International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

CASE STUDY: HYBRID CNN-LSTM WITH ATTENTION MECHANISM FOR INTRUSION DETECTION IN SDN ENVIRONMENTS

P. Loganayagi[1], Dr. G. Ramesh[2]

[1]*Information Technology, K.L.N College of Engineering*
[2]*Information Technology, K.L.N College of Engineering*

Abstract - Network management is improved by Software-Defined Networking (SDN), which offers centralised control and programmability. Nevertheless, this centralisation also makes it susceptible to a number of assaults, such as brute force, botnet, infiltration, online attacks, Distributed Denial of Service (DDoS), and Denial of Service (DoS). In order to successfully detect and categorise these attacks, this paper suggests a hybrid deep learning model that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks with an attention mechanism. To improve detection accuracy, the CNN component extracts spatial characteristics, the LSTM records temporal dependencies, and the attention mechanism highlights important features. The model's effectiveness in recognising various attack types in SDN environments is demonstrated by experimental assessments.

***Key Words*:** SDN Security, Intrusion Detection, CNN-LSTM Hybrid, Attention Mechanism, Cyberattack Detection.

1.INTRODUCTION

Software-Defined Networking (SDN), a paradigm that separates the control plane from the data plane to enable centralised network management, has been adopted as a result of the development of contemporary network architecture. SDN is very flexible in complicated networking contexts because of this separation, which enables dynamic, programmable, and effective control over network traffic. But these benefits are also made possible by centralisation, which also creates serious security flaws. This architectural central point of control can be used by malicious actors to initiate a variety of cyberattacks that jeopardise network stability and data security, including Distributed Denial of Service (DDoS), brute force intrusions, botnet infections, and more.

Due to the size, speed, and unpredictability of contemporary attack patterns, traditional security measures like rule-based firewalls and signature-based intrusion detection systems frequently fail. These systems have trouble identifying advanced multi-vector intrusions that are frequently encountered in SDN deployments or previously unknown (zero-day) threats. The application of cutting-edge machine learning methods, especially deep learning models, has proven to be a potent remedy for these problems. While Long Short-Term Memory (LSTM) networks are excellent at capturing temporal dependencies across sequential data, Convolutional Neural Networks (CNNs) are best suited for identifying spatial patterns in traffic data. These models are further improved by the addition of attention mechanisms, which enable them to dynamically concentrate on the most pertinent characteristics in real-time data streams. This hybrid method is a very successful tactic for protecting SDN systems since it not only increases detection accuracy but also makes it possible to respond to network threats in real time and automatically.

2. CORE TECHNOLOGIES AND THREAT LANDSCAPES

2.1 Networking that is defined by software (SDN)

SDN is a networking architecture that allows for centralised network control by separating the control plane from the data plane. Better resource management and dynamic network setup are made possible by this architecture. The SDN controller is a prime target for cyberattacks, though, because centralisation also creates a single point of failure.

2.2 Cyberattacks in SDN

Because of its centralised architecture, Software-Defined Networking (SDN) is intrinsically susceptible to a variety of assaults, even while it provides enhanced control and flexibility in managing network infrastructures. The security and operation of SDN-based systems are seriously threatened by these flaws.

Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks are among the most dangerous types of attacks. In these situations, malevolent actors send a large number of traffic or service requests to the SDN controller or related network components. When system resources are overloaded, the network becomes inaccessible to authorised users due to severe performance degradation or total service disruptions.

Another threat vector is brute force assaults, in which hackers methodically try every password combination in an effort to access the controller or network nodes without authorisation. Even one exploited entry point has the potential to cause extensive harm or unapproved control over the network because of SDN's programmable architecture and centralised control mechanisms.

A group of hacked devices, frequently dispersed throughout several geographic locations, collaborate to carry out coordinated attacks on the SDN infrastructure in botnet attacks. It can be challenging to identify and stop these assaults, especially when machines are operating in stealth mode or often switch IP addresses. When an attacker successfully gains access to a network in order to obtain private data or change network behaviour without permission, this is known as an infiltration attack. This may entail eavesdropping on data,

rerouting traffic, or injecting harmful flows. Finally, web-based attacks take advantage of flaws in SDN controllers' web interfaces or APIs. In order to compromise the controller and possibly obtain complete administrative access, attackers may employ strategies like SQL injection, cross-site scripting (XSS), or other types of code injection. These attack methods highlight how crucial it is to put in place strong, perceptive, and flexible security measures—especially intrusion detection systems based on deep learning—to protect SDN settings.

