Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

A Review of IoT Networking Threats and Vulnerability Analysis, Identification, Detection, and Mitigation in Communication Systems

[1]Dr. Suma M.R., Ph.D. (VTU), [2]Sanjana Prasanna, M.S. (USA), [3]Dr. T. C. Manjunath

[1]Assistant Professor, Department of Electronics & Communication Engineering, Dayananda Sagar College of Engineering, Shavigemalleshwara Hills, Kumaraswamy Layout, Bangalore-560111, Karnataka

[2]Information Security Engineer, Bug Bounty Team - Application Security, eBay Inc, 2025 Hamilton Ave, San Jose, California, CA 95125, United States of America

[3]Ph.D. (IIT Bombay), Professor & Head, Electronics & Communication Engineering Department, Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bangalore-560111, Karnataka

Email : [1]sumamr-ec@dayanandasagar.edu [2]sanprasanna@ebay.com sanjanaprasanna088@gmail.com , [3]tcmanju@iitbombay.org

Abstract: The proliferation of Internet of Things (IoT) devices has been remarkable, driven by the ever-expanding landscape of IoT applications. These devices find widespread use across diverse industries, spanning from smart homes, smart apparel, and smart manufacturing to smart cars and smart medical care. Amid this wide array of applications, security stands out as a paramount concern, given the potential risks it poses to user privacy and property. In response to these challenges, numerous scholars and innovators have been actively developing applications and solutions aimed at mitigating the threats that loom over IoT networks. These endeavors seek to strike a delicate balance between safeguarding IoT systems and selecting the most effective measures to prevent and combat potential attacks. This article, therefore, embarks on a comprehensive review of IoT Networking Threats and Vulnerability Analysis, covering aspects of identification, detection, and mitigation. The review is structured into five categories to provide a comprehensive analysis. It begins by delving into security protocols designed to fortify IoT networks through the establishment of robust identity and trust mechanisms. Subsequently, the study scrutinizes the various vulnerabilities and attacks that pose threats to IoT networks. In the quest for enhanced security, the article explores the use of Intrusion Detection Mechanisms, harnessing the power of Machine Learning (ML) and Deep Learning (DL) techniques. These mechanisms serve as a shield against impending threats. Moreover, the article delves into the adoption of new technologies to bolster the thread mitigation process. To gauge the effectiveness of these methods, the performance evaluation encompasses an array of metrics, including accuracy, error rates, precision, execution time, encryption time, and decryption time. Two critical scenarios are considered in this evaluation: the detection of anomalies within IoT networks and the mitigation of threats within these networks. Among the various techniques explored, APSO-CNN emerges as a standout performer, exhibiting superior accuracy, minimal error rates, and high precision in the detection of attacks. Furthermore, ECC-CoAP is identified as the most efficient mitigation strategy, particularly excelling in execution time. In conclusion, this review endeavors to shed light on the multifaceted realm of IoT network security by addressing threats and vulnerabilities, harnessing advanced technologies, and assessing the performance of these methods. It serves as a valuable resource for the ongoing efforts to fortify IoT systems against potential risks and attacks.

Keywords: *IoT network, Threats and vulnerability analysis, Detection, Mitigation, ML DL*

1. Introduction

The concept of internet of things come from the integration of very simple as well as low power gadgets like, actuators, sensors and etc. Moreover, IoT described the network which comprises thousands of devices that is attained with an aid of modern technologies [1]. Due to the rapid evaluation of IoT that extend internet technologies to wireless sensor networks. IoT gadgets are primarily distinguished based on their limited power, memory, bandwidth resources and processor [2]. This is the key reason for typical security protocols and network operations cannot deployed in IoT ecosystem. The reality is that there are numerous benefits offered by delivering

embedded security to the devices by design, including cost reduction in the security architecture, increased reliability and enhanced overall performance [3]. Furthermore, IoT network is employed in numerous application due to the widely use of smart objects. For instance, IoT servers as smart agriculture, traffic monitoring and surveillance, health care domains and etc. The enormous amount of growth in automation which suffered from various security concerns in IoT ecosystem. There are different kinds of vulnerable attacks are always exist in internet and several common vulnerable are denial of service, worms, Trojans and port scans [4].

