International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A Study on Deep Learning Methods Used for Intrusion Detection and Prevention

Sonali V. R. P. Reddy[1], Nadine Dias[2]

[1]Student, Information Technology Department, Goa College of Engineering, Farmagudi, Goa.
[2]Assistant professor, Information Technology Department, Goa College of Engineering, Farmagudi, Goa.

Abstract - Cyberattacks are growing swiftly as the Internet grows, and the situation of cyber security is not encouraging. The availability of vital services is disrupted by denial-of-service (DoS) attacks, one of the most dangerous security risks facing the Internet today. The range of attack strategies and the amount of real-time traffic that has to be analysed provide a barrier to DoS detection. This study report describes key literature surveys about detecting and preventing denial of service (DoS) attacks using different deep learning methods.

Key Words: Deep Learning, Intrusion Detection, Intrusion Prevention, Network, TensorFlow.

1. INTRODUCTION

Due to the numerous cyberattacks that influence concerns with confidentiality, integrity, and availability, intrusion detection systems (IDS) now play a crucial role in companies [1]. So there arises a need to detect and prevent these attacks [2]. One of the most dangerous cyberattacks now targeting Internet users is the denial of service (DoS) attack, which prevents genuine users from accessing online services. Thus, a DoS attack detection system is required to safeguard online services from these assaults [3]. Experts in this profession often employ a variety of tools and techniques that monitor network traffic to spot odd activities, preserve data, and prevent negative outcomes. From a detection angle, there are two methods for detecting intrusions:

- signature-based detection, which identifies intruders using a database of signatures established from information from prior assaults, and
- Anomaly-based detection, which detects intruders by monitoring, collecting, and analysing network packets that are further classified as benign or malicious.

Machine Learning (ML) is also used to address various cybersecurity issues but it has several drawbacks. One of them is that it may mistakenly label a malicious data packet as benign and accept it for learning, which would totally ruin the algorithm. Another is that it might mistakenly label anomalous packets as benign packets. The second problem is that processing the numerous packets that are sent over the network takes a lot of time, making it challenging to analyse them in real-time Machine Learning (ML) is also used to address various cybersecurity issues but it has several drawbacks. One of them is that it may mistakenly label a malicious data packet as benign and accept it for learning, which would totally ruin the algorithm. Another is that it might mistakenly label anomalous packets as benign packets. The second problem is that processing the numerous packets that are sent over the network takes a lot of time, making it challenging to analyse them in real-time and perhaps affecting computer system performance. These problems can be solved with the help of Deep Learning (DL). With the use of deep learning, a subset of machine learning, a computer-based system can be trained to do beneficial tasks including disease diagnosis, speech recognition, picture recognition, fraud detection, and prediction [4].

2. ANALYSIS OF VARIOUS METHODS USED FOR INTRUSION DETECTION AND PREVENTION

A. TensorFlow Model

In [1], developed an intrusion detection method based on a deep learning model that can categorise various attack types without the use of signature mapping or rules created by people. They used Keras on top of TensorFlow to classify five common types of assaults using the supervised deep learning technologies RNN, Stacked RNN, and CNN. Their method simply needs the packet header data; the user payload is not required. They compared their results with those from Snort IDS in order to validate the performance using the pcap files from the MAWI dataset. The results demonstrate that Snort was unable to identify the network scan attack through ICMP and UDP due to the absence of user payloads. They demonstrate that RNN, Stacked RNN, and CNN may be used to accurately categorise attacks such as port scans, network scans over ICMP, network scans over UDP, network scans over TCP, and denial-of-service attacks. The most accurate technology was RNN.

