International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Designing A Network Intrusion Detection System Using Advanced Bi-LSTM Based Model for Identifying and Classifying Intrusions

Deen Bandhu[1], Simrandeep Kaur[2], Dr. Gurpreet Singh[3]

Research Scholar[1], Assistant Professor[2], Professor[3]

Department of Computer Science & Engg. St. Soldier Institute of Engineering and Technology, Jalandhar

Abstract: By enabling the control and administration of the entire network from a single location, a software-defined network, or SDN, was created to make network administration easier. Today's data center network infrastructure frequently uses SDN, but emerging threats like Distributed Denial-of-Service (DDoS), online attacks, and the User to Root (U2R) attack pose serious problems that could prevent SDNs from being widely adopted. SDN controllers find intruders appealing because they are worthwhile targets. An attacker may take control of an SDN controller and use it to route traffic anyway they see fit, which would have disastrous effects on the network as a whole. The quality of the training datasets affects how well the detection models work, even though the combined vision of SDN and deep learning techniques creates new opportunities for the security of IDS deployment. Most of the studies ignored the effects of data redundancy and an unbalanced dataset, despite the fact that deep learning for NIDSs has recently demonstrated encouraging outcomes for a variety of concerns. This could therefore have a negative impact on the anomaly detection system's robustness, leading to less-than-ideal model performance. We imported all necessary libraries, including the UNSW-NB15 training dataset, and used the proposed model in this investigation. We are combining the Random Forest model with the BiLSTM model, a deep learning method. The combined output is then analyzed to determine the accuracy, precision, recall, and F1-score.

Keywords: Software Designed networks, ML, DL, Bi-LSTM.

I.INTRODUCTION

Earlier concepts that focused primarily on control-data plane separation and programmable networks gave rise to software-defined networking (SDN) [1]. The Open Networking Foundation (ONF), a nonprofit industry consortium that provides support and guarantees various advancements in the SDN field, maintains the OpenFlow protocol, which is used by the controller, which functions as a logically centralized controlling point in the SDN paradigm, to effectively manage and collect flow-based statistics. Despite SDN's many benefits, there might be security concerns that need to be resolved before it can be extensively adopted. An intrusion on an SDN controller could have far-reaching effects on the entire network, but in a traditional network, the damage is primarily limited to a single node or segment. The network can be susceptible to malfunctions if an attacker manages to take down the controller. Furthermore, a hacker can bombard the network with dangerous cyberattacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Because of the high channel bandwidth and network resource usage, legitimate inquiries could be rejected [2].

SDN's dynamic and adaptable features could lead to more false attack detections. An attacker might take control of an SDN controller and use it to route traffic as they see fit, which would have an impact on the entire network. It is unclear whether SDN's more intricate flow management may make service failures more likely, despite the fact that intrusion detection systems (IDS) are a valid means of ensuring a network is secure and capable of identifying and preventing intrusions. The unique characteristics of SDN

may increase exposure to sophisticated cyber-attacks, despite the fact that an intrusion detection system's (IDS) primary function is to monitor network traffic and alert the administrator of any malicious threats in the network. This has raised concerns about the need to develop innovative IDS approaches to secure SDN, protect user communication [3], and uncover emerging security issues.

A crucial step in getting ready for network classification challenges is feature selection. The feature selection process aids in the reduction and elimination of redundant and unnecessary features from the main database that don't affect the classification outcomes. By enabling feature selection, a subset of the original dataset is chosen based on certain criteria that include the original dataset's characteristics. When fundamental strategies are used to decrease the features of huge datasets, Kantardzic [4] asserts that classification improves. Filter-based and wrapper-based feature selection algorithms are the two varieties. Filtering techniques are less likely to be over adjusted, have quick processing speeds, and are computationally efficient. ANOVA, chi-squared, and Pearson's correlation are popular techniques for filter selection. Wrapper approaches, on the other hand, offer the best subset of pertinent functions; but they take longer to compute, which lowers system performance. Wrappers frequently use backward elimination, forward selection, and recursive selection. Intrusion detection systems encounter issues with data dimensions and complexity as network traffic grows.