These security threats are happened due to the exponential rise in IoT gadgets and it is critical to address the IoT's privacy and security concerns. Therefore, the security of current IoT networks and devices is inadequate when employed in critical infrastructures [5]. IoT devices are vulnerable to anomalous activity due to software threats and delayed software updates. So, new and improved techniques must be developed for monitoring such activities and developing countermeasures to mitigate these concerns [6]. Various scholars focusing on interested on the detection and prevention of anomalies on internet of things. The use of machine learning techniques is one of the most popular contemporary approaches of detecting aberrant behavior in computer networks [7]. In contrast, as more connected devices are added to IoT networks, their amount of information flow increases. For preventing the attacks in IoT various security protocol like

The major objective of this paper is to review the overview of threat surfacing and mitigation strategies in IoT network by analyzing the effectiveness of various techniques in the mitigation and prevention of threads in IoT applications. There are more than fifty articles review are carried out for this review that is taken from different journals like, taylor francis, springer, elsevier, IEEE and wiley in last five years [2018-2022]. The number of articles considered for this analysis into five distinct categories which is display in Fig. 1.

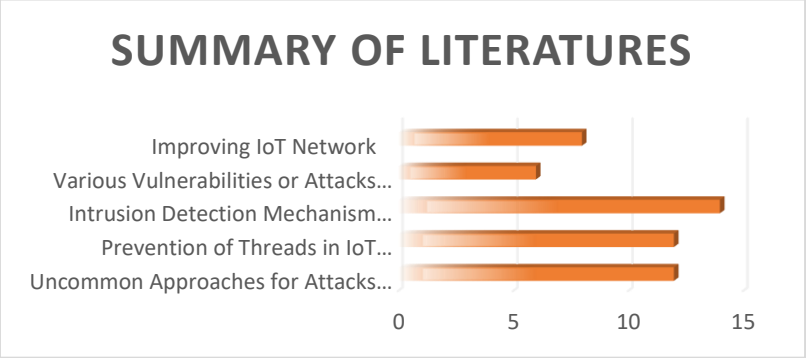

Fig 1: Summary of literatures considered for this analysis

The data packets are gathered for this detection process which comprises the data traffic behavioral as normal and malicious. After that, the gathered data was subjected into preprocessing with standard normal distribution with zero mean and unit variance. Figure 3 illustrates the malware attack process in IoT network.

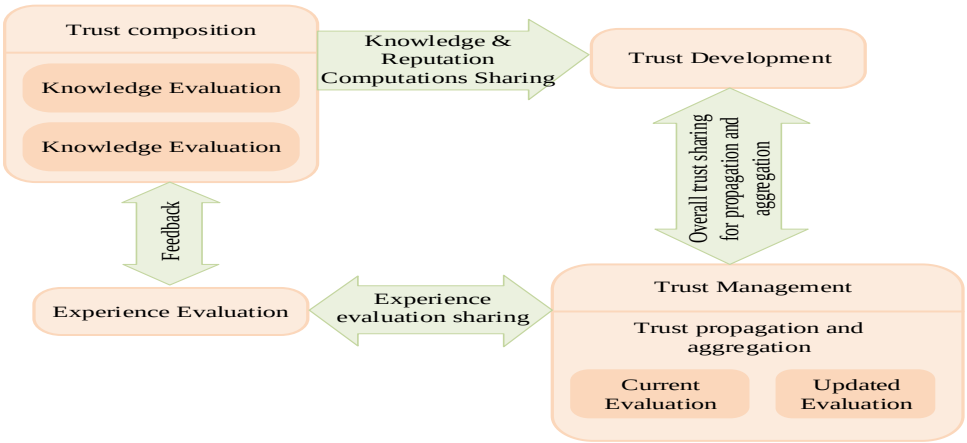

Fig 2: Trust evaluation process

The data packets are gathered for this detection process which comprises the data traffic behavioral as normal and malicious. After that, the gathered data was subjected into preprocessing with standard normal distribution with zero mean and unit variance. Figure 3 illustrates the malware attack process in IoT network.