2.3 Intrusion Detection Using Deep Learning

Network security is one area where deep learning models have demonstrated great promise. CNNs can be used to analyse network traffic patterns because of their proficiency in extracting spatial information from data. Recurrent neural networks (RNNs), of which LSTMs are a subset, are excellent at simulating temporal sequences and capturing how traffic changes over time. By enabling the network to concentrate on the most pertinent portions of the input, the attention mechanism improves detection performance and strengthens these models even more.

3. RELATED WORK

The utilisation of deep learning models for intrusion detection in SDN systems has been investigated in earlier research. For example, by capturing both geographical and temporal characteristics of network traffic, a hybrid CNN-LSTM model showed great accuracy in detecting DDoS attacks. By highlighting important aspects in the data, an attention-based CNN-LSTM architecture was presented in another study, which enhanced performance in identifying different sorts of attacks. These studies demonstrate how hybrid models, particularly those that include attention methods, can improve network security. SDN technology has been widely used in many different sectors and can increase network capacity. Ouamari MA et al. discovered problems with the wide area network's data interchange between the corporate office and nearby branches. They suggested the SDN-WAN method to address this issue. First, adjust network administration to satisfy service needs. The server's latency issue was then resolved by the dual optimisation problem of average request latency and survival. The findings demonstrated that the research approach greatly enhanced the system's performance when compared to conventional techniques [7].
The CNN algorithm has been used extensively in many different industries in recent years and has shown positive outcomes. A novel model was put forth by Chen et al. with the goal of speeding up gas detection computations. This model combines CNN-based Memristor. According to the study, the model is constructed using convolution cores of different sizes, extracts feature information of different dimensions using the multi-dimensional convolution method, and uses a memristor to boost the hardware structure's overall utilisation rate for faster operation [13]. In radar study, Bao and Yang discovered that human motion and other factors cause the signal to become unstable. As a result, a new technique for counting employees was created based on CNN. By using this technique, researchers seek to get more lucid graphical data in order to finish the counting task. The outcomes confirmed this method's superiority and produced the desired outcome [14].

Due to the current dearth of simultaneous multi-task models, Chen et al. created a model of laser-induced breakdown spectroscopy in conjunction with a two-dimensional CNN algorithm for the field of rock investigation. In order to carry out categorisation and recycling activities concurrently, this model is built with two different kinds of outputs. The findings demonstrated that this model's accuracy outperformed that of conventional models [15]. In order to solve the problem of CNN architecture design requiring a significant amount of computing time and human resources, Xue et al. devised an architecture search approach. This technique automates CNN architecture design by modifying the approach based on adaptive mutation neural structure. The outcomes demonstrated that this approach lowered calculation time, saved labour expenses, and accomplished the desired results [17]. Using SDN, Khalid et al. offered a way to guarantee the security of the Internet of Things by enabling the creation of independent verification and Tamper-resistance techniques [19].

In conclusion, recent studies demonstrate the expanding use of deep learning in Software-Defined Networking (SDN) contexts for intrusion detection systems (IDS). In detecting sophisticated network attacks like Distributed Denial of Service (DDoS), hybrid models—especially those that include Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks—have demonstrated encouraging outcomes. These models make use of LSTM's expertise in modelling temporal data and CNN's capacity to extract spatial characteristics. Attention methods, which allow the model to highlight important elements in network data, have been incorporated into CNN-LSTM architectures to further enhance detection performance.
SDN is being used in many industries to improve network scalability and control in addition to intrusion detection. Ouamari et al., for example, proposed an SDN-WAN technique to address performance concerns in wide area networks (WANs). When compared to conventional networking techniques, their technology greatly improves system performance by optimising both request latency and network resilience. Chen et al. created a two-dimensional CNN model for laser-induced breakdown spectroscopy (LIBS) in the field of scientific analysis and automation with the goal of classifying and recycling rock samples at the same time. The accuracy of this multitask learning strategy was higher than that of conventional single-task models.

Additionally, the computational difficulty of CNN architecture design was addressed by Xue et al. They presented an adaptive mutation-based automated neural architecture search technique that preserved model efficacy while drastically cutting down on development time and resource consumption. SDN integration is also helping to improve security in new technologies like the Internet of Things (IoT). In order to enhance IoT infrastructure against potential threats, Khalid et al. suggested utilising SDN to ensure tamper-resistance and independent verification. When taken as a whole, these studies demonstrate how well deep learning and SDN integration may improve cybersecurity and operational performance across a range of application areas.

