IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10710

# PACKET INSPECTION TO IDENTIFY NETWORK LAYER ATTACKS

**Sarvesh Ganesh Hegde[1], H.P.Mohan Kumar [2]**

Dept. of MCA, P.E.S College of Engineering, Mandya, Karnataka-571401, India[1]

Dept. of MCA, P.E.S College of Engineering, Mandya, Karnataka-571401, India[2]

**Abstract:** In the recent years, the usage of internet is at its peak. As the usage of internet increases the number of people who will try to make money in an easy way through the growing internet also increases. In order to do achieve this the attacks on the user's computer system happens so that the hackers can collect the user's data and can be used for various purposes. Such attacks take place just by inserting the spoofed packets into the user's line of communication in the network. To prevent this type of attacks bifurcation of the incoming and outgoing packets from a system's network can be an accurate solution. To achieve such bifurcation between the normal packets and spoofed packets the model is developed using Deep Learning algorithm. By using the Deep Learning algorithm Long Short-Term Memory the user can obtain a comparatively higher accuracy.

**Keywords:** Deep Learning, Long Short-Term Memory, LSTM, Packets, Attack, Network

## 1. INTRODUCTION

As the internet is growing it is providing many convenient and revolutionary services to its users. But the users also facing many security issues in the internet. The attacks may be in the form of Denial of Service, Probe, User to Root attack or Root to Local attack. And these attacks can be prevented by finding out which packets are being used to initiate the attacks and alerting the user about the same. In order to perform this differentiation, there are multiple models are there most of them are developed by using the machine learning algorithms such as K-means, SVM, Naive Bayes, ANN, CNN etc.

The proposed model is developed by using the Deep Learning algorithm called Long Short-Term Memory or LSTM. The LSTM algorithm is used to classify the normal packets and the packets that contains the harmful contents in it which may affect the computer system. And the nature of those packets can be identified by using the payload of the packet.

## 2. RELATED WORKS

" An Incremental Learning Method Based on Dynamic Ensemble RVM for Intrusion Detection", journal paper published by Zhijun Wu, Pan Gao, Lei Cui have used the DEIL-RVM algorithm to develop their intrusion detection system with the average accuracy of 80.[1]

"Improving the Intrusion Detection using Discriminative Machine Learning Approach and Improve the Time Complexity by Data Mining Feature Selection Methods", was proposed by Karan Bajaj and Amit Arora have explained about the various types of approaches used for different model and they have compared those models. And they have used feature selection concept in order to increase the accuracy of the same models.[2]

" Decision Tree: A Machine Learning for Intrusion Detection" by Shilpashree. S, S. C. Lingareddy, Nayana G Bhat, Sunil Kumar G. They used Decision Tree to solve the problem of Intrusion but they have used KDDCUP99 dataset which is an older version which has many drawbacks in it.[3]

"Network Intrusion Detection By SVM & ANN With Feature Selection" proposed by B. VenkataRamana, K Chandra Mouli, Aileni Eenaja they have used the SVM and ANN algorithm to build their model which provides an average accuracy of 88.[4]

"Decision Tree Based Algorithm for Intrusion Detection" by Kajal Rai, M. Syamala Devi developed their model using Decision Tree Algorithm.[5]

"An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic", published by Xiaoxuan Zhang, Jing Ran, Jize Mi have used CNN algorithm to develop their model the main drawback of this model is that the algorithm is mostly used and optimized for image classification so it will be less efficient to use it for packet classification. The model has achieved 83.31% accuracy which is comparatively less.[6]

"Intrusion Detection System Using Recurrent Neural Networks and Attention Mechanism", published by Praveen Kumar Kollu, R. Satya Prasad have used RNN algorithm to obtain intrusion detection system.[7]

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10710

"Intrusion detection system using K-Means based on Cuckoo search optimization" by M. Deepa, Dr. P. Sumitra the model is developed by using the K-Means machine learning algorithm.[8]

"Feature Dependent Naive Bayes For Network Intrusion Detection System" proposed by Panny Agustia Rahayuningsih, Reza Maulana, Windi Irmayani, Dedi Saputra, Deasy Purwaningtias the model is developed by using the Naïve Bayes machine learning algorithm.[9]

"Intrusion Detection System Using Ensemble of Rule Learners and First Search Algorithm as Feature Selectors" published by D P Gaikwad the model is developed by using Novel Ensemble classifier [10]

"Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach" by Jabez, Dr.B.Muthukumar was developed by using the Outlier detection method using which the difference between the original packets and spoofed packets can be found out.[11]

Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan have proposed a work "Intrusion Detection System" which is a survey on different intrusion detection systems. [12]

"Intrusion Detection System using Random Forest" published by Saurabh Kumar, Joy Pal, Abhijeet Giri, Aditya Raj, Ritu Raj, Mangayarkarasi R. They have used Random forest algorithm to perform intrusion detection process.[13]

"Intrusion detection system combined enhanced random forest with SMOTE algorithm" published by Tao Wu, Honghui Fan, Hongjin Zhu, Congzhe You, Hongyan Zhou and Xianzhen Hua. They have combined the random forest algorithm with the SMOTE algorithm to obtain more accuracy and efficiency in intrusion detection.[14]

"Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms" by Mehrnaz Mazini, Babak Shirazi, Iraj Mahdavi was developed by using the combination of bee colony and AdaBoost algorithms.[15]

## 3. METHODOLOGY

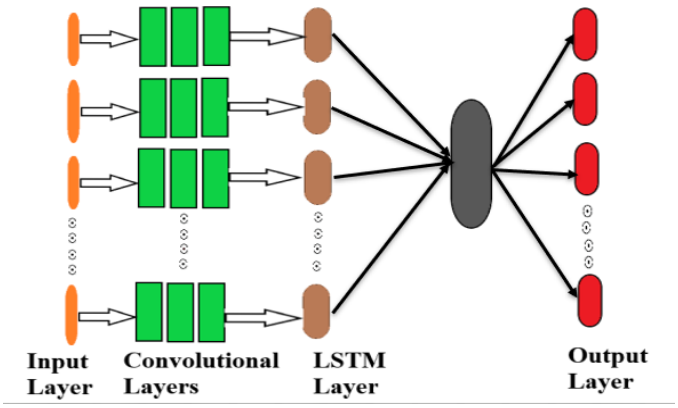
### I.Dataset

NSL-KDD is one of the most used datasets for packet differentiation in different domains. The dataset contains the packets used for Denial of Service, Probe, User to Root and Root to Local types of attacks in which each record is labelled as normal or not. This dataset is the updated version of KDD'99 in which the problem of data redundancy is eliminated. NSL-KDD contains both training and testing data, which is the basic necessity of a model. The testing dataset is loaded into the model once the model is built.

### II.Normalization

Once the dataset is loaded to the model the records which are not required, they may be a null record or any faulty records will be removed in normalization process. This operation can be done by just clicking a button in the UI.

## III.SYSTEM ARCHITECTURE




## IV.MODEL TRAINING

Both a forward run and a reverse pass are used while training the proposed system. Reverse Propagation The LSTM layer and attention layer make up the majority of the model; every layer has a distinct structure and, as a result, a different function within the overall framework. The attention layer receives the forward propagation from the LSTM layer. The processing of the prior model yields the input for the current model. After the complete forward propagating, the final identification result is acquired.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10710

**V.LSTM Layer**

The context information of the data may be efficiently used by BLSTM to learn features from the time series data made up of traffic bytes. The time series feature in the data packet is learned using the BLSTM. Each data packet's traffic bytes are sequentially entered into a BLSTM, which produces a Long Short-Term Memory. The forward LSTM and backward LSTM models are connected using the BLSTM model to retrieve coarse-grained information. By comparing the inner memory cell C when new information is received, the input gate I the forget gate f, and the output gate o of the LSTM are created to regulate how to replace the information.

According to pertinent criteria, we can determine if data entering an LSTM network is valuable. Only data that passes algorithmic authentication will be kept, while data that doesn't will be erased through a forget gate. Considering the hidden layers of a Bidirectional LSTM layer and an incoming sequence x at period t.

## 4. IMPLEMENTATION

The proposed system is developed by using the Deep Learning algorithm called Long Short-Term Memory which is an improved version of RNN algorithm. The model is trained and tested by using the NSL-KDD dataset an upgraded version of KDDCUP99 dataset. This upgraded version is used to train and test the model because of the drawbacks of previous version of the dataset. The dataset is created by Canadian Institute for Cybersecurity which contains both normal packets as well as spoofed packets.

The proposed system has the User Interface which is created by using the tkinter package which is a standard Python Interface toolkit. Through this interface the user can interact with the built model and perform the necessary actions to obtain the output which is required.

