Proceedings of the 7th International Conference on Intelligent Sustainable Systems (ICISS-2025)
IEEE Xplore Part Number: CFP25M19-ART; ISBN: 979-8-3315-2243-8

Development of a CNN Model for Anomaly Detection in SDN Environments

Monisha.T.,
Department of CSE,
Jeppiaar Engineering College,
Semmencherry Chennai , Tamil Nadu - 600 119
mailonlyformonisha@gmail.com

S. Kalarani,
Department: of CSE,
PSG Institute of Technology and Applied Research
Coimbatore, Tamil Nadu - 641062
kalarani@psgitech.ac.in

2025 7th International Conference on Intelligent Sustainable Systems (ICISS) | 979-8-3315-2243-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICISS63372.2025.11076439

Abstract—**This work develops a Convolutional Neural Network (CNN) for** anomaly **detection (AD) in Software-Defined Networking (SDN) environments, utilizing six flow dimensions: bits per second, packets per second, source and destination IP entropy, and source and destination port entropy. The model is designed to identify network anomalies, including DDoS and portscan attacks, by analyzing network traffic and predicting future destination IP entropy. Two decision threshold strategies were evaluated to balance detection accuracy and system reliability. The first method aimed at maximizing the F1 score but resulted in a high number of false positives (15%) and false negatives (18%), decreasing the model's reliability due to frequent false alarms. The second method focused on minimizing false positives, reducing them to near zero but at the cost of higher false negatives (25%) and delayed anomaly detection by over one second in some cases.**

Keywords—Software-Defined Networking, Convolutional Neural Network, Anomaly detection, Attack scenarios

I. INTRODUCTION

The growing reliance on Software-Defined Networking (SDN) in modern communication systems underscores the critical need for robust and adaptive anomaly detection (AD) mechanisms. SDN, with its centralized control and dynamic reconfiguration capabilities, enhances network flexibility and efficiency but also exposes networks to sophisticated cyberattacks, including Distributed Denial of Service (DDoS) and port scan attacks. Anomalies in SDN traffic, if undetected, can compromise network performance, availability, and security [1-4].

In this context, the use of machine learning, particularly convolutional neural networks (CNNs), offers a promising avenue for enhancing AD. CNNs are known for their ability to learn hierarchical features from complex datasets, making them suitable for analyzing network traffic patterns. This work focuses on developing a CNN-based model that detects anomalies in SDN networks by analyzing six flow dimensions: bits per second, packets per second, source IP entropy, source port entropy, destination IP entropy, and destination port entropy. These dimensions provide a comprehensive view of network behavior, enabling the detection of both subtle and significant anomalies [5-8].

Two decision threshold selection methodologies were explored to optimize detection accuracy and reliability. The first approach aimed to balance false positives and false negatives, resulting in a low F1 score due to the high rates of both errors. This balance, while statistically meaningful, rendered the system impractical due to its susceptibility to false alarms [9].

The second methodology prioritized minimizing false positives, even at the expense of increased false negatives. This strategy proved effective in reducing false alarms to nearly zero, ensuring the reliability of anomaly alerts. However, this approach introduces latency in AD, as multiple false negatives may precede a true positive. While this delay is tolerable for certain attacks like DDoS, where anomalies are consistently detected during the attack's progression, it poses risks for less impactful anomalies that might evade detection altogether [10].

Despite its limitations, the proposed CNN model demonstrated a high detection rate for DDoS and port scan attacks. However, its specificity to these attack types may limit its generalizability to novel or less common attack patterns. Addressing these challenges is critical for advancing AD in SDN networks, ensuring resilience against an evolving landscape of cyber threats. This study contributes to the development of efficient and reliable network defense mechanisms, balancing detection accuracy, latency, and adaptability.

II. LITERATURE REVIEW

Sahoo et al. (2020), which integrates genetic algorithms for improved classification accuracy and adaptability in detecting Distributed Denial-of-Service (DDoS) attacks.

Similarly, Ethilu, Sathappan, and Rodrigues (2022) developed a deep learning-based framework using Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to identify malicious SDN switches, thereby improving system efficiency and reducing vulnerabilities in the centralized control plane.

Abdullahi et al. (2022) conducted a systematic literature review assessing artificial intelligence-based intrusion detection in IoT environments, highlighting the effectiveness of machine learning, deep learning, and reinforcement learning models in identifying threats like botnets, ransomware, and data exfiltration. However, their study also noted computational limitations that pose deployment challenges in resource-constrained IoT environments.

dataset, generated with Mininet, included network traffic from six switches and 60 hosts over four days, with normal traffic on day one and DDoS/port scan attacks on subsequent days. The data was normalized for training and visualization. The model aimed to predict destination IP entropy, a key metric for anomaly detection, and set a classification threshold by optimizing the F1 score.

Two decision threshold strategies were explored. The first, optimizing the F1 score, set the threshold at 0.046, achieving a balanced detection rate but with high false positives and negatives. The second strategy, predicting attack probability, set the threshold at 72%, reducing false positives and improving detection accuracy. While the model showed potential for real-time anomaly detection, further refinement is needed, especially in balancing false positives and negatives. Future work could focus on hyperparameter optimization, alternative models, and broader attack scenarios.

This study aligns with recent research in SDN anomaly detection using CNNs, similar to works by Liu et al. (2023) and Zhang et al. (2022), who also applied deep learning for DDoS and port scan detection. The use of a Mininet-based dataset with six flow dimensions for feature extraction is consistent with current practices in network traffic simulation. However, the decision threshold strategies used here, focusing on F1 score optimization and minimizing false positives, differ from other studies that prioritize detection speed or balanced detection rates. While the model achieved a 93% detection rate, it highlights the need for further research on improving generalizability to novel attack scenarios, as seen in works like Sharma et al. (2023), which explored hyperparameter optimization and alternative models for better adaptability in real-time AD.