4. PROPOSED HYBRID CNN-LSTM WITH ATTENTION MODEL

4.1 Architecture of the Model

In order to capture the temporal and geographical aspects of network traffic and highlight important information, the suggested model combines CNN and LSTM layers with an attention mechanism. The architecture is made up of:

- Network traffic data that has been pre-processed is received by the input layer.
- CNN Layers: Identify patterns suggestive of different cyberattacks by extracting spatial elements from the input data.
- LSTM Layers: Track the changes in traffic patterns over time by modelling temporal dependencies. By concentrating on the most pertinent aspects of the data, the attention mechanism improves the model's capacity to identify minute irregularities.
- Features from earlier levels are combined in the fully connected layer.
- The output layer offers the last categorisation, indicating whether or not particular attack types are present.

4.2 Pre-processing of Data

Datasets of traffic are encoded and normalised. Sliding windows are used to extract sequential characteristics, which are then transformed into input matrices for CNN processing.

4.3 Formulation in Mathematics

The following formulas are used to describe the model's computational dynamics:

A. 1D Convolution Operation:

$$f_i^{(l)} = \sum_{j=1}^{k} \omega_j^{(l)} . x_{i+j-1} + b^{(l)}$$

B. Max Pooling:

$$p_i = max(x_i, x_{i+1}, \dots\dots, x_{i+k-1})$$

C. LSTM Equations (per time step t):

$$\mathbf{f_t} = \sigma(W_f . [\mathbf{h_{t-1}}, \mathbf{x_t}] + \mathbf{b_f})$$

$$i_t = \sigma(W_i . [h_{t-1}, x_t] + b_i)$$

$$\bar{C}_t = tanh(W_C . [h_{t-1}, x_t] + b_c)$$

$$C_t = f_t . C_{t-1} + i_t . \bar{C}_t$$

$$\sigma_t = \sigma(W_0 [h_{t-1}, x_t] + b_0)$$

$$h_t = O_t . tanh (C_t)$$

D. Attention Mechanism:

$$Score(h_t) = tanh (W_a h_t + b_a)$$

$$\alpha_t = \frac{\exp(Score(h_t))}{\sum_{i=1}^{T} \exp (Score(h_i))}$$

$$C = \Sigma_{t=1}^{T} \alpha_t h_t$$

E. Final Dense Output:

$$\hat{y} = softmax(w_{d^c} + b_d)$$

Where,

- h_t: hidden state from LSTM at time t
- α_t: attention weight
- **C**: context vector used for prediction
- $\hat{y}$: output classification vector

5. CONCLUSIONS

An attention mechanism added to the Hybrid CNN-LSTM model offers a reliable and understandable intrusion detection solution for Software-Defined Networking (SDN) environments. Securing these infrastructures from more complex cyber-attacks has become a top challenge as SDN designs continue to be deployed across a variety of sectors due to their flexibility and centralised control.

Three key deep learning capabilities—spatial feature extraction, temporal sequence modelling, and dynamic focus on important data attributes—are combined in the proposed model by merging Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and attention processes. While LSTMs are good at detecting long-term temporal correlations, which are crucial for identifying slowly evolving attacks or coordinated infiltration campaigns, CNNs are excellent at spotting local anomalies and traffic patterns in flow-based data. The model may prioritise features that are most suggestive of harmful behaviour thanks to the attention method, which further improves classification accuracy and interpretability.

Without the need for manual feature engineering or previous rule definitions, this architecture enables the real-time detection and categorisation of a variety of cyberattacks, including as DDoS, DoS, brute force, botnet, infiltration, and web-based threats. Furthermore, even if attack tactics change, the model's capacity to adaptively learn from dynamic network behaviours guarantees its continued efficacy. The hybrid CNN-LSTM with attention mechanism not only improves detection performance but also makes a substantial contribution to the development of intelligent, automated, and robust intrusion detection systems for SDN environments, laying the groundwork for next-generation network security solutions, as shown by experimental evaluations.

REFERENCES

[1] H. Xue and B. Jing, "SDN Attack Identification Model Based on CNN Algorithm," in IEEE Access, vol. 11, pp. 87652-87666, 2023

[2] E.W. E.Viklund, I. Nilsson, and A. K. Forsman, ‘‘Nordic population-based study on internet use and perceived meaningfulness in later life: How they are linked and why it matters,’’ *Scand. J. Public Health*, vol. 50, no. 3, pp. 381–388, May 2022.

[3] N. Ravi and S. M. Shalinie, ‘‘Black Nurse-SC: A novel attack on SDN controller,’’ *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2146–2150, Jul. 2021.

