ISSN: 2366-1313

Network security using the Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection

[1]BATHULA SREEJA, [2]Dr.D. RAMESH

[1]M. Tech Scholar, [2]Professor, Dept. Of CSE,

JNTUHU COLLEGE OF ENGINEERING, JAGTIAL, T.S., INDIA

Abstract:

We have seen a dramatic increase in the number of edge and Internet of Things (IoT) devices utilized in daily life in recent years. In order to safeguard its users, this necessitates enhancing the security of these devices against cyberattacks. In order to improve the reliability and resilience of Network Intrusion Detection Systems (NIDS), Machine Learning (ML) approaches have been employed for years. DT outperformed the preceding ML approaches. Deep Learning (DL) approaches have been employed recently in an effort to create more dependable systems. In this study, we created a 13-feature Deep Neural Network (DNN) model and a Deep Learning enabled Long Short-Term Memory (LSTM) Autoencoder that performed much better in terms of accuracy on the UNSWNB15 and Bot-IoT datasets. Thus, we constructed NIDS models based on stacked LSTM and bidirectional LSTM versions of LSTM and suggested LBDMIDS, validating their performance on the UNSW NB15 and BoTIoT datasets. This study comes to the conclusion that these LBDMIDS variations outperform conventional ML approaches and perform similarly to previously proposed DNN models.

Index Terms: IoT Security, Intrusion, IDS, LSTM, Deep Learning

I. INTRODUCTION

In recent years, data security has become a critical component of the internet. Intruder broke into the system to obtain information from the network or utilize it for illicit purposes. An intrusion is nothing more than an assault, hack, packet sniff, or data stilling. Attacks try to compromise system privacy or networks in order to extort money, accomplish other nefarious goals, or seize crucial data. Through the use of malicious code, intrusion can change a programmer, data, or piece of logic in a computer, which has a number of negative effects that can give or take away an organization's confidential information and make it available to cybercriminals. Cyber-attacks cover a wide range of offences, including data hacking, service denial, malware, phishing, and theft. Cyber security defenders face several dangers from these cyber attackers as the percentage of cyberattacks or illicit actions increases worldwide. Security measures are crucial because they may have a significant and massive impact on human life. Additionally, an intrusion detection system can carry out these actions (IDS). By gathering data packets, examining them, and looking for any unwanted, suspicious, or malicious items in the traffic to alert the administrator, intrusion detection can be carried out. This equipment is equipped to protect our data from attacks and unauthorized use.

Threats to security are particularly prevalent in the digital environment. Websites are being hacked by hackers increasingly frequently for a variety of reasons. Due to the multiple security risks this generates, many businesses have had to review their security protocols. To get around the system and implement their malicious ideas, hackers identify the website's vulnerabilities. Security information and event management system is another name for an intrusion detection system. The two most common techniques are anomaly-based and signature-based. As well as host-based, perimeter-based, VM-based, and network intrusion detection system types. The system recognizes a network when a data packet moves from one location to another. This action is helpful for preventing the loss of data, information, and other things because of an attack.

The main reason to use LSTM is because it has an approach that is not constrained by the drawbacks of traditional DL (neural networks) techniques. Since the input and output sequences between the layers are varied in this case, it may be effective to detect both known and unidentified attacks.

II. RELATED WORK

Recent advancements in intrusion detection systems are included in this section. Anomaly detection uses a variety of machine learning techniques. The techniques evolve together with technological advancement to meet demands. These approaches currently use deep learning for greater precision and accuracy, which was translated from machine learning.

SVM and the Naive Bayes approach were utilized by Anish Halimaa and Dr. K. Sundarakantha [1] for intrusion detection. The NLS-KDD dataset is used in this paper to compare the analysis of SVM and Nave bayes. Both approaches were employed to resolve the classification issue. SVM performs better than Nave Bayes when accuracy and misclassification rate are calculated. Comparative analysis also uses normalization and feature reduction. Accuracy is a key factor in a model's performance; by improving accuracy, the main goal is to decrease the false alarm rate (FAR) and raise the detection rate. SVM algorithms are utilized for image processing and pattern rearrangement applications, while Naive Bayes, which is based on Bayes' theorem, is used for statistical classification.