In this system, a Convolutional Neural Network (CNN) is chosen for anomaly detection due to its ability to capture spatial features in data, making it suitable for time-series data like network traffic. The CNN processes network traffic features (e.g., bits per second, source IP entropy) to identify temporal patterns and detect deviations such as DDoS or port scanning attacks. The system follows a structured approach, starting with pre-processing where Shannon entropy is computed to detect changes in network behavior. The network is trained on normal traffic data to predict future traffic values, and anomalies are detected by comparing predicted values with actual observations. If the error exceeds a predefined threshold, the event is flagged as anomalous. The threshold is selected based on a balance between accuracy and minimizing false positives, ensuring effective real-time detection of network anomalies. The role of Software-Defined Networking (SDN) is crucial in enhancing the system's flexibility by allowing real-time adjustments to network configurations based on detected anomalies. Reliability is achieved through robust training and validation processes, which minimize errors in the detection process. False alarms are reduced by fine-tuning the decision thresholds, balancing sensitivity and specificity to better recognize attack patterns while filtering out normal traffic fluctuations. This ensures a more accurate and responsive anomaly detection system.

VI. CONCLUSION

In the work, a convolutional neural network was The developed model detects anomalies in SDN networks using six flow dimensions and explores two threshold selection methods. The first method, focused on maximizing the F1 score, resulted in high false positives and false negatives, leading to an unreliable system due to excessive false alarms. The second method, designed to minimize false positives, significantly reduced false alarms but increased false negatives. This approach is effective for detecting DDoS attacks, as anomalies are detected at various points, but the downside is the potential delay in alerting, which could allow damage before detection. The model performs well for DDoS and portscan attacks but may struggle with detecting different types of attacks. The research faces limitations in generalization, as the CNN model is tailored to specific attack types, limiting its detection of novel threats. Detection delays occur when minimizing false positives, and balancing false positives with false negatives affects reliability. The model's computational demands may impact network performance, and scalability in large SDN environments is uncertain. Additionally, the reliance on labeled training data limits its effectiveness based on dataset quality. Future work will focus on enhancing generalizability and responsiveness.

REFERENCES

[1] H. Liu and H. Wang, "Real-Time anomaly detection of network traffic based on CNN," *Symmetry*, vol. 15, no. 6, p. 1205, 2023. doi: 10.3390/sym15061205.

[2] Z. Liu, Q. Wang, and L. Zhang, "Deep learning-based anomaly detection in software-defined networks for DDoS and port scan attacks," J. Network Comput. Appl., vol. 58, pp. 124-135, 2023.

[3] Y. Zhang, X. Chen, and W. Li, "Convolutional Neural Networks for network anomaly detection in SDN environments," Int. J. Network Security, vol. 30, no. 4, pp. 456-470, 2022.

[4] A. S. F. Subhamathi, C. Sathiyapriyan, A. T, A. J. Anand, A. Rheem, and M. R. Arun, "Traffic Sign Detection Problems using Convolutional Neural Techniques in Image Processing," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, Gurugram, India, 2024, pp. 1-6.

[5] S. Sharma, R. Gupta, and P. Kumar, "Optimizing hyperparameters for real-time anomaly detection in SDN using deep learning models," J. Inf. Security Appl., vol. 62, pp. 101-112, 2023.

[6] G. Ashok and A. J. Anand, "Modified Image Encryption Algorithm Based on Chaotic Cryptography," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2023, pp. 1506-1512.

[7] S. Mahalakshmi, C. Rajeswari, A. J. Anand, and A. Rahul, "Client Authentication by Signature Verification Method Using Robotic Process Automation (RPA)," in *2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, Chennai, India, 2022, pp. 1-5.

[8] A. Ponmalar, A. J. Anand, T. Muthamizhan, T. Sobana, and J. H. Vishwath, "Automatic Forensic Analysis of Criminal Navigation System using Machine Learning," in *IEEE First International Conference on Computational Science & Technology (ICCST 2022)*, 2022, pp. 1-5.

[9] G. Mohamed, J. Visumathi, M. Mahdal, J. Anand, and M. Elangovan, "An effective and secure mechanism for phishing attacks using a machine learning approach," *Processes*, vol. 10, no. 7, p. 1356, 2022, doi: 10.3390/pr10071356.

[10] M. V. Arokiamary and J. Anand, "Analysis of dynamic interference constraints in cognitive radio cloud networks," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 815–823, 2021, doi: 10.48175/ijarsct-1484.

[11] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/access.2020.3009733.

[12] T. Ethilu, A. Sathappan, and P. Rodrigues, "Improving performance and efficiency of software defined networking by identifying malicious switches through deep learning model," *Int. J. Comput. Netw. Appl.*, vol. 9, no. 1, p. 72, 2022, doi: 10.22247/ijcna/2022/211627.

[13] M. Abdullahi *et al.*, "Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, 2022, doi: 10.3390/electronics11020198.

[14] L. Mhamdi and M. M. Isa, "Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation," *J. Netw. Comput. Appl.*, vol. 225, p. 103868, 2024, doi: 10.1016/j.jnca.2024.103868.

[15] C. Wang *et al.*, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 2, pp. 905–974, 2023, doi: 10.1109/comst.2023.3249835.

[16] G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proenca, "Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks," *IEEE Access*, vol. 8, pp. 100172–100184, 2020, doi: 10.1109/access.2020.2997939.