Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Utilizing Machine Learning to Detect Cyberattacks for Healthcare Systems

Alladi Karthik
dept. of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India

G. Teja Srinivas
dept. of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India

Sashank Desu
dept. of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India

Vamsikrishna Manne
dept. of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India

Narendra Kumar
dept. of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India

V. Jyothi
dept. of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India

***Abstract*—The healthcare industry handles sensitive and important data that must be protected from unauthorized access. Software-defined networks (SDNs) are extensively implemented in healthcare systems to assure optimal resource utilization, security, network administration, and control. Due to the sensitivity of patient data, SDNs are exposed to a wide spectrum of intrusions despite their many benefits. These attacks harm the overall network performance and can lead to network failures that pose a risk to human lives. Therefore, we aim to propose a machine learning-based cyber-attack detector for healthcare systems, by adapting a layer three (L3) learning switch application to collect normal and abnormal traffic, and then deploy ML model on the Ryu controller. Our findings are beneficial for enhancing the security of healthcare applications by mitigating the impact of cyberattacks. This work covers the testing of ML Model using a wide spectrum of both ML algorithms and attacks and provides a performance comparison for every pair of ML algorithms/attacks to illustrate the strengths and weaknesses of different algorithms against a specific attack. The model shows impressive performance, achieving a good F1-score on normal and attack classes, respectively, which implies a high level of reliability. Model also achieved 5,709,692 samples per second on throughput, which reflects a high-performance real-time system with respect to complexity.**

***Keywords*—Network resilience, network management, intrusion detection system (IDS), software defined networking, healthcare, machine learning.**

I. INTRODUCTION

In the last few years, SDNs have been extensively used in different fields, principally thanks to their advantages as reliable network technology that allows controlling and managing a network by disaggregating both control and data planes. In contrast to traditional networks, where the network simply has application awareness, the SDN architecture provides additional information about the condition of the entire network from the controller to its applications. Following the recent high-paced progress in information and communications technologies (ICT), healthcare establishments have begun to employ numerous infrastructure factors of the same types of off-the-shelf technologies, applications, and procedures employed by companies from other sectors. This situation was expected, due to the ability of networked or Internet-connected medical tools to increase the effectiveness of asset management, communications, and electronic health records, among other requirements, which reduces cost. Furthermore, the safety of systems and devices, together with user data confidentiality are the two factors that are primarily taken into account in the majority of information systems, since confidentiality and safety are crucial in a healthcare context due to the exacting requirements of the industry. Therefore, it is important that the current McAfee record highlighted that networked medical tools may reveal security gaps in the attempt by the medical industry to incorporate all the technical elements related to networked infrastructure and operational controls though expenses for hospital equipment are expected.

This research aims to enhance the security of healthcare systems by developing a machine learning-based cyber-attack detector implemented within software-defined networks (SDNs). Utilizing a layer three (L3) learning switch application to gather and analyse normal and abnormal network traffic, ML model will be deployed on the Ryu controller. The study includes extensive testing involving multiple machine learning algorithms and cyberattack scenarios, providing a comprehensive performance evaluation. Model demonstrates robust performance with a high F1-score for both normal and attack classes, indicating

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

reliability, while achieving a high throughput rate for real-time operations.

The healthcare industry faces a critical challenge in safeguarding sensitive patient data within software-defined networks (SDNs). Despite their advantages, SDNs are susceptible to a wide range of cyber intrusions, endangering network integrity and patient safety. To address this issue, this research aims to develop a machine learning-based cyber-attack detector for healthcare systems, leveraging a layer three (L3) learning switch application on the Ryu controller. This study seeks to comprehensively assess ML model performance against various machine learning algorithms and attack scenarios to bolster healthcare data security and network resilience.