Using Deep Learning (DL) models is one of the suggested ways to enhance network intrusion detection system (NIDS) monitoring. The quality of the training datasets determines how effective the detection method is, even though the combined vision of SDN and deep learning techniques offers up new possibilities for the security of IDS deployment. Most of the studies ignored the effects of data redundancy and an unbalanced dataset, despite the fact that deep learning for NIDSs has recently demonstrated encouraging outcomes for a variety of concerns. This could therefore have a negative impact on the anomaly detection system's robustness, leading to less-than-ideal model performance.

Our model uses a CNN–BiLSTM hybrid approach to improve SDN security. For the earlier DL models to work well, a large number of training parameters were needed. Making the model employ a lot of parameters could make the training process take longer and cost more money. Consequently, it increases the SDN architecture's computational overhead. In order to optimize NIDS deployment, our method recommends deep learning over SDN. For network monitoring, the SDN controller's NIDS implementation uses a deep learning methodology. This study suggests applying tree-based deep-learning techniques to more accurately detect anomalies. To identify whether an intrusion has happened as well as categorize the type of intrusion, ten features were employed in a multi-class categorization. Prior research has employed deep learning algorithms in NIDS to secure SDN, in contrast to earlier studies. Nevertheless, they only used common datasets that aren't specifically focused on SDN, like NSL-KDD and UNSW-NB15. The InSDN database was used by other authors [5], but their CNN-LSTM model was deemed weaker than the CNN-BiLSTM model. BiLSTM, which contains distinct sequences, was employed in this model. Every BiLSTM sequence has two LSTM layers that travel forward and backward. This makes up for LSTM's lack of contextual semantic information. A bidirectional structure that offers information about the past and future covers every single point in the output layer's input sequence. Our model's BiLSTM Networks were utilized to increase classification accuracy and more effectively identify LSTM dependant features.

The organization of paper is as follows: section II describes the literature survey and section III shows the proposed work and section IV gives the results and discussions and section V conclude the paper.

II.LITERATURE SURVEY

Sotiris Chatzimiltis et al. (2024) proposes a new SDN-based SG architecture, highlighting the existence of IDSs in the SDN application layer. We implemented a new smart meter (SM) collaborative intrusion detection system (SM-IDS), by adapting the split learning methodology. Finally, a comparison of a federated learning and split learning

neighbourhood area network (NAN) IDS was made. Numerical results showed, a five-class classification accuracy of over 80.3% and F1-score 78.9 for a SM-IDS adapting the split learning technique. Also, the split learning NAN-IDS exhibit an accuracy of over 81.1% and F1-score 79.9[6].

Abdulsalam O. Alzahrani et al.(2022) introduces two created datasets generated from SDN using Mininet and Ryu controller with different feature extraction tools that contain normal traffic and different types of attacks (Fin flood, UDP flood, ICMP flood, OS probe scan, port probe scan, TCP bandwidth flood, and TCP syn flood) that is used for training a number of supervised binary classification machine learning algorithms such as k-nearest neighbor, AdaBoost, decision tree (DT), random forest, naive Bayes, multilayer perceptron, support vector machine, and XGBoost. The DT algorithm has achieved high scores to fit a real-time application achieving F1 score on attack class of 0.9995, F1 score on normal class of 0.9983, and throughput score of 6,737,147.275 samples per second with a total number of three features. In addition, using data preprocessing to reduce the model complexity, thereby increasing the overall throughput to fit a real-time system [7].

K.A. Dhanya et al. (2023) Proposed models have experimented with the UNSW-NB15 dataset of 49 features for nine different attack samples. Decision Tree classifier produced the best accuracy of 99.05% compared to ensemble models - Random Forest (98.96%), Adaboost(97.87%), and XGBoost(98.08%). K-Nearest Neighbour classifier trained for various values of K and best performance obtained for K=7 with the accuracy of 95.58%. A Deep Learning model with two dense layers with ReLU activation and a third dense layer with a Sigmoid activation function is designed for binary classification and produced good accuracy of 98.44% with ADAM optimizer, 80:20 Train-Test Split Ratio. Network attack exploits are detected with an accuracy 95% by XGBoost, Fuzzers attack with 90% accuracy by Random Forest, Generic attacks with 99% accuracy by Random Forest, and Reconnaissance attacks with 79% by Decision Trees [8].