[4] H. Li, J. Lu, J.Wang, H. Zhao, J. Xu, and X. Chen, ‘‘*SDM4IIoT* : An SDNbased multicast algorithm for industrial Internet of Things,’’ *IEICE Trans. Commun.*, vol. 105, no. 5, pp. 545–556, May 2022.

[5] D. Tang, Y. Yan, S. Zhang, J. Chen, and Z. Qin, ‘‘Performance and features: Mitigating the low-rate TCP-targeted DoS attack via SDN,’’ *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 428–444, Jan. 2022.

[6] S. Ravikumar and D. Kavitha, ‘‘CNN-OHGS: CNN-oppositional-based Henry gas solubility optimization model for autonomous vehicle control system,’’ *J. Field Robot.*, vol. 38, no. 7, pp. 967–979, May 2021.

[7] M. A. Ouamri, M. Azni, D. Singh, W. Almughalles, and M. S. A. Muthanna, ‘‘Request delay and survivability optimization for software defined-wide area networking (SD-WAN) using multi-agent deep reinforcement learning,’’ *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 7, Jul. 2023, Art. no. e4776.

[8] M. A. Ouamri, G. Barb, D. Singh, and F. Alexa, ‘‘Load balancing optimization in software-defined wide area networking (SD-WAN) using deep reinforcement learning,’’ in *Proc. Int. Symp. Electron. Telecommun. (ISETC)*, Timişoara, Romania, Nov. 2022, pp. 1–6.

[9] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, ‘‘SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective,’’ *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8421–8434, Sep. 2019.

[10] S. Badotra and S. N. Panda, ‘‘SNORT based early DDoS detection system using open daylight and open networking operating system in software defined networking,’’ *Cluster Compute.*, vol. 24, no. 1, pp. 501–513, Mar. 2021.

[11] U. Ahmed, J. C.-W. Lin, and G. Srivastava, ‘‘A resource allocation deep active learning based on load balancer for network intrusion detection in SDN sensors,’’ *Compute. Commun.*, vol. 184, pp. 56–63, Feb. 2022.

[12] A. El Kamel, H. Eltaief, and H. Youssef, ‘‘On-the-fly (D)DoS attack mitigation in SDN using deep neural network-based rate limiting,’’ *Compute. Commun.*, vol. 182, pp. 153–169, Jan. 2022.

[13] J. Chen, L. Wang, and S. Duan, ‘‘A mixed-kernel, variable-dimension memristive CNN for electronic nose recognition,’’ *Neurocomputing*, vol. 461, pp. 129–136, Oct. 2021.

[14] R. Bao and Z. Yang, ‘‘CNN-based regional people counting algorithm exploiting multi-scale range-time maps with an IR-UWB radar,’’ *IEEE Sensors J.*, vol. 21, no. 12, pp. 13704–13713, Jun. 2021.

[15] S. Chen, H. Pei, J. Pisonero, S. Yang, Q. Fan, X. Wang, and Y. Duan, ‘‘Simultaneous determination of lithology and major elements in rocks using laser-induced breakdown spectroscopy (LIBS) coupled with a deep convolutional neural network,’’ *J. Anal. At. Spectrometry*, vol. 37, no. 3, pp. 508–516, 2022.

[16] S. Guo, Z. Wang, Y. Lou, X. Li, and H. Lin, ‘‘Detection method of photovoltaic panel defect based on improved mask R-CNN,’’ *J. Internet Technol.*, vol. 23, no. 2, pp. 397–406, Mar. 2022.

[17] Y. Xue, Y. Wang, J. Liang, and A. Slowik, ‘‘A self-adaptive mutation neural architecture search algorithm based on blocks,’’ *IEEE Compute. Intell. Mag.*, vol. 16, no. 3, pp. 67–78, Aug. 2021.

[18] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, ‘‘Toward software-defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects,’’ *IEEE Access*, vol. 10, pp. 70850–70901, 2022.

[19] M. Khalid, S. Hameed, A. Qadir, S. A. Shah, and D. Draheim, ‘‘Towards SDN-based smart contract solution for IoT access control,’’ *Compute. Commun.*, vol. 198, pp. 1–31, Jan. 2023.

[20] K. Renuka, D. S. Roy, and K. H. K. Reddy, ‘‘An SDN empowered location aware routing for energy efficient next generation vehicular networks,’’ *IET Intell. Transp. Syst.*, vol. 15, no. 2, pp. 308–319, Feb. 2021.