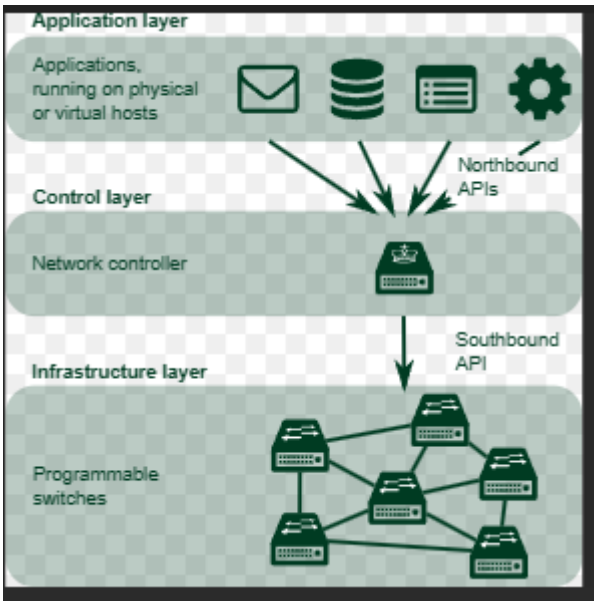

Fig 1.1 SDN Architecture

Besides the susceptibility of information in healthcare networks, the intricacy, quantity, and variety of tools, particularly networked medical devices (e.g., wireless pacemakers) creating this infrastructure, networks will be exposed to a wider variety of privacy risks and security [4], [5]. During the COVID-19 pandemic, the number of attacks has increased five times. Consequently, 90% of healthcare providers have been subjected to data violations [6]. As proven in recent ransomware incidents [7], the healthcare industry is particularly vulnerable to cyberattacks, which may be attributable to confidentiality breaches (e.g., leaked or comprised sensitive medical records), incidental errors, or deliberate and extensive interference (e.g., caused by flawed construction, use, or function). Researchers have recently begun to explore the prospect of using SDN in healthcare establishments due to the ability of SDN to abstract network policy from network devices [8].

II. LITERATURE SURVEY

Intelligent Edge Load Migration in SDN-IIoT for Smart Healthcare:

In present day era use of emerging technologies has given a rise to the healthcare issues. Combination of sensors, the industrial Internet of Things (IIoT), and big data analytics to enhance patient care can lower the healthcare costs. This will enable the patients with more secure, affordable, and rising medical services. Besides problems, such as resource-constrained IoT stuff, identity theft attacks, and malicious insiders, there is a need to address smart healthcare in big data and artificial intelligence using edge computing services. To fix these concerns, we are proposing a software-defined networking (SDN)-based security compliance structure for smart healthcare load migration systems. Toward this end, the use of SDN-IIoT technology for effective and real-time protection against security attacks is being explored by researchers and professionals. In our proposed framework, there are three domains and each domain has one virtual machine and various OpenFlow virtual switches. This scenario helps in migrating the heavily loaded domain healthcare data to the lightly loaded domain to make the domain balanced and prevent the migration from happening any type of security attacks. The RYU SDN controller is used to test the simulations and effectiveness of the performance obtained in the mininet after capturing the OpenFlow packets in Wireshark. Secure data management is achieved through the proposed framework and proposed algorithm gives 80% accurate for all the fetched healthcare data packets.

Studying the effect of internal DOS attacks over SDN controller during switch registration process:

Software defined networks bring many benefits with the centralization, application programmability interfaces and quick implementation of policies across whole network. Scalability and security are improved comparing with traditional networks, but centralized control have some drawbacks as it can be vulnerable for internal or external denial of service attacks. In this article, a comparison between two of the most used SDN controllers and the effect of internal denial of service attack towards the southbound interface during switch registration is presented. During the attack the CPU utilization and response time of the controller is collected and analysed.

Intruder Detection System Based Artificial Neural Network for Software Defined Network:

This paper shows the implementation of an Intruder Detection System (IDS) integrated into an Artificial Neural Network (ANN), called (Snort + RNA); as an option to mitigate the risks of active computer attacks towards a Software Defined Network (SDN). Which leverages the network hyperconverged of the data centre of the Faculty of Engineering of Applied Science (FICA) at the Technical University of the North. This proposal is tested under the PDCA model offered by the ISO/IEC 27001 standard and the processes provided by the hacker circle. The results show that Snort + RNA detects the anomalies that cause active-type attacks against the SDN, this is visible both in the alerts generated and in the record of the captured traffic, however, it is not possible to analyse all the packets it receives from attacks from DoS since some packages remain on hold or rejected. This shows that, although the system does not

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

evaluate all the packets that circulate on the network, that it takes care of the protection of the SDN, providing alerts when its third parties tried to violate it with attacks that caused an increase in network traffic.