A. d. R. L. Ribeiro et al. (2021) present an anomaly-based approaches that uses machine learning algorithms over continuous data stream for intrusion detection in a SDN environment. Our approach is to overcome the main challenges that happen when developing an anomaly-based system using machine learning algorithms. For characterising the anomalies, we have analysed a type of DDoS attack classified as infrastructure attack that considers the impact of both bandwidth and resource depletions. The resource depletion attack attempts to exhaust the flow table of switches through SYN flooding. From experiments, we notice that the solution obtains 97.83% accuracy, 99% recall, 80% precision and 2.3% FPR for 10% DDoS attacks on the normal traffic. These results show the effectiveness of the proposed technique [9].

M. Kavitha et al. (2022) uses machine learning models to detect Distributed Denial of Service (DDoS) attacks. The machine learning model is trained using data from KDD Cup 99.K Nearest Neighbor Classifier, Logistic Regression, and Decision Tree have been used to train and test the datasets. It can be concluded that machine learning methods can be more effective at detecting DDoS attacks than traditional methods, that can be applied to software defined networks. Several experiments demonstrate the potential of our proposal to detect intrusion in SDN environments after extensive evaluation [10].

Tsung-Han Lee et al. (2020) introduce a deep learning enabled intrusion detection and prevention system (DL-IDPS) to prevent secure shell (SSH) brute-force attacks and distributed denial-of-service (DDoS) attacks in SDN. The packet length in SDN switch has been collected as a sequence for deep learning models to identify anomalous and malicious packets. Four deep learning models, including Multilayer Perceptron (MLP), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and Stacked Auto-encoder (SAE), are implemented and compared for the proposed DL-IDPS. The experimental results show that the proposed MLP based DL-IDPS has the highest accuracy which can achieve nearly 99% and 100% accuracy to prevent SSH Brute-force and DDoS attacks, respectively [11].

Z. Chen et al., (2023) propose a new method that uses deep learning for attack detection in an SDN environment. In this method, we first utilize fisher score to remove insignificant features, then design a network model combining bi-directional long short-term memory network (BiLSTM) and gated convolutional neural network (GCNN) to capture the spatio-temporal features of network traffic, and finally use a fully connected layer to perform seven classifications of data. We choose focal loss as the loss function due to the imbalance of samples. The proposed model is evaluated based on the InSDN dataset, which is the latest IDS dataset developed specifically for SDN environments, and the CIC-IDS2017 dataset. The results show that the proposed model improves the performance for anomaly detection and achieves an accuracy of 99.80% and 98.85% on the InSDN and CIC-IDS2017 datasets, respectively. This level of detection accuracy provides great confidence in protecting SDN networks from anomalous traffic [12].

III.PROPOSED WORK

- **PROBLEM FORMULATION**

Recently the authors proposed an effective mechanism for detecting intrusions in IoT systems in which they used different variants of LSTM. No doubt that the model was showing good results, however after studying literature carefully we observed that there is a scope of improvement. One of the major limitations in traditional model was that they used LSTM for detecting intrusions in IoT network. However, more advanced techniques are already available that can show greater results. Furthermore, LSTM is able to retain only past information and doesn't keep any record for future information. Also, LSTMs are sensitive to various random weight initializations and undergo through overfitting issues. Moreover, it requires longer time and memory to train LSTM. Furthermore, the authors didn't use any feature selection technique which causes dataset dimensionality issues and hence degrade the accuracy rate as well.

- **Objectives**

- To implement an effective feature selection technique for overcoming dataset dimensionality
- To propose advanced Bi-LSTM based model for identifying and classifying intrusions.
- To analyze the performance of proposed model by comparing it with traditional models in terms of various performance metrics.