We suggest using deep convolutional generative adversarial networks (DCGAN), which allows features to be extracted directly from the raw data and then generates new training sets by learning from the raw data, to address the issue of unbalanced positive and negative learning samples, as proposed by Jin Yang et al. [3]. Long short-term memory (LSTM) is used in this paper to automatically learn the characteristics of network intrusion behaviors. We provide a simple recurrent unit-based (SRU)-based model to get rid of this dependency and enable intrusion detection in real time. The suggested model in this research was validated through extensive tests on KDD'99 and NSL-KDD, two standard datasets for intrusion detection that are highly successful at distinguishing between legitimate and malicious network activity. On the KDD'99 dataset, it obtains 99.73% accuracy, and on the NSL-KDD dataset, 99.62% accuracy.

Data collection, feature selection/conversion, and decision engine are the three primary components of the paper by Gozde Karatas et al. [4] that surveyed deep learning-based intrusion detection system approaches. It is necessary to implement the system as anomaly detection with a learning system in order to increase the system's adaptability rather than using signature-based detection. In order to provide a concise overview of deep learning-based intrusion detection systems with an overview of many aspects of intrusion detection and deep learning algorithms, this study aims to do just that. This work also identifies and describes a few publicly accessible datasets, along with their strengths and weaknesses.

III. DATA SET AND PROCESSING

Data selection is required in order to train our models and assess their dependability throughout the testing phase. In the past, comprehensive datasets for Network Intrusion Detection Systems included KDD98, KDDCUP99, and NSLKDD (NIDS). Recent studies have revealed that these databases don't accurately represent contemporary network activity (normal and attack vectors). Therefore, we chose a few datasets that were recently made available to the public by researchers. These datasets included network data that had been labelled and created in labs using a virtual network architecture. If an effective data set is available, the datasets are a mix of real network traffic and fake botnet assault traffic. An intrusion detection system can only benefit from training and testing with a data set that contains a lot of high-quality data and simulates the crucial time.

It's possible that the NSL-KDD data set is an improved version of the KDD-99 data set. The NSL-KDD data set is examined in this report in order to determine how well different classification algorithms can identify anomalies in network traffic patterns. It can be suggested to use the NSL-KDD dataset to solve some of the underlying issues with the KDD'99 data. Due to this benefit, it is feasible to conduct the experiments on the full set without the need to pick a small sample at random. Additionally, the NSL-KDD train and test sets contain a reasonable number of records. Due to this benefit, it is feasible to conduct the experiments on the full set without the need to pick a small sample at random. As a result, evaluation findings from multiple research projects will be comparable and consistent.

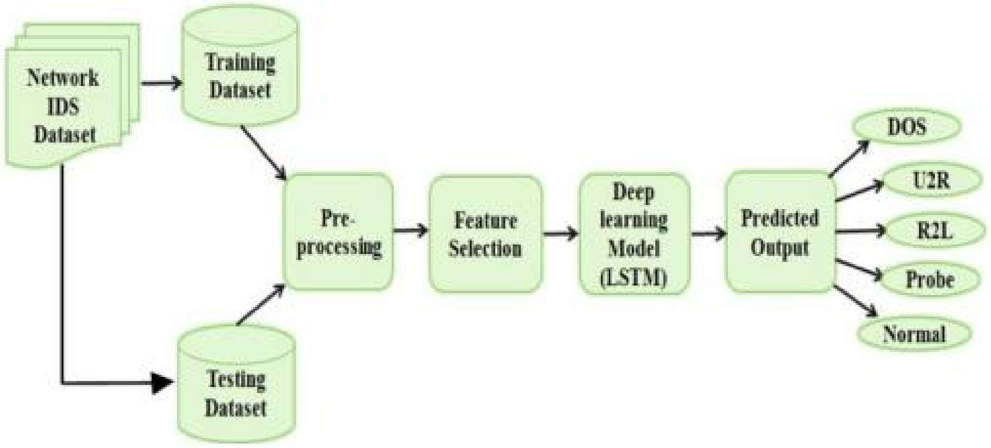

Fig 1: Proposed working model

IV. PROPOSED METHODOLOGY

For the purpose of detecting network intrusions, the article applied the deep learning LSTM method. This process involves numerous steps. The LSTM model is trained and tested using the NSL-KDD dataset. The Model was applied to two different output classification schemes. One uses binary classification to distinguish between legitimate and malicious data for testing. The second method is for multiclass data categorization, which produces five types of output, including DOS, U2R, R2L, Probe, and Normal data.

