2024 International Conference on Smart Systems for Electrical, Electronics, Communication and Computer Engineering (ICSSEECC) | 979-8-3503-7817-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICSSEECC61126.2024.10649533

Intrusion Detection in SDN using Ensemble Learning Technique

Bharath S
Department of CSE
PSG Institute of Technology and Applied Research
Tamilnadu, India
bharathsenthilkumar1980@gmail.com

Dhanashree D
Department of CSE
PSG Institute of Technology and Applied Research
Tamilnadu, India
dhanashreesekar2003@gmail.com

Nandika M
Department of CSE
PSG Institute of Technology and Applied Research
Tamilnadu, India
nandikanair22@gmail.com

A. Sunitha Nandhini
Department of CSE
PSG Institute of Technology and Applied Research
Tamilnadu, India
asn@psgitech.ac.in

***Abstract*— Software Defined Networks (SDN) have provided an advancement in terms of flexibility and scalability in recent times in networking. SDN paves the way for a centralized monitoring system. This centralisation has also led to increased security threats which has made the network monitors to focus on the improved security of the systems with utmost priority. The proposed methodology simulates an SDN environment using two Virtual Machines with Mininet and RYU controller. A traffic is generated to create a false attack and the detection is visualized using this environment. Machine Learning techniques provide an efficient and logical way to implement a solution. Feature Selection is an important aspect and Recursive Feature Elimination with Cross-Validation (RFECV) is used to get the final subset of features based on the importance of their significance. Synthetic Minority Oversampling Technique (SMOTE) is used in data preprocessing to handle the data imbalance. Models like XGBoost, Random Forest and Convolutional Neural Networks are used. Using ensemble technique, a meta-learner is constructed using Random Forest, XGBoost and AdaBoost to use the strengths of the standalone models and create the best version of the classifier that shows 98.8% accuracy. Accuracy, F1 score, Precision and Recall are used to evaluate and compare the performance of the models. The generalization of the constructed meta-learner is tested on another dataset and the results show good accuracy. This model can be integrated into real-world networks to enhance security by accurate intrusion detection.**

Keywords*— *Intrusion, Software Defined Networks, Ensemble technique, Controller.

I. INTRODUCTION

Software Defined Networks' behaviour is where the entire network is governed by a centralized control plane, in contrast to traditional networking techniques where network devices are individually configured and havefixed functionality. SDN's centralized control, which offers a comprehensive picture of network activity and makes uniform policy enforcement throughout the infrastructure possible, is one of its main benefits.

Owing to the different operating features and architectural differences from traditional changing networks, intrusion detection in Software Defined Networking settings poses special challenges. Being visible and monitored is a major obstacle. Intrusion detection systems may have blind spots since network traffic in SDN frequently passes through a centralized controller, which simplifies management. In highlycentralized setups like this, traditional intrusion detection systems could have trouble keeping an eye on and analyzing traffic, which could result in decreased visibilityand security vulnerabilities. Detecting intrusions is more difficult with SDN's dynamic structure. It might be confusing for intrusion detection systems to be able to effectively detect anomalies when network resources are dynamically reconfigured in response to fluctuating demands. Network topology and traffic patterns can change quickly, overwhelming IDS systems and increasing false positives or negatives.

In the field of cybersecurity, it is essential for stoppingmany types of cyberattacks that are made possible by botnets, including malware distribution, phishing campaigns, and distributed denial-of-service attacks. Intrusion detection approaches encompass host-based and network-based methods [9]. The analysis of network traffic is the foundation of network-based methods. One technique for detection is traffic analysis, in which anomalous patterns such as an abrupt increase in outboundconnections or a large number of similar requests point topossible botnet activity. While anomaly detection finds departures from predetermined baselines, signature-baseddetection generates patterns that represent known botnet behaviours. Host-based strategies focus on the actions of specific devices. Flow-based methods focus on flow analysis, looking at how devices communicate with one another.

Machine learning models hold paramount significance in the realm of cybersecurity related threat detection, offering unique advantages that contribute to the ongoing battle against the dynamic cyber threats. As cybercriminals continuously modify their strategies to avoid detection, these models can dynamically adjust to patterns and behaviours, ensuring the efficacy of the detection system over time. Real-time analysis is another notable advantage,

ensemble model stacks the results of multiple models and produces as aggregated output, it includes advantages of all the base learners, performing better than standalone models.

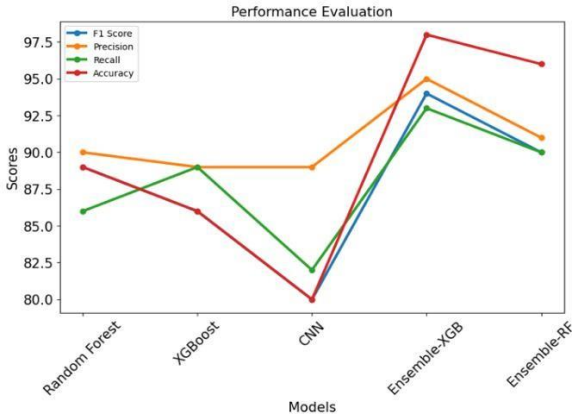

Fig. 6. Comparison for F1 score, Precision, Recall, Accuracyof the models.

Figure 6 visually illustrates the performance of the five implemented models based on evaluation metrics such as accuracy, precision, recall and F1 score.

The proposed ensemble model with an accuracy of 98.8% outperforms the DNN models proposed by Chaganti, et al.,[11] that has an accuracy range of 94% to 96% and also the system proposed by Alzahrani et al.,[12] that has an accuracy of 96.55%.