Survey on Intrusion Detection System in IoT Network:

Internet of Things (IoT) has emerged as a powerful communication and networking system for smart and automation processing. With the increasing usage of the Internet of Things in numerous critical activities, it is essential to ensure that the communication among these devices is safe and secure. The biggest threat to safe and secure communication is from cyberattacks. Cyberattacks have evolved and become more complex, henceforth posing increased challenges to the data integrity, communication security, and confidentiality of the data. With its success in detecting security vulnerabilities in a communication network, intrusion detection systems are best integrated for securing IoT-based devices. But the integration of an intrusion detection system in an IoT-based network is a challenging task. This paper investigates the state of the art of IoT and intrusion detection system, the technology in use, and the technology challenges by reviewing notable existing works. A systematic literature review of 25 sources comprising 22 research papers and articles covering the threat models, intrusion detection system key challenges in IoT, Proposed models, and implementation of models, reviews, and evaluations are reviewed. The findings explore the needs and the best ways of integrating artificial intelligence-based intrusion detection systems in IoT networks for ensuring security and safety of communication.

Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks:

Internet of Things (IoT) devices work mainly in wireless mediums; requiring different Intrusion Detection System (IDS) kind of solutions to leverage 802.11 header information for intrusion detection. Wireless-specific traffic features with high information gain are primarily found in data link layers rather than application layers in wired networks. This survey investigates some of the complexities and challenges in deploying wireless IDS in terms of data collection methods, IDS techniques, IDS placement strategies, and traffic data analysis techniques. This paper's main finding highlights the lack of available network traces for training modern machine-learning models against IoT specific intrusions. Specifically, the Knowledge Discovery in Databases (KDD) Cup dataset is reviewed to highlight the design challenges of wireless intrusion detection based on current data attributes and proposed several guidelines to future-proof following traffic capture methods in the wireless network (WN). The paper starts with a review of various intrusion detection techniques, data collection methods and placement methods. The main goal of this paper is to study the design challenges of deploying intrusion detection system in a wireless environment. Intrusion detection system deployment in a wireless environment is not as straightforward as in the wired network environment due to the architectural complexities. So this paper reviews the traditional wired intrusion detection deployment methods and discusses how these techniques could be adopted into the wireless environment and also highlights the design challenges in the wireless environment. The main wireless environments to look into would be Wireless Sensor Networks (WSN), Mobile Ad Hoc Networks (MANET) and IoT as this are the future trends and a lot of attacks have been targeted into these networks. So it is very crucial to design an IDS specifically to target on the wireless networks.

III. METHODOLOGY

In literature They improved a similar IoT-enabled real-time heart monitoring system by making use of the cloud computing concept for obtaining sensor data, visualizing it with less cost and power, storing it at local storage, tracking it, and interacting with it remotely. They created a novel fog computing interface by combining Software Defined Networking with three sensing devices that retrieve health data. Analysis of medical data, bio signals, and sensor-generated data, signals, demonstrated the system's viability. Cost, power usage, and latency were also factored in to the analysis of the system's performance and compatibility. The wearable health system has been developed and tested, and the results show that it is ideal for relieving medical staff while providing round-the-clock, remote patient care.

Drawbacks:

1. The existing IoT-enabled heart monitoring system relies on cloud computing, which can be resource-intensive in terms of processing power and energy consumption.
2. The existing work might have limitations in terms of security measures, as it primarily focuses on real-time heart monitoring and remote patient care.
3. The existing system may raise concerns about patient data privacy, especially when transmitting sensitive medical information to the cloud.
4. The existing IoT-enabled system might have potential latency issues due to cloud-based communication.
5. The existing system might face challenges related to interoperability between different sensor devices and cloud platforms.

We aim to proposes a machine learning-based cyber-attack detector for healthcare systems, by adapting a layer three (L3) learning switch application to collect normal and abnormal traffic, and then deploy model on the Ryu controller. This work covers the testing of model using a wide spectrum of both ML algorithms such as KNN, Decision Tree (DT), random forest (RF), Naïve Bayes (NB), logistic regression (LR), adaptive boosting (AdaBoost), and XGBoost (XGB) for training on the datasets mentioned earlier and attacks, and provides a performance comparison for every pair of ML algorithms to illustrate the strengths and weaknesses of different algorithms against a specific attack. The effectiveness of the proposed system is demonstrated and tested.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Benefits:

- Our work prioritizes cybersecurity by specifically addressing the detection of cyber-attacks within healthcare systems. This focus on security helps safeguard sensitive patient data and critical healthcare infrastructure from potential breaches and threats.
- The machine learning-based cyber-attack detector is designed to identify a wide spectrum of cyber-attacks, providing a comprehensive defence against different types of threats, including intrusion attempts and unauthorized access.
- Our work leverages machine learning algorithms to efficiently detect cyber-attacks by adapting a layer three learning switch application. This approach optimizes the use of resources, making it well-suited for real-time detection without unnecessary strain on computational and energy resources.
- The focus on real-time cyber-attack detection allows our work to quickly identify and respond to threats as they occur. This can mitigate potential damage and minimize disruption within healthcare systems, which is essential for patient safety.