The model accepts the dataset which contains the testing data. Once the user uploads the testing dataset the model normalizes the dataset with a single click on the button given in the UI. After the normalization of data in the dataset if the user needs, he can build the Sequential neural network to perform the packet classification in order to compare it with LSTM algorithm classification. Once the model is built the UI automatically provides the confusion matrix of the model. Then the user can go for the process of testing the data using LSTM algorithm with a single click. When the data is classified using LSTM algorithm the user can see the confusion matrix of the same. Once the execution of both algorithms completed the user can click on a given button in order to view the comparison between both the algorithms through a plotted chart.

## 5. RESULT AND ANALYSIS

The model [1] gave the accuracy of Highest 85.47 %. The model [2] gave the highest accuracy of 82%. The proposed [4] model gave 82.34% of accuracy using SVM model and 94.02% of accuracy using ANN model. [5] gave highest accuracy of 80%. The model [6] gave the accuracy of 83.31%. The model [14] has given 78.47% of accuracy on the test data.

The highest accuracy of proposed LSTM model is 95.42 when it was trained on 20000 records and validated on 4000 records with the Validation loss of 8.59. F1 score of 95.15, Precision of 95.64 was obtained from the proposed model. The model provides higher accuracy than most of the existing systems. The model is developed using the LSTM algorithm which is more suitable for packet classification than most of the other algorithms. The model can use the dataset to the fullest which provides more accuracy in the output. The used dataset is NSL-KDD which has a large number of packets through which the model can be trained and tested in an efficient way. Interaction between the user and model is made easier through the UI so there is no need for the user to do any extra tasks. Same system allows the user to compare between the algorithms which helps the user to choose the best.

## 6. CONCLUSION

Security in the Internet has become the need of the day. To secure the privacy, to avoid the important files falling into wrong hands, to avoid the internal damage of the electronic devices which can use the Internet for their communication the Intrusion Detection System is a must. So, in this research paper we have proposed a system which can perform such detection mechanism with more accuracy. Which can provide higher security to not only computer systems but also to the IOT devices which can be accessed over internet if implemented. The model can be upgraded as per the technology evolves so that it will be up to date. Model has to be trained and tested with the real time packets frequently. The proposed model can be implemented in the real time applications to avoid the possible internet threats.

DOI: 10.17148/IJIREEICE.2022.10710

## REFERENCES

[1] Zhijun Wu, Pan Gao, Lei Cui" An Incremental Learning Method Based on Dynamic Ensemble RVM for Intrusion Detection" IEEE transactions on network and service management, VOL. 19, NO. 1, March 2022

[2] Karan Bajaj and Amit Arora "Improving the Intrusion Detection using Discriminative Machine Learning Approach and Improve the Time Complexity by Data Mining Feature Selection Methods", International Journal of Computer Applications (0975 – 8887) Volume 76– No.1 August

[3] Shilpashree. S, S. C. Lingareddy, Nayana G Bhat, Sunil Kumar G" Decision Tree: A Machine Learning for Intrusion Detection" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue- 6S4, April 2019

[4] B. VenkataRamana, K Chandra Mouli, Aileni Eenaja "Network Intrusion Detection By SVM & ANN With Feature Selection" 2020 IJCRT | Volume 8, Issue 6 June 2020 | ISSN: 2320-2882

[5] Kajal Rai, M. Syamala Devi "Decision Tree Based Algorithm for Intrusion Detection" Int. J. Advanced Networking and Applications Volume: 07 Issue: 04 Pages: 2828-2834 (2016) ISSN: 0975-0290

[6] Xiaoxuan Zhang, Jing Ran, Jize Mi "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic" 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)

[7] Praveen Kumar Kollu, R. Satya Prasad "Intrusion Detection System Using Recurrent Neural Networks and Attention Mechanism" Volume 7, No. 8 August 2019 International Journal of Emerging Trends in Engineering Research

[8] M. Deepa, Dr. P. Sumitra, "Intrusion detection system using K-Means based on Cuckoo search optimization" IOP Conf. Series: Materials Science and Engineering 993 (2020) 012049 doi:10.1088/1757-899X/993/1/012049

[9] Panny Agustia Rahayuningsih, Reza Maulana, Windi Irmayani, Dedi Saputra, Deasy Purwaningtias, "Feature Dependent Naive Bayes For Network Intrusion Detection System". Journal of Physics: Conference Series 1641 (2020) 012023 doi:10.1088/1742-6596/1641/1/012023.

[10] D P Gaikwad "Intrusion Detection System Using Ensemble of Rule Learners and First Search Algorithm as Feature Selectors" I. J. Computer Network and Information Security, 2021, 4, 26-34 Published Online August 2021 in MECS DOI: 10.5815/ijcnis.2021.04.03

[11] Jabez, Dr.B