ISSN: 2366-1313

Training / Testing Dataset:

The LSTM model is trained and tested using the NSL-KDD train and NSL-KDD test dataset. It is separated into a 60-40 ratio, which means that 60% of the dataset is used for model training and 40% for model testing. Depending on the researcher and application, the ratio of instruction to testing may change.

Preprocessing:

The purpose of the pre-processing step is to create data that is useful for intrusion detection. The general activities, such as transforming the data into readable form and into another format, are the major emphasis of pre-processing. Taking data from the training dataset to model or test the data that is input data also eliminates redundant data from the dataset. The feature extraction process uses this data as input to choose features. To prevent confusion in learning and testing, some of this data that has no values in some columns will be removed.

Training values:

The amount of time needed for training or testing data is determined as the model's assessment time. The length of the assessment process for binary classification or multiclass classification depends on the system's specifications and parameters. Because deep learning requires the most recent specifications for better task executions. Therefore, the evaluation time for binary classification or testing is 8.28 seconds, and for multiclass classification it is 3.25 seconds.

Performance Statistical Measure: The values are derived from the confusion matrix, which is used to calculate various parameters. These variables are nothing more than the model's performance indicators. This section includes a binary classifier's performance metric, which contains values for both malicious and benign data.

ISSN: 2366-1313

Additionally, the Multiclass Classifier incorporates values for four distinct attack and baseline data.

Table-I gives parameters for Binary Classification

True Positive	13719
False Negative	99
True Negative	9711
False Positive	89
Accuracy	99.3656
Error Rate	0.6354

V. EXPERIMENTAL RESULT

The dataset was divided into 25% for validation and 75% for training. The training phase has 50 epochs totaling more than 5 hours. The validation phase for Stacked LSTM took 128 seconds with a processing speed of 0.2 ms/sample, whereas the validation phase for Bidirectional LSTM took 90 seconds with a processing speed of 0.14 ms/sample. Stacked LSTM had an accuracy of 96.60%, whereas Bidirectional LSTM had an accuracy of 96.41%.

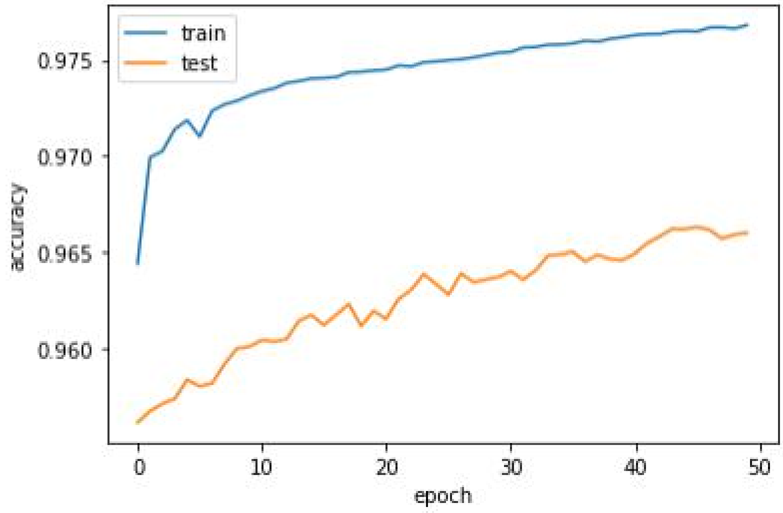

Fig. 2. Training vs.Validation accuracy

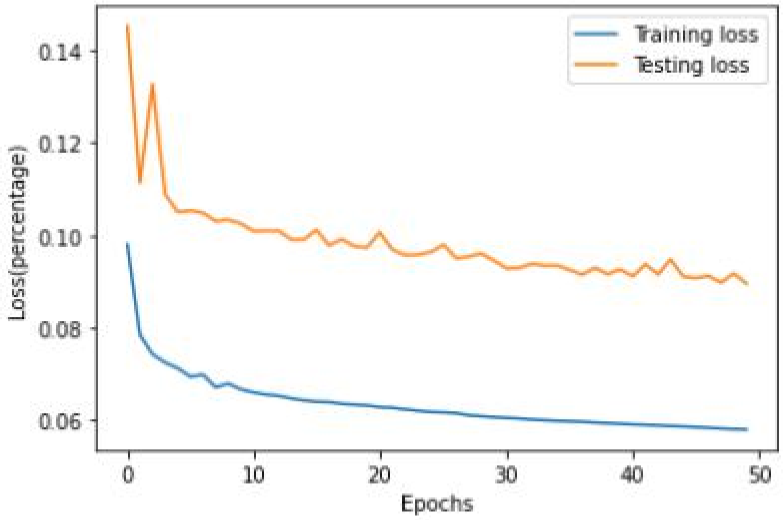

Fig 3: Training vs. Validation loss (BI-LSTM)