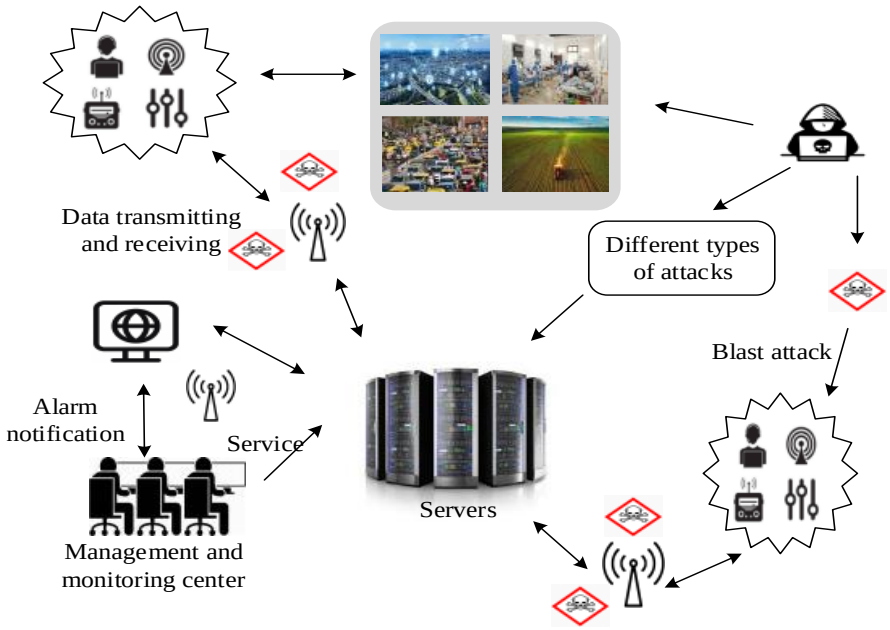

Fig 3: Malware attack process

2. Conclusions

In this paper reviewed various IoT Networking Threats and Vulnerability Analysis, Identification, Detection, and Mitigation techniques. This review included five categorizes for the thread analysis, detection and mitigation. Initially several security protocols are considered for improving IoT Network Through establishing Identity and Trust. Then various Vulnerabilities or Attacks Threatening the IoT Network are analyzed. Intrusion Detection Mechanism for Mitigating Treads Using ML and DL Techniques are provides and new technologies involved for the thread mitigation process are considered. Finally the performance of the considered methods are implemented with several performance metrics such as, accuracy, error, precision, execution time, encryption time and decryption time. APSO-CNN, DNN, DBN and BiLSTM are the techniques considered in the first scenario and ECC, CCN-ECC, ECC-MTTP and ECC-CoAP are the techniques considered in the second scenario. According to these both scenarios, APSO-CNN achieves better accuracy, error and precision values such as,96%, 97% and 4% in the detection of attacks. ECC-CoAP attained better execution time among the considered mitigation strategies. Based on this review this article suggest that new models are developed for both detection of malwares i.e. attacks and mitigation techniques which can ensure security in a better way.

References

[1] Foerster, J. R., Costa-Perez, X., & Prasad, R. V. (2020). Communications for iot: Connectivity and Networking. IEEE Internet of Things Magazine, 3(1), 6-7.

[2] Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. International Advanced Research Journal in Science, Engineering and Technology, 5(1), 41-44.

[3] Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Internet of Things Journal, 8(13), 10474-10498.

[4] Kuo, P. H., Mourad, A., & Ahn, J. (2018). Potential applicability of distributed ledger to wireless networking technologies. IEEE Wireless Communications, 25(4), 4-6.

[5] Qasim, H. H., Hamza, A. E., Ibrahim, H. H., Saeed, H. A., & Hamzah, M. I. (2020). Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IOT. International Journal of Electrical and Computer Engineering, 10(3), 2617.

[6] Chavhan, S., Gupta, D., Chandana, B. N., Khanna, A., & Rodrigues, J. J. (2019). IoT-based context-aware intelligent public transport system in a metropolitan area. IEEE Internet of Things Journal, 7(7), 6023-6034.

[7] Bello, O., & Zeadally, S. (2019). Toward efficient smartification of the Internet of Things (IoT) services. Future Generation Computer Systems, 92, 663-673.

[8] Gai, K., & Qiu, M. (2018). Optimal resource allocation using reinforcement learning for IoT content-centric services. Applied Soft Computing, 70, 12-21.

[9] Cecil, J., Albuhamood, S., Ramanathan, P., & Gupta, A. (2019). An Internet-of-Things (IoT) based cyber manufacturing framework for the assembly of microdevices. International Journal of Computer Integrated Manufacturing, 32(4-5), 430-440.