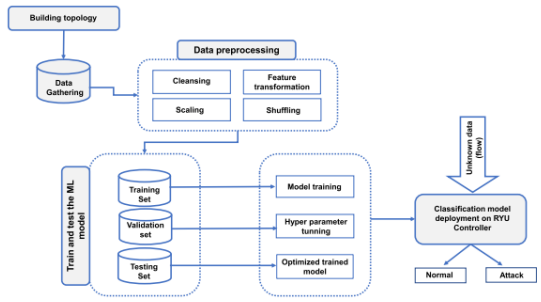

Fig 3.1 Proposed Architecture

Modules:

1. Data gathering: using this module we will load data into the system
2. Data Processing: Using the module, we will read data for processing.
3. Splitting data into train & test: using this module data will be divided into train & test
4. Model generation: Model building – KNN, Decision Tree, Random Forest, Naïve Bayes, Logistic Regression, AdaBoost, XGBoost. Algorithms accuracy calculated
5. User signup and login: Using this module will get registration and login
6. User input: Using this module will give input for prediction
7. Prediction: final predicted displayed
8. Extension: As an extension, we applied an ensemble method combining the predictions of multiple individual models to produce a more robust and accurate final prediction.

IV. IMPLEMENTATION

Algorithms:

KNN: The k-nearest neighbours algorithm, also known as KNN or k-NN, is a non-parametric, supervised learning classifier, which uses proximity to make classifications or predictions about the grouping of an individual data point.
DT: A decision tree is a non-parametric supervised learning algorithm, which is utilized for both classification and regression tasks. It has a hierarchical, tree structure, which consists of a root node, branches, internal nodes and leaf nodes.
RF: Random forest is a commonly-used machine learning algorithm trademarked by Leo Breiman and Adele Cutler, which combines the output of multiple decision trees to reach a single result. Its ease of use and flexibility have fuelled its adoption, as it handles both classification and regression problems.
NB: The Naïve Bayes classifier is a supervised machine learning algorithm, which is used for classification tasks, like text classification. It is also part of a family of generative learning algorithms, meaning that it seeks to model the distribution of inputs of a given class or category.
LR: Logistic regression is a supervised machine learning algorithm mainly used for classification tasks where the goal is to predict the probability that an instance of belonging to a given class or not. It is a kind of statistical algorithm, which analyse the relationship between a set of independent variables and the dependent binary variables. It is a powerful tool for decision-making.
AdaBoost: AdaBoost, also called Adaptive Boosting, is a technique in Machine Learning used as an Ensemble Method. The most common estimator used with AdaBoost is decision trees with one level which means Decision trees with only 1 split. These trees are also called Decision Stumps.
XGBoost: XGBoost is an optimized distributed gradient boosting library designed for efficient and scalable training of machine learning models. It is an ensemble learning method that combines the predictions of multiple weak models to produce a stronger prediction.

V. EXPERIMENTAL RESULTS

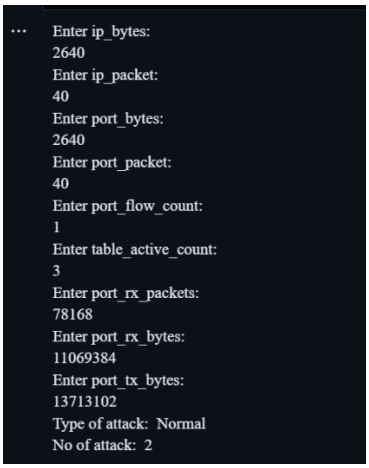

Fig 5.1 Predicting Attack (Normal Result)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

The image shows the prediction when the displayed values are entered. It predicts that there is nothing unusual happening in the network.