B. Multi-Layer Perceptron Model

In [2], To accomplish intrusion detection and prevention tasks more quickly and effectively, the separate intrusion detection system and the intrusion prevention system are merged into a single system. Deep learning is being used to develop an intrusion detection and prevention system that can quickly identify and stop assaults like DOS, Probe, R2L, and U2R. A Multi-Layer Perceptron Deep Learning model, which was very accurately trained on the dataset kddcup99, is used to detect the

intrusion as it occurs. The deployed Deep learning model receives the pertinent network data, stores it as a CSV file, and uses it to forecast the attacks in real-time, enabling detection. A script that runs in the background is used to stop the intrusion in the second phase. The script is created to carry out the preventive phase by making the proper decisions on the various preventative actions to be taken for various sorts of attacks. The categorization component of the data obtained by the Multi-Layer Perceptron model can be used to make the choice.

C. VCDeepFL Model

In [3], There are several machine learning-based attack detection techniques, however, they lack the ability to distinguish between known and unidentified DoS attacks and have a high false alarm rate. The proposed Vector Convolutional Deep Feature Learning (VCDeepFL) approach for identifying DoS attacks addresses these problems. The Vector Convolutional Neural Network (VCNN) and Fully Connected Neural Network (FCNN) are both used in the VCDeepFL method. By down sampling the input vector, VCNN extracts the feature and improves the representation of the input vector. The attack detection system's performance is improved using FCNN, a multiclass classifier, by automatically determining the ideal set of training weights. The suggested method is examined using the NSL-KDD dataset and evaluated against cutting-edge attack detection systems and base classifiers. It is clear that the suggested strategy produces notable outcomes for the majority of the classes. Additionally, Receiver Operating Characteristics (ROC) analysis is carried out, and it can be shown from the ROC curve that the suggested technique has a large Area Under the Curve (AUC).

D. Deep Neural Network Model

In [4], The proposed deep learning-based DDoS detection model's performance was assessed experimentally using the NSL-KDD dataset. Normal network traffic and 23 distinct DDoS attacks, each with 41 features, are both included in the NLSKDD dataset. Two distinct experiments are run as part of the experimental investigation. First off, the proposed deep neural network accurately classified the Dos assaults with an accuracy of 0.988. By reviewing earlier feature reduction studies on the NSL-KDD dataset, the second experiment reduces the number of features in the NSL-KDD dataset to 24. All cyberattacks were classified by the suggested deep neural network with a classification accuracy of 0.984. For all experiments, the 10-fold cross-validation is applied. The proposed deep learning-based DDoS detection consequently performed well.

E. DeepDefensen Model

In [5], It is hard to detect low rate attack because it looks similar to the legitimate network traffic from the victim end. Meanwhile, DDoS attacks toward victim systems must be generated over time. Otherwise, it will not be malicious to the network/system resources. This suggests the importance of historical information in DDoS detection. The single-packet-based detection method cannot improve performance due to the missing historical pattern in the learning model. Therefore, the DeepDefense approach is introduced to identify DDoS attacks based on Recurrent Neural Networks (RNN) (e.g., LSTM, GRU) and presented four RNN models. From experimental results, all of them outperform shallow machine learning models. RNN demonstrates the effectiveness of identifying attacking network packets. The performance improves with the increase of the length of history. They also adopted CNN in their model to gain the local correlations among network fields. They reduced the error rate from 0.07517 to 0.02103 compared with the conventional machine learning method in the larger dataset.

F. DNN Based Anomaly Detection Model

In [6], Recent research has focused more on anomaly identification using Deep Neural Networks (DNNs). Despite their excellent accuracy, DNNs' black-box design makes them impractical for practical implementation. Explanations of DNN-identified abnormalities are essential, especially in industrial anomaly detection systems. This study offers a framework for DNN-based anomaly detection that explains abnormalities found. During online processing, the framework responds to the queries "Why is it an anomaly?" and "What is the confidence?" The framework increases the user's trust in the system by minimizing the transparent nature of the DNN-based anomaly detector. The benchmark KDDNSL dataset is used in this study to build the first steps of the proposed framework for detecting DoS attacks. Offline DNN explanations show that the DNN was capable of identifying DoS attacks with an accuracy of about 0.97 based on characteristics indicating the connection's destination, frequency, and volume of data exchanged.