IV.RESULTS

On Google Colab, we are using Python to create the suggested model and importing all required libraries, including the UNSW-NB15 training dataset. We are integrating the Random Forest model with a deep learning technique, namely the BiLSTM model. The accuracy, precision, recall, and F1-score are then determined by analyzing the combined output.

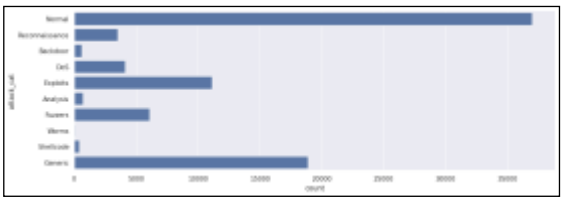

Figure 1: Types of attacks

All attacks and their frequencies are displayed for each type of attack in Figure 1. To translate all assault labels into numerical numbers, we are use Label Encoder. The dataset is then subjected to the Principal Component Analysis (PCA) method, and the data is divided into training and testing 70-30 using the output of the min max value transformation.

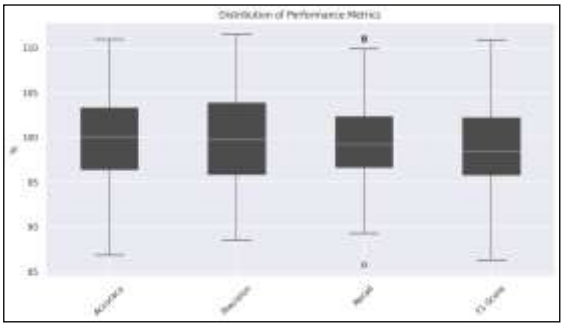

Figure 2: Distribution of performance metrics

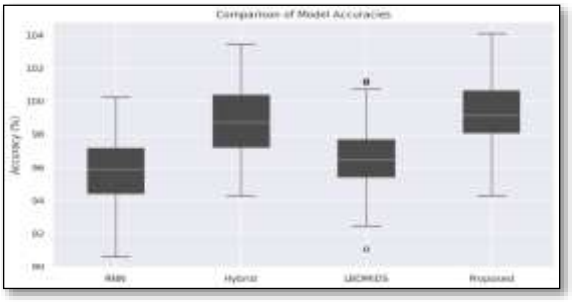

Figure 3: Comparison of Model Accuracies

From table 1 clearly shown that the proposed model achieved best accuracy as compared to other methods.

Table 1: Accuracy for Different methods

Techniques	Accuracy
RNN	95.8 %
Hybrid	98.4%
LBDMIDS	96.2%
Proposed	98.6%

Figure 4: Confusion Matrix

By displaying the numbers of accurate and inaccurate predictions for each class, a confusion matrix is a table that is used to assess a classification model's performance. It displays the frequency with which each class was successfully or mistakenly predicted by comparing the model's predicted values with the actual values. Each cell (i,j) in a matrix with k rows and k columns reflects the number of examples with true class I that were predicted to be class J in a multi-class issue with k classes. This makes it possible to examine both the kinds of accurate classifications and the kinds of incorrect categories the model produced.

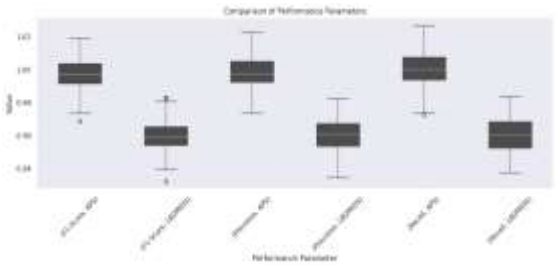

Figure 5: Comparison of Performance Parameters

The f1 score, precision, and recall values for various accuracies are displayed in figure 5, and the suggested method performs better.