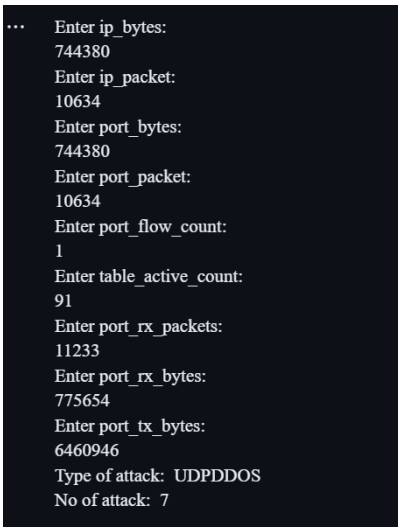

Fig 5.2 Predicting Attack (UDPDDOS Result)

The image shows the prediction when the displayed values are entered. It predicts that there is a Distributed Denial of Service (DDoS) attack happening in the network.

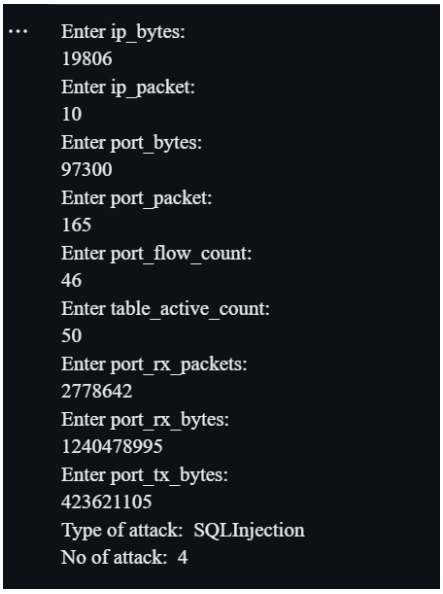

Fig 5.3 Predicting Attack (SQL Injection Result)

The image shows the prediction when the displayed values are entered. It predicts that there is a SQL Injection attack happening in the network.

VI. CONCLUSION

In this work, we presented a full investigation of the critical problem related to having a generalized method of detection of attacks and threats in the SDN environment in healthcare systems. We proposed a new detection model, which uses machine learning to achieve better and more efficient performance, with a wider spectrum that can cover many different attacks. To make sure that our model can perform required tasks, we contemplated different attack scenarios which match real-world scenarios, and then analysed the impact of developed attacks that can be identified by the model on different ML algorithms. It can be seen clearly that the model provides really good performance for most of the attacks with some of the ML algorithms used. Using RF for detection gives outstanding performance with all types of attacks, even that that have patterns that are hard to distinguish from normal traffic. Other techniques, like KNN and DT, provide really close performance, while some other tested ML algorithms struggled to detect some types of attacks.

VII. FUTURE ENHANCEMENTS

In the near future, we aim to extend this work in three different directions; first by using other ML techniques, then by considering more attacks/combinations of attacks in the datasets; and finally by testing the models on a more complex network model that may lead us to change the model's architecture.

REFERENCES

[1] M. Jarschel, T. Zinner, T. Hossfeld, P. Tran-Gia, and W. Kellerer, ''Interfaces, attributes, and use cases: A compass for SDN,'' IEEE Commun. Mag., vol. 52, no. 6, pp. 210–217, Jun. 2014.

[2] W. Meng, K.-K.-R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, ''Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks,'' IEEE Trans. Netw. Service Manage., vol. 15, no. 2, pp. 761–773, Jun. 2018.

[3] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scuffham, ''The Internet of Things: Impact and implications for health care delivery,'' J. Med. Internet Res., vol. 22, p. 11, Nov. 2020.

[4] (2022). Networked Medical Devices: Security and Privacy Threats—Sym antec—[PDF Document]. [Online]. Available: https://fdocuments. net/document/networked-medical-devices-security-and-privacy-threatssymantec.html

[5] P. A. Williams and A. J. Woodward, ''Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem,'' Med. Devices, Evidence Res., vol. 8, pp. 305–316, Jul. 2015.

[6] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, ''Cybersecurity risks in a pandemic,'' J. Med. Internet Res., vol. 22, no. 9, Sep. 2020, Art. no. e23692.

[7] N. Thamer and R. Alubady, ''A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,'' in Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), I. Babil, Ed., Apr. 2021, pp. 210–216.

[8] H. Babbar, S. Rani, and S. A. AlQahtani, ''Intelligent edge load migration in SDN-IIoT for smart healthcare,'' IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 8058–8064, Nov. 2022.

[9] R. Hasan, S. Zawoad, S. Noor, M. M. Haque, and D. Burke, ''How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis,'' in Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC), Jun. 2016, pp. 417–422.

[10] (Apr. 2015). 92% of Healthcare IT Admins Fear Insider Threats Thales. Accessed: Mar. 21, 2023. [Online]. Available: https://cpl.thalesgroup. com/about-us/newsroom/news-releases/92-healthcare-it-admins-fearinsider-threats

[11] D. Chaulagain, K. Pudashine, R. Paudyal, S. Mishra, and S. Shakya, ''OpenFlow-based dynamic traffic distribution in software-defined networks,'' in Mobile Computing and Sustainable Informatics. Singapore: Springer, Jul. 2021, pp. 259–272.

[12] R. Khondoker, A. Zaalouk, R. Marx, and K. Bayarou, ''Feature-based comparison and selection of software defined networking (SDN) controllers,'' in Proc. World Congr. Comput. Appl. Inf. Syst. (WCCAIS), Jan. 2014, pp. 1–7.

[13] T. Mekki, I. Jabri, A. Rachedi, and L. Chaari, ''Software-defined networking in vehicular networks: A survey,'' Trans. Emerg. Telecommun. Technol., vol. 33, no. 10, pp. 1–10, Apr. 2021, doi: 10.1002/ett.4265.

[14] Z. Ghaffar, A. Alshahrani, M. Fayaz, A. M. Alghamdi, and J. Gwak, ''A topical review on machine learning, software defined networking,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Internet of Things applications: Research limitations and challenges,'' Electronics, vol. 10, no. 8, p. 880, Apr. 2021, doi: 10.3390/electronics10080880.

[15] C.-S. Li and W. Liao, ''Software defined networks [guest editorial],'' IEEE Commun. Mag., vol. 51, no. 2, p. 113, Feb. 2013.

[16] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, ''Software defined networks-based smart grid communication: A comprehensive survey,'' IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.

[17] L. F. Eliyan and R. Di Pietro, ''DoS and DDoS attacks in software defined networks: A survey of existing solutions and research challenges,'' Future Gener. Comput. Syst., vol. 122, pp. 149–171, Sep. 2021, doi: 10.1016/j.future.2021.03.011.

[18] K. Benton, L. J. Camp, and C. Small, ''OpenFlow vulnerability assessment,'' in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw., 2013, pp. 151–152, doi: 10.1145/2491185.2491222.

[19] B. Mladenov and G. Iliev, ''Studying the effect of internal DOS attacks over SDN controller during switch registration process,'' in Proc. Int. Symp. Netw., Comput. Commun. (ISNCC), Jul. 2022, pp. 1–4.

[20] H. Domínguez-Limaico, W. N. Quilca, M. Zambrano, F. Cuzme-Rodríguez, and E. Maya-Olalla, ''Intruder detection system based artificial neural network for software defined network,'' in Proc. Int. Conf. Technol. Res. Cham, Switzerland: Springer, Aug. 2022, pp. 315–328.

[21] S. A. Mehdi and S. Z. Hussain, ''Survey on intrusion detection system in IoT network,'' in Proc. Int. Conf. Innov. Comput. Commun. Singapore: Springer, Sep. 2022, pp. 721–732.

[22] V. Ponnusamy, M. Humayun, N. Z. Jhanjhi, A. Yichiet, and M. F. Almufareh, ''Intrusion detection systems in Internet of Things and mobile ad-hoc networks,'' Comput. Syst. Sci. Eng., vol. 40, no. 3, pp. 1199–1215, 2022, doi: 10.32604/csse.2022.018518.

[23] K. Malasri and L. Wang, ''Securing wireless implantable devices for healthcare: Ideas and challenges,'' IEEE Commun. Mag., vol. 47, no. 7, pp. 74–80, Jul. 2009.

[24] D. Yin, L. Zhang, and K. Yang, ''A DDoS attack detection and mitigation with software-defined Internet of Things framework,'' IEEE Access, vol. 6, pp. 24694–24705, 2018.

[25] R. Wang, Z. Jia, and L. Ju, ''An entropy-based distributed DDoS detection mechanism in software-defined networking,'' in Proc. IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug. 2015, pp. 310–317