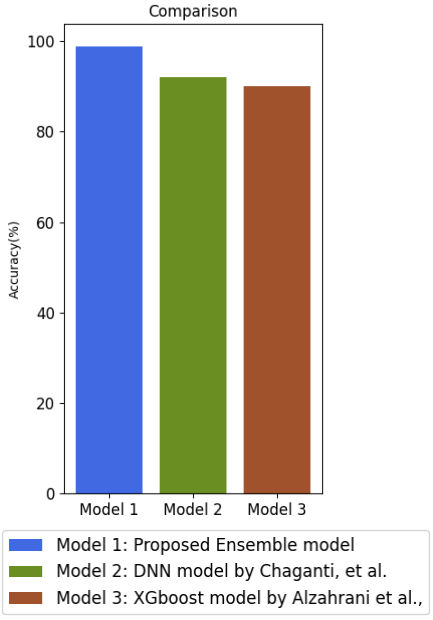

Fig. 7. Comparison of accuracy with existing systems

Figure 7. illustrates the comparison of the proposed systemusing Ensemble model with previously existing systems for intrusion detection in SDN.

V. CONCLUSION

Through The proposed intrusion detection system using ensemble technique has been a dedicated effort in enhancing cybersecurity measures to safeguard software defined networks against malicious botnet activities. The primary goal has been to develop a system capable of effectively identifying and neutralizing these threats, thus ensuring the integrity and security of digital infrastructures. Through extensive research and experimentation, a sophisticated solution has been designed that utilizes ensemble learning technique and data analysis techniques like SMOTE and RFECV to differentiate between normal network traffic and malicious behaviour. By rigorously testing the system across various datasets and scenarios, optimal results have been observed, indicating its ability to accurately detect intrusions in the traffic with high accuracy and relatively low false positive rates to existing systems. The method underscores the importance of proactive cybersecurity measures in combating evolving cyber threats and protecting sensitive data from unauthorized access. This also serves as a testament to the power of technology in fortifying digital ecosystems against malicious adversaries.

REFERENCES

[1] Rashid, Mamunur, Joarder Kamruzzaman, Tasadduq Imam, Santoso Wibowo, and Steven Gordon. "A tree-based stacking ensemble technique with feature selection for network intrusion detection." In Applied Intelligence vol. 52, no. 9, pp. 9768-9781, 2022.

[2] Mishra, Amit Kumar, and Shweta Paliwal. "Mitigating cyber threats through integration of feature selection and stacking ensemble learning: the LGBM and random forest intrusion detection perspective." In Cluster Computing vol. 26, no. 4, pp. 2339-2350, 2023.

[3] Mohammed, Badiea Abdulkarem, and Zeyad Ghaleb Al-Mekhlafi. "Optimized Stacking Ensemble Model to Detect Phishing Websites." In Advances in Cyber Security: Third International Conference, Penang, Malaysia, pp. 379-388, 2021.

[4] Alghanam, Orieb Abu, Wesam Almobaideen, Maha Saadeh, and Omar Adwan. "An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning." In Expert Systems with Applications vol. 213, p. 118745, 2023.

[5] Tang, Tuan Anh, Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, Mounir Ghogho, and Fadi El Moussa. "DeepIDS: Deep learning approach for intrusion detection in software defined networking." In Electronics vol 9, no. 9, p. 1533, 2020.

[6] Rao, Routhu Srinivasa, and Alwyn Roshan Pais. "Detection of phishing websites using an efficient feature-based machine learning framework." In Neural Computing and applications vol. 31, pp. 3851-3873, 2019.

[7] Ren, Ye, Le Zhang, and Ponnuthurai N. Suganthan. "Ensemble classification and regression-recent developments, applications and future directions." In IEEE Computational intelligence magazine vol. 11, no. 1, pp. 41-53, 2016.

[8] Sultana, Nasrin, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. "Survey on SDN based network intrusion detection system using machine learning approaches." In Peer-to-Peer Networking and Applications vol. 12, no. 2, pp. 493-501, 2019.

[9] Almutairi, Suzan, Saoucene Mahfoudh, Sultan Almutairi, and Jalal S. Alowibdi. "Hybrid botnet detection based on host and network analysis." In Journal of Computer Networks and Communications vol. 2020, pp. 1-16, 2020.

[10] Shabudin, Shafaizal, Nor Samsiah Sani, Khairul Akram Zainal Ariffin, and Mohd Aliff. "Feature selection for phishing website classification." In International Journal of Advanced Computer Science and Applications vol. 11, no. 4, 2020.

[11] Chaganti, Rajasekhar, Wael Suliman, Vinayakumar Ravi, and Amit Dua. "Deep learning approach for SDN-enabled intrusion detection system in IoT networks." In Information vol. 14, no. 1, p. 41, 2023.

[12] Alzahrani, Abdulsalam O., and Mohammed JF Alenazi. "Designing a network intrusion detection system based on machine learning for software defined networks." In Future Internet vol. 13, no. 5, p. 111, 2021.

[13] Sebopelo, Rodney, Bassey Isong, Naison Gasela, and Adnan M. Abu-Mahfouz. "A review of intrusion detection techniques in the SDN environment." In 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), pp. 1-9. IEEE, 2021.

[14] Adamou Djergou, Abass, Yassine Maleh, and Soufyane Mounir. "Machine learning techniques for intrusion detection in SDN: A survey." In Advances in Information, Communication and Cybersecurity: Proceedings of ICI2C'21, pp. 460-473, 2022.

[15] Sarica, Alper Kaan, and Pelin Angin. "A novel sdn dataset for intrusion detection in iot networks." In 2020 16th International Conference on Network and Service Management (CNSM), pp. 1-5, 2020.