V.CONCLUSION

SDN has the potential to significantly reduce the complexity of network configuration and management while enabling network operation. SDN can effectively manage the difficulties in a traditional network. To detect and stop attacks in the transmitted packets, SDN developed intrusion detection. The goal of the IDS is to collect data from different systems or network sources and examine the collected data for potential threats. The first chapter provides a thorough understanding of the fundamentals of the SDN network and covers the architecture, applications, and numerous problems. The types, different approaches, network assaults, and evaluation metrics of intrusion detection systems are then covered. The main goal of the project is to improve SDN security.

Also provides a detailed presentation of the several machine learning and deep learning techniques utilized for SDN intrusion detection, as well as an analysis of these techniques based on categorization and dataset. Because it offers a workable solution and more precisely detects the type of attack, the ML and DL model optimization utilized for IDS is crucial. The optimization algorithms that were employed to enhance the learning model were also covered. Numerous SDN security issues have been identified from the literature, and managing the emergence of novel attack types is a significant security challenge due to the dynamic nature of SDN.

REFERENCES

[1] Md. Rayhan Ahmed, salekul Islam, Swakkhar Shatabda, “Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques --A Comprehensive Survey”, TechRxiv. November 21, 2022.

[2] S. Prathibha *et al.*, "Detection Methods for Software Defined Networking Intrusions (SDN),” International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-6, doi: 10.1109/ACCAI53970.2022.9752574.

[3] Anurag Bhardwaj, Ritu Tyagi, Neha Sharma, Akhilendra Khare, Manbir Singh Punia, Vikash Kumar Garg, “Network intrusion detection in software defined networking with self-organized constraint-based intelligent learning framework”, Measurement: Sensors, Volume 24,2022,

[4] A.O. Alzahrani, M.J.F. Alenazi, “Designing a network intrusion detection system based on machine learning for software defined networks”, Future internet, 13 (2021), p. 111, 10.3390/fi13050111

[5] N. Thomas Rincy, Roopam Gupta, “Design and development of an efficient network intrusion detection system using machine learning techniques”, Wireless Commun. Mobile Comput., 2021 (2021).

[6] Sotiris Chatzimiltis; Mohammad Shojafar; Mahdi Boloursaz Mashhadi; Rahim Tafazolli, “A Collaborative Software Defined Network-Based Smart Grid Intrusion Detection System”, IEEE Open Journal of the Communications Society (Volume: 5), Page(s): 700 – 711,2024.

[7] Abdulsalam O. Alzahrani, Mohammed J. F. Alenazi, “ML-IDSDN: Machine learning based intrusion detection system for software-defined network”, Volume35, Issue1,10 January 2022.

[8] K.A. Dhanya, Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T., T. “Detection of Network Attacks using Machine Learning and Deep Learning Models”, Procedia Computer Science, Volume 218, 2023, Pages 57-66.

[9] A. d. R. L. Ribeiro, R. Y. C. Santos and A. C. A. Nascimento, "Anomaly Detection Technique for Intrusion Detection in SDN Environment using Continuous Data Stream Machine Learning Algorithms,” IEEE *International Systems Conference (SysCon)*, Vancouver, BC, Canada, 2021, pp. 1-7, doi: 10.1109/SysCon48628.2021.9447092.

[10] M. Kavitha, M. Suganthy, A. Biswas, R. Srinivsan, R. Kavitha and A. Rathesh, “Machine Learning Techniques for Detecting DDoS Attacks in SDN”, *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, 2022, pp. 634-638, doi: 10.1109/ICACRS55517.2022.10029110.

[11] Tsung-Han Lee; Lin-Huang Chang; Chao-Wei Syu, “Deep Learning Enabled Intrusion Detection and Prevention System over SDN Networks”, 2020 IEEE International Conference on Communications Workshops (ICC Workshops)

[12] Z. Chen, A. Hou, C. Q. Wu, X. Qu, Y. Wang and L. Ru, "On a Hybrid BiLSTM-GCNN-Based Approach for Attack Detection in SDN,″ 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Melbourne, Australia, 2023, pp. 233-240, doi: 10.1109/HPCC-DSS-SmartCity-DependSys60770.2023.00040.