VI. CONCLUSION

In this study, a long short-term memory method based on anomaly detection was presented for intrusion detection in network security. The method includes binary classification for detection as well as multiclass classification. Four primary forms of attacks on multiclass categories are present in the NSL-KDD dataset. Using deep learning for intrusion detection can meet the need for very precise assault detection. In this study, multiclass classifier accuracy is 96.9% and binary classifier accuracy is 99.2%. Various parameters were calculated to assess the efficacy of the model for detecting intrusions, including sensitivity of 99.26%, specificity of 99.26%, and false positive rate of 0.97.

VII. REFERENCES

[1] Anish Halimaa A, Dr. K.Sundarakantham, "Machine Learning Based Intrusion Detection System", 2019. Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019).

[2] Mohammed Ishaque, Ladislav hudec, "Feature extraction using Deep Learning for Intrusion Detection System", IEEE 2019.

[3] Jin Yang, Tao Li, Gang Liang, Wenbo He and Yue Zhao, A Simple Recurrent Unit Model Based Intrusion Detection System with DCGAN, 2019 IEEE.

[4] Felipe de Almeida Florencio, Edward David Moreno, Hendrik Teixeira Macedo, Ricardo J. P. de Britto Salgueiro, Filipe Barreto do Nascimento, Flavio Arthur Oliveira Santos, Intrusion Detection via MLP Neural Network using an Arduino Embedded System, 2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC).

[5] Alex Shenfield, David Day, Aladdin Ayesh, Intelligent intrusion detection systems using artificial neural networks, A. Shenfield et al. / ICT Express 4 (2018).

[6] Gozde Karatas, Onder Demir, Ozgur Koray Sahingoz, Deep Learning in Intrusion Detection Systems, International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) 2018.

[7] Dimitar Nikolov, Iliyan Kordev, Stela Stefanova, Concept for network intrusion detection system based on recurrent neural network classifier, International Scientific Conference Electronics - ET2018.

[8] Lee, Brian; Amaresh, Sandhya; Green, Clifford; and Engels, Daniel, Comparative Study of Deep Learning Models for Network Intrusion Detection, SMU Data Science Review: Vol. 1: No. 1, Article 8 (2018).

[9] Nathan Shone , Tran Nguyen Ngoc, Vu Dinh Phai , and Qi Shi, Deep Learning Approach to Network Intrusion Detection, IEEE Transaction on Emerging Topics in Computational Intelligence, VOL. 2, NO. 1, February 2018.

[10] Leila Mohammadpour, Teck Chaw Ling, Chee Sun Liew and Chun Yong Chong, A Convolutional Neural Network for Network Intrusion Detection System, Proceedings of the APAN – Research Workshop 2018.

[11] Nenekazi N. P. Mkuzangwe avd Fulufhelo Nelwamondo, Ensemble of Classifiers Based Network Intrusion Detection System Performance Bound, The 2017 4th International Conference on Systems and Informatics (ICSAI) 2017.

[12] Fernando M. de Almeida, Admilson de R. L. Ribeiro, Edward D. Moreno, Carlos A. E. Montesco, Performance Evaluation of an Artificial Neural Network Multilayer Perceptron with Limited Weights for Detecting Denial of Service Attack on Internet of Things, The Twelfth Advanced International Conference on Telecommunications (AICT) 2016.

[13] Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam, A Deep Learning Approach for Network Intrusion Detection System, (ICST) 2016.

[14] Leila Mohammadpour, Teck Chaw Ling, Chee Sun Liew, and Chun Yong Chong, A Convolutional Neural Network for Network Intrusion Detection System, Proceedings of the APAN – Research Workshop 2018 ISBN 978-4-9905448-8-1,2018.

[15] K.Q.Yan,S.C.Wang,C.W.Liu, A Hybrid intrusion Detection System of Cluster-based Wireless Sensor Networks, Proceedings of the International MultiConference of engineers and Computer Scientists 2009 Vol 1 IMECS 2009, March 18-20,2009.