G. C-LSTM Neural Networks Model

In [7], The identification of Web traffic anomalies was done using C-LSTM neural networks. a C-LSTM neural network for efficiently simulating the temporal and spatial information in the one-dimensional time series signal of traffic data. furthermore, offered a technique for automatically extracting reliable spatial-temporal information characteristics from raw data. Tests show that their C-LSTM technique, which combines a convolutional neural network (CNN), long short-term memory (LSTM), and deep neural network, can extract more

complicated data (DNN). The LSTM layer is suited for modeling time information, the DNN layer is used to map data into a more separable space, and the CNN layer is used to reduce the frequency fluctuation in spatial information. Even for extremely similar signals that were previously thought to be very difficult to categorise, the C-LSTM approach provides virtually flawless anomaly detection performance for online traffic data. For Yahoo's well-known Webscope S5 dataset, the C-LSTM algorithm beats other cutting-edge machine learning methods, reaching an overall accuracy of 0.986 and recall of 0.897 on the test dataset.

H. Deep Neural Network with Gated Recurrent Units Model

In [8], Consider the time-related intrusion features before proposing a unique intrusion detection system (IDS) made up of a gated recurrent unit (GRU), multilayer perceptron (MLP), and softmax module. On the well-known KDD 99 and NSL-KDD datasets, experiments demonstrate the system's superior performance. The overall detection rate was 0.9942 using KDD 99 and 0.9931 using NSL-KDD with false positive rates as low as 0.0005 and 0.0084, respectively. In particular, for detecting denial of service attacks, the system achieved detection rates of 0.9998 and 0.9955, respectively. Comparative tests demonstrated that the GRU is a more effective simplification and advancement of LSTM and that it is better appropriate as a memory unit for IDS. Moreover, when compared to previously released algorithms, the bidirectional GRU may get the greatest performance.

3. CONCLUSIONS

This paper presents a study on deep learning methods for intrusion detection and prevention systems. The examination of comparisons between the various approaches to the implementation of an intrusion detection and prevention system becomes clear that each technique has advantages and disadvantages of its own. As a result, choosing one intrusion detection system implementation technique over another is challenging. Network intrusion detection datasets are crucial for system testing and training. Without representative data, deep learning techniques cannot be used, and gathering such a dataset is challenging and time-consuming. The current public dataset, however, has numerous issues, including inconsistent data and out-of-date material. The growth of research in this field has been significantly constrained by these issues. Rapid network information updates make it challenging to train and apply deep learning models, necessitating quick and thorough retraining. So, future research in this area will concentrate on incremental learning and lifetime learning.

ACKNOWLEDGEMENT

The authors would like to thank the head of the department, Dr. Nilesh B. Fal Dessai, of the Information Technology Department at the Goa College of Engineering, for his valuable comments and suggestions.

REFERENCES

[1] N. Chockwanich and V. Visoottiviseth, "Intrusion Detection by Deep Learning with TensorFlow," 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019, pp. 654-659, doi: 10.23919/ICACT.2019.8701969.

[2] A. Krishna, A. Lal M.A., A. J. Mathewkutty, D. S. Jacob and M. Hari, "Intrusion Detection and Prevention System Using Deep Learning," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 273-278, doi: 10.1109/ICESC48915.2020.9155711.

[3] N. G. B. Amma and S. Subramanian, "VCDeepFL: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks", TENCONIEEAcknowledgment2018.

[4] A. S. Unal and M. Hacibeyoglu, "Detection of DDOS attacks in network traffic using deep learning", Int. Conf. Adv. Technol, 2018.

[5] X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS attack via deep learning", Proc. IEEE Int. Conf. Smart Comput., pp. 1-8, May 2017.

[6] K. Amarasinghe, K. Kenney and M. Manic, "Toward explainable deep neural network based anomaly detection", 11th Int. Conf. Hum. Syst. Interact. (HSI), 2018.

[7] T.-Y. Kim and S.-B. Cho, "Web traffic anomaly detection using C-LSTM neural networks", Expert Syst. Appl., vol. 106, pp. 66-76, Sep. 2018.

[8] C. Xu, J. Shen, X. Du and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units", IEEE Access, vol.