[10] Ooi, B. Y., & Shirmohammadi, S. (2020). The potential of IoT for instrumentation and measurement. IEEE Instrumentation & Measurement Magazine, 23(3), 21-26.

[11] Awan, K. A., Din, I. U., Almogren, A., Guizani, M., Altameem, A., & Jadoon, S. U. (2019). Robusttrust–a pro-privacy robust distributed trust management mechanism for internet of things. IEEE Access, 7, 62095-62106.

[12] Gebresilassie, S. K., Rafferty, J., Morrow, P., Chen, L., Abu-Tair, M., & Cui, Z. (2020, June). Distributed, secure, self-sovereign identity for iot devices. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE.

[13] Alshehri, M. D., & Hussain, F. K. (2019). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing, 101(7), 791-818.

[14] Marche, C., & Nitti, M. (2020). Trust-related attacks and their detection: A trust management model for the social IoT. IEEE Transactions on Network and Service Management, 18(3), 3297-3308.

[15] Sadique, K. M., Rahmani, R., & Johannesson, P. (2020). IMSC-EIoTD: identity management and secure communication for edge IoT devices. Sensors, 20(22), 6546.

[16] Simpson, S. V., & Nagarajan, G. (2021). An edge based trustworthy environment establishment for internet of things: an approach for smart cities. Wireless Networks, 1-17.

[17] Esposito, C., Tamburis, O., Su, X., & Choi, C. (2020). Robust decentralised trust management for the internet of things by using game theory. Information Processing & Management, 57(6), 102308.

[18] Azad, M. A., Bag, S., Hao, F., & Shalaginov, A. (2020). Decentralized self-enforcing trust management system for social Internet of Things. IEEE Internet of Things Journal, 7(4), 2690-2703.

[19] Nuss, M., Puchta, A., & Kunz, M. (2018, September). Towards blockchain-based identity and access management for internet of things in enterprises. In International Conference on Trust and Privacy in Digital Business (pp. 167-181). Springer, Cham.

[20] Alshehri, M. D., Hussain, F. K., & Hussain, O. K. (2018). Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT). Mobile networks and applications, 23(3), 419-431.

[21] Awan, K. A., Din, I. U., Zareei, M., Talha, M., Guizani, M., & Jadoon, S. U. (2019). Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things. Ieee Access, 7, 52191-52201.

[22] Qureshi, K. N., Iftikhar, A., Bhatti, S. N., Piccialli, F., Giampaolo, F., & Jeon, G. (2020). Trust management and evaluation for edge intelligence in the Internet of Things. Engineering Applications of Artificial Intelligence, 94, 103756.

[23] Kan, X., Fan, Y., Fang, Z., Cao, L., Xiong, N. N., Yang, D., & Li, X. (2021). A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network. Information Sciences, 568, 147-162.

[24] Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. International Journal of Parallel Programming, 48(2), 280-295.

[25] Gulzar, B., & Gupta, A. (2021). DAM: a theoretical framework for SensorSecurity in IoT applications. International Journal of Next-Generation Computing, 12(3).

[26] Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. Computers & Security, 78, 398-428.

[27] George, G., & Thampi, S. M. (2018). A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. IEEE Access, 6, 43586-43601.

[28] Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with layered approach to Internet of Things security. Measurement and Control, 52(5-6), 338-353.

[29] Anand, P., Singh, Y., Selwal, A., Singh, P. K., & Ghafoor, K. Z. (2022). IVQFIoT: An intelligent vulnerability quantification framework for scoring internet of things vulnerabilities. Expert Systems, 39(5), e12829.

[30] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems. IEEE Access, 8, 185938-185949.

[31] Kumar, P., Gupta, G. P., & Tripathi, R. (2021). Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks. Arabian Journal for Science and Engineering, 46(4), 3749-3778.

[32] Bhayo, J., Hameed, S., & Shah, S. A. (2020). An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT). IEEE Access, 8, 221612-221631.

[33] Sahu, A. K., Sharma, S., Tanveer, M., & Raja, R. (2021). Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 176, 146-154.

[34] Popoola, S. I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M., & Jogunola, O. (2021). Federated deep learning for zero-day botnet attack detection in IoT-edge devices. IEEE Internet of Things Journal, 9(5), 3930-3944.

[35] Abdollahi, A., & Fathi, M. (2020). An intrusion detection system on ping of death attacks in IoT networks. Wireless Personal Communications, 112(4), 2057-2070.

[36] Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning. IEEE Access, 8, 183678-183689.

[37] Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020). A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE Access, 8, 89337-89350.

[38] Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access, 8, 77396-77404.

[39] Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2020). CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. IEEE Internet of Things Journal, 8(5), 3242-3254.

[40] Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated-Learning-Based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal, 9(4), 2545-2554.

[41] Salim, M. M., Singh, S. K., & Park, J. H. (2021). Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks. Applied Soft Computing, 113, 107859.

[42] Majumder, S., Ray, S., Sadhukhan, D., Khan, M. K., & Dasgupta, M. (2021). ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. Wireless Personal Communications, 116(3), 1867-1896.

[43] Selvaraj, R., Kuthadi, V. M., Baskar, S., Shakeel, P. M., & Ranjan, A. (2021). Creating security modelling framework analysing in internet of things using EC-GSM-IoT. Arabian Journal for Science and Engineering, 1-13.

[44] Haseeb, K., Islam, N., Almogren, A., & Din, I. U. (2019). Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. Ieee Access, 7, 185496-185505.

[45] Rajesh, S., Paul, V., Menon, V. G., & Khosravi, M. R. (2019). A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. Symmetry, 11(2), 293.

[46] Pullmann, J., & Macko, D. (2019). A new planning-based collision-prevention mechanism in long-range IoT networks. IEEE Internet of Things Journal, 6(6), 9439-9446.
[47] Maktoubian, J., & Ansari, K. (2019). An IoT architecture for preventive maintenance of medical devices in healthcare organizations. Health and Technology, 9(3), 233-243.
[48] Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The journal of supercomputing, 76(9), 7081-7106.
[49] Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. Wireless Personal Communications, 112(3), 1947-1980.
[50] Adhikari, S., & Ray, S. (2019). A Lightweight and secure IoT communication framework in content-centric network using elliptic curve cryptography. In Recent trends in communication, computing, and electronics (pp. 207-216). Springer, Singapore.
[51] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.
[52] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12), 9463-9472.
[53] De Rango, F., Potrino, G., Tropea, M., & Fazio, P. (2020). Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive and Mobile Computing, 61, 101105.
[54] Sathya, M., Jeyaselvi, M., Krishnasamy, L., Hazzazi, M. M., Shukla, P. K., Shukla, P. K., & Nuagah, S. J. (2021). A novel, efficient, and secure anomaly detection technique using DWU-ODBN for IoT-enabled multimedia communication systems. Wireless Communications and Mobile Computing, 2021.
[55] Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S., & Shah, S. A. (2021). A time-efficient approach toward DDoS attack detection in IoT network using SDN. IEEE Internet of Things Journal, 9(5), 3612-3630.
[56] Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. N. (2021). PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Transactions on Network Science and Engineering, 8(3), 2326-2341.
[57] Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., & Rafiqul, I. (2022). Dependable Intrusion Detection System for IoT: A Deep Transfer Learning-based Approach. IEEE Transactions on Industrial Informatics.
[58] Gavel, S., Raghuvanshi, A. S., & Tiwari, S. (2021). Distributed intrusion detection scheme using dual-axis dimensionality reduction for Internet of things (IoT). The Journal of Supercomputing, 77(9), 10488-10511.
[59] Khan, I. A., Keshk, M., Pi, D., Khan, N., Hussain, Y., & Soliman, H. (2022). Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems. Ad Hoc Networks, 134, 102930.
[60] Srinivas, T., & Manivannan, S. S. (2021). Black Hole and Selective Forwarding Attack Detection and Prevention in IoT in Health Care Sector: Hybrid meta-heuristic-based shortest path routing. Journal of Ambient Intelligence and Smart Environments, 13(2), 133-156.
[61] Javadpour, A., Pinto, P., Ja'fari, F., & Zhang, W. (2022). DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments. Cluster Computing, 1-18.
[62] Dake, D. K., Gadze, J. D., Klogo, G. S., & Nunoo-Mensah, H. (2021). Multi-Agent Reinforcement Learning Framework in SDN-IoT for Transient Load Detection and Prevention. Technologies, 9(3), 44.
[63] Justindhas, Y., & Jeyanthi, P. (2022). Attack detection and prevention in IoT-SCADA networks using NK-classifier. Soft Computing, 1-13.