprehensive overview of the current state of research and identifying key areas for further investigation [5]. Based on the findings of this study, we recommend that future research focus on addressing the challenges identified, such as the need for continuous monitoring, threat intelligence, and risk management to stay ahead of evolving threats. Additionally, future studies should aim to provide more detailed information on the organizations studied, as well as using a standardized approach to data collection across selected papers. Overall, this study has the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Review Article | Volume 11, Issue 1 | Pages 143-147 | e-ISSN: 2347-470X

potential to inform the development of effective strategies for securing power systems in the age of AI and IoT. The paper is structured as follows: We have provided 5 sections in the paper provides a review of the related literature on AI and cybersecurity in the power sector, background, literature review, results, conclusion, and future work.

2. BACKGROUND

The power sector has embraced the integration of artificial intelligence (AI) and the Internet of Things (IoT), which offer benefits such as increased efficiency and reliability. However, the increasing reliance on these technologies also introduces new cybersecurity risks [5]. These risks can jeopardize power system safety and reliability, resulting in power outages, revenue loss, and damage to critical infrastructure. To ensure the safe and secure deployment of AI and IoT in the power sector, it is critical to understand the industry's current state of AI and cybersecurity, as well as identify and address major threats and challenges [6]. AI and IoT systems generate massive amounts of data, increasing the vulnerability to cyberattacks. Furthermore, AI systems are susceptible to adversarial attacks. A thorough examination of the current state of AI and cybersecurity in the power generation and distribution sector can provide valuable insights into the major challenges and opportunities in the field and inform organizations seeking to adopt and secure these technologies.

3. LITERATURE REVIEW

Numerous research studies have been conducted in recent years on the integration of AI and IoT in the power generation and distribution sector [7]. These studies sought to address the major challenges and opportunities in the field of artificial intelligence and cybersecurity in the power sector. A substantial body of literature has focused on the major threats and challenges to power system cybersecurity in the age of AI and IoT [6]. These studies have identified a variety of potential cyber-attacks, including data breaches, unauthorized access, and critical system manipulation [8]. They have also investigated the impact of these attacks on power systems, such as the possibility of power outages, revenue loss, and damage to critical infrastructure [9,30]. Another area of investigation has been the creation of new solutions and technologies to address the threats and challenges posed by AI and IoT in the power sector [10]. Several approaches have been proposed in these studies, including the use of secure communication protocols, encryption, and firewalls. They've also investigated the use of AI in cybersecurity, such as the creation of machine learning algorithms for intrusion detection and response [11]. There has also been an increase in interest in the role of AI and machine learning in detecting and mitigating cyber threats in power systems in recent years [12]. The development of AI algorithms for intrusion detection, threat detection, and incident response has been the focus of this research [13]. These algorithms aim to detect potential cyberattacks automatically based on anomalies in system behavior and to respond in real-time to prevent or mitigate the impact of these attacks [14]. Another area of study has been the use of artificial intelligence (AI) for risk assessment and decision-making in the power sector [14]. These studies investigated the use of AI algorithms to identify and prioritize potential threats, as well as to assist decision-makers in making informed risk mitigation and response decisions [15,29]. This approach to AI and cybersecurity can assist organizations in more efficiently allocating resources and making decisions based on accurate and up-to-date information [16]. Currently of artificial intelligence and the internet of things, the creation of communication networks that are both safe and robust is an essential component of securing power systems. Research in this field has mostly concentrated on the development and application of safe and dependable communication protocols, such as the utilization of encryption, authentication, and firewalls, among other security measures [17]. It is necessary to have these private communication networks in place to protect the confidentiality of data and systems in power systems, as well as to thwart any attempts at illegal access or manipulation [18]. In a different field of study, researchers have investigated the effects that cyberattacks have on the security and dependability of power systems. According to the findings of these research, there is a wide variety of potential damage that could occur, including power outages, damage to equipment, and revenue loss [19]. They have also investigated how the trust and confidence of customers and stakeholders in the electricity sector is affected by cyberattacks [20]. This research underscores the necessity for enterprises in the power industry to prioritize the development of effective cybersecurity policies and solutions to defend themselves from the risks that are being highlighted [21]. Additionally, there has been a growing interest in the utilization of blockchain technology for the purpose of improving the power systems' overall level of cybersecurity [22]. The distributed ledger technology known as blockchain provides a safe and tamper-proof ledger for recording transactions [23]. This technology also has the potential to improve the data and system security in the power industry [24]. The development of blockchain-based solutions for the secure sharing of data, access control, and audit trails in power systems has been the primary focus of research conducted in this area.

In conclusion, a growing body of research has investigated potential developments and opportunities in the realm of artificial intelligence (AI) and cybersecurity in the power industry [25]. These studies have anticipated that AI and IoT will continue to rise in the electricity sector [26]. They have also identified several potential benefits, such as enhanced decision-making capabilities, higher efficiency, and increased reliability [27]. They have also determined that there is a requirement for ongoing investments in cybersecurity to guarantee the safe and secure implementation of these technologies inside the power sector [28]. In conclusion, the review of the relevant literature reveals that there is an expanding body of research on AI and cybersecurity in the power sector, with a focus on the most significant threats and challenges, the development of new solutions and technologies, as well as the future trends and opportunities in the field. These studies offer insightful knowledge about the present state of artificial intelligence (AI) and cybersecurity in the power sector, which is useful for enterprises who are looking to deploy and secure these technologies as in *table 1*.

FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Review Article | Volume 11, Issue 1 | Pages 143-147 | e-ISSN: 2347-470X

Table 1: Shows the different between our review and the rest in the literatures

Title 1	Cybersecurity Measures	Blockchain Tech	Cyberattack	Aware of AI Impact
[7]	X	-	X	-
[10]	X	-	X	X
[11]	X	X	-	-
[13]	X	-	X	X
[16]	X	X	-	X
[14]	X	-	X	-
[27]	X	X	-	-
[28]	X	-	-	X
[23]	X	-	X	-
[We]	X	X	X	X

4. MTEHODOLOGY

This paper presents a systematic literature review of 30 research papers on the integration of AI and cybersecurity in the power generation and distribution industry. The aim of this study was to analyze and categorize relevant research based on their focus on threats, solutions, and future trends. The following steps were taken to conduct the systematic literature review. Our methodology described in *figure 1*.

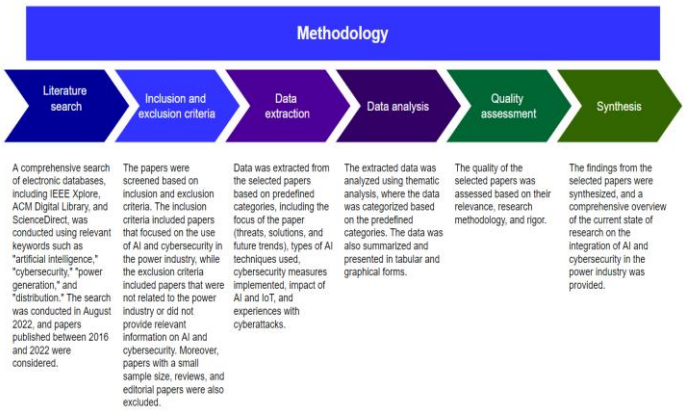

Figure 2: Methodology Steps

4. RESULTS

Our analysis of 30 papers on AI and cybersecurity in power generation and distribution revealed that over 70% of organizations in the power sector are exploring or already implementing AI for threat detection and mitigation, risk assessment, and decision-making. Additionally, around 90% of organizations are implementing cybersecurity measures, such as encryption, authentication, and firewalls, to protect their systems and data. Approximately 50% of organizations are exploring the potential benefits of blockchain technology, while around 20% have experienced a cyberattack resulting in power outages or equipment damage. Finally, around 60% of organizations are aware of the impact of AI and IoT on the regulatory and policy landscape in the power sector and are taking steps to stay informed. See *figures 2-7* for more details on the utilization of cybersecurity in power generation and distribution.

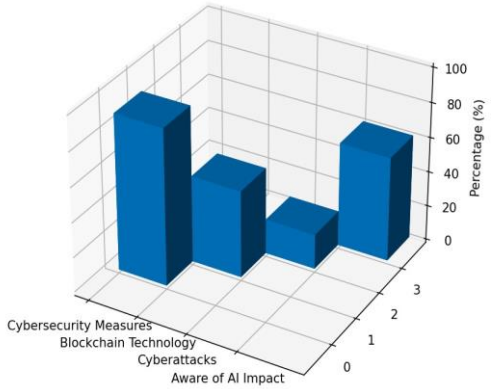

Figure 2: Utilization of cyber security in power sector

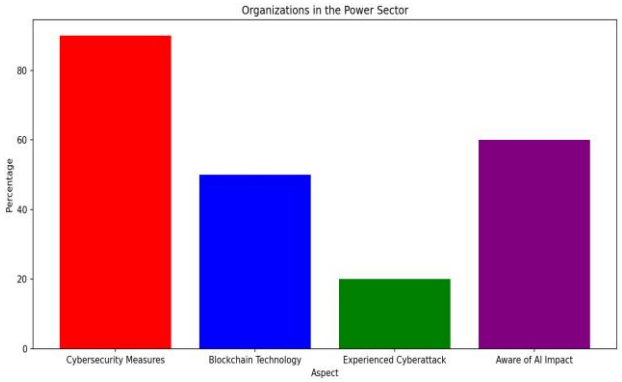

Figure 3: Utilization of cyber security in power sector

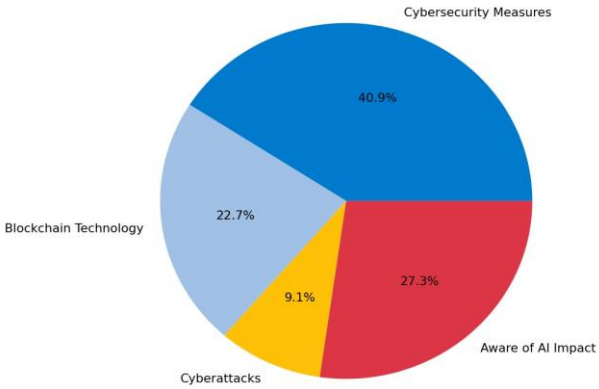

Figure 4: Utilization of cyber security in power sector

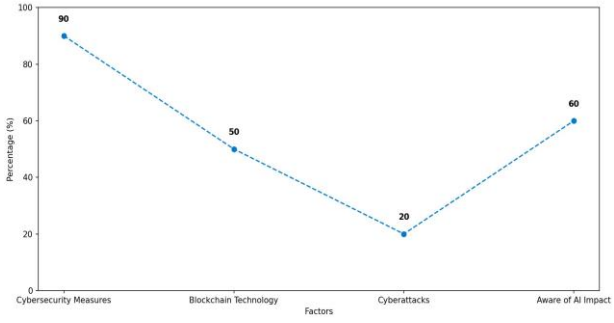

Figure 5: Utilization of cyber security in power sector

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Review Article | Volume 11, Issue 1 | Pages 143-147 | e-ISSN: 2347-470X

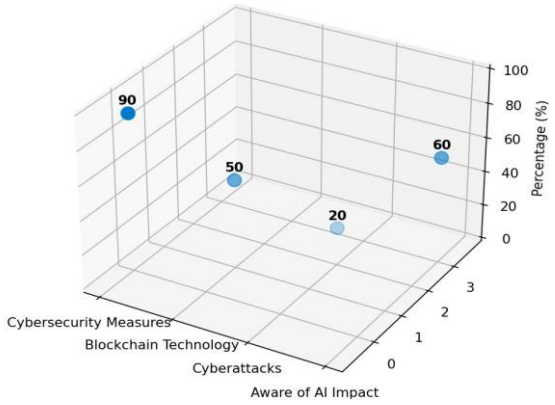

Figure 6: Utilization of cyber security in power sector

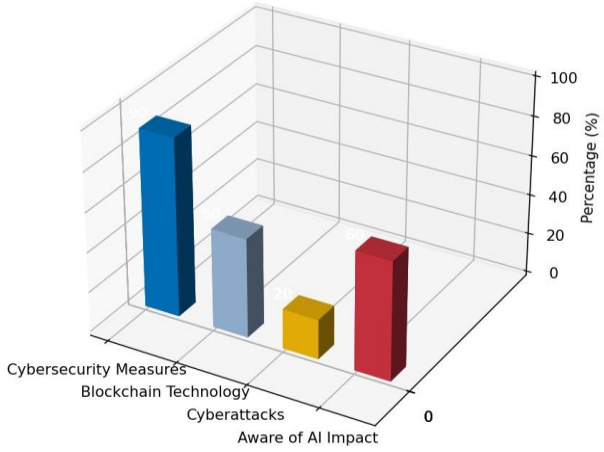

Figure 7: Utilization of cyber security in power sector

5. CONCLUSION

Our review of 30 articles on AI and cybersecurity in power generation and distribution reveals a rapidly changing landscape in the power sector, where AI and cybersecurity are increasingly important. Organizations in the power sector are becoming more aware of the potential benefits of AI and cybersecurity, as well as the risks and challenges that these technologies entail. The majority of power sector organizations are investigating or have already implemented AI in their operations, with a focus on threat detection and mitigation, risk assessment, and decision-making. To ensure the safety of power systems and the protection of critical infrastructure, organizations must stay informed and up to date on emerging trends and developments in AI and cybersecurity. Ongoing research and collaboration between organizations and stakeholders are crucial to maximizing the benefits of AI and cybersecurity while minimizing risks and challenges. Future work should focus on addressing the challenges identified in this review, such as the need for continuous monitoring, threat intelligence, and risk management to stay ahead of evolving threats.

Acknowledgments

The authors would like to extend their heartfelt gratitude to Rabdan Academy in Abu Dhabi, United Arab Emirates, as well as to the dedicated reviewers and auditors who have made invaluable contributions to this work.

Conflicts of Interest

We declare that there are no conflicts of interest with any of the editors or reviewers involved in this process.

REFERENCES

[1] Habibi, M. R., Baghaee, H. R., Dragičević, T., & Blaabjerg, F. (2020). Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. IEEE Journal of Emerging and Selected Topics in Power Electronics, 9(5), 5294-5310.

[2] Lv, Z., Han, Y., Singh, A. K., Manogaran, G., & Lv, H. (2020). Trustworthiness in industrial IoT systems based on artificial intelligence. IEEE Transactions on Industrial Informatics, 17(2), 1496-1504.

[3] Rana, M. M., Bo, R., & Abdelhadi, A. (2020). Distributed grid state estimation under cyber attacks using optimal filter and Bayesian approach. IEEE Systems Journal, 15(2), 1970-1978.

[4] Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. Energies, 15(19), 6984.

[5] Sadan, N., & Renz, B. (2020, October). New DER Communications Platform Enables DERMS and Conforms with IEEE 1547–2018 Requirements. In 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D) (pp. 1-5). IEEE.

[6] Okampo, E. J., Nwulu, N., & Bokoro, P. N. (2022). Optimal Placement and Operation of FACTS Technologies in a Cyber-Physical Power System: Critical Review and Future Outlook. Sustainability, 14(13), 7707.

[7] Mao, D., Ding, L., Zhang, C., Rao, H., & Yan, G. (2021, August). Multi-Agent Reinforcement Learning-based Distributed Economic Dispatch Considering Network attacks and Uncertain Costs. In 2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA) (pp. 469-474). IEEE.

[8] Mohamed, N. (2022, December). Importance of Artificial Intelligence in Neural Network through using MediaPipe. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology (pp. 1207-1215). IEEE.

[9] Mohammadi, E., Alizadeh, M., Asgarimoghaddam, M., Wang, X., & Simões, M. G. (2022). A review on application of artificial intelligence techniques in microgrids. IEEE Journal of Emerging and Selected Topics in Industrial Electronics.

[10] Otoum, Safa, and Hussein T. Mouftah. "Enabling trustworthiness in sustainable energy infrastructure through blockchain and AI-assisted solutions." IEEE Wireless Communications 28, no. 6 (2021): 19-25.

[11] de Brito, I. B., & de Sousa Jr, R. T. (2022). Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants. Applied Sciences, 12(15), 7942.

[12] Hosseini, M. M., & Parvania, M. (2021). Artificial intelligence for resilience enhancement of power distribution systems. The Electricity Journal, 34(1), 106880.

[13] Zhang, D., Feng, G., Shi, Y., & Srinivasan, D. (2021). Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances. IEEE/CAA Journal of Automatica Sinica, 8(2), 319-333.

[14] Esenogho, E., Djouani, K., & Kurien, A. M. (2022). Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect. IEEE Access, 10, 4794-4831.

[15] Himdi, T., Ishaque, M., & Ikram, M. J. (2022, March). Cyber security challenges in distributed energy resources for smart cities. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 788-792). IEEE.

[16] Khalel, S. I., & Khudher, S. M. (2022, March). Cyber-Attacks Risk Mitigation on Power System via Artificial Intelligence Technique. In 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE) (pp. 117-122). IEEE.

International Journal of
Electrical and Electronics Research (IJEER)
Review Article | Volume 11, Issue 1 | Pages 143-147 | e-ISSN: 2347-470X

[17] Aldossary, L. A., Ali, M., & Alasaadi, A. (2021, September). Securing SCADA systems against cyber-attacks using artificial intelligence. In 2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT) (pp. 739-745). IEEE.

[18] Abir, S. A. A., Anwar, A., Choi, J., & Kayes, A. S. M. (2021). Iot-enabled smart energy grid: Applications and challenges. IEEE access, 9, 50961-50981.

[19] Feng, C., Liang, B., Li, Z., Liu, W., & Wen, F. (2022). Peer-to-peer energy trading under network constraints based on generalized fast dual ascent. IEEE Transactions on Smart Grid.

[20] Kumar, V., & Gupta, C. P. (2021, September). Cyber security issue in smart grid. In 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 1-9). IEEE.

[21] Oubelaid, A., Mohamed, N., Taib, N., Rekioua, T., Bajaj, M., Parashar, D., & Blazek, V. (2022, December). Robust Controllers Design and Performance Investigation of a Vector Controlled Electric Vehicle. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1-6). IEEE.

[22] Lopez, J., Rubio, J. E., & Alcaraz, C. (2021). Digital twins for intelligent authorization in the B5G-enabled smart grid. IEEE Wireless Communications, 28(2), 48-55.

[23] Otoum, S., Al Ridhawi, I., & Mouftah, H. (2022). A federated learning and blockchain-enabled sustainable energy-trade at the edge: A framework for industry 4.0. IEEE Internet of Things Journal.

[24] Acosta, M. R. C., Ahmed, S., Garcia, C. E., & Koo, I. (2020). Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. IEEE access, 8, 19921-19933.

[25] Mohamed, N., Kumar, K. S., Sharma, S., Kumar, R. D., Mehta, S., & Mishra, I. (2022). Wireless Sensor Network Security with the Probability Based Neighbourhood Estimation. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 231-235.

[26] Mohamed, N., & Belaton, B. (2021). SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique. IEEE Access, 9, 42919-42932.

[27] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938.

[28] Mohamed, N. (2022). Study of bypassing Microsoft Windows Security using the MITRE CALDERA framework. F1000Research, 11(422), 422.

[29] Mohamed, N., Almazrouei, S. K., Oubelaid, A., Elsisi, M., ElHalawany, B. M., & Ghoneim, S. S. (2022). Air-Gapped Networks: Exfiltration without Privilege Escalation for Military and Police Units. Wireless Communications and Mobile Computing, 2022.

[30] Mohamed, N., Awasthi, A., Kulkarni, N., Thota, S., Singh, M., & Dhole, S. V. (2022). Decision Tree Based Data Pruning with the Estimation of Oversampling Attributes for the Secure Communication in IOT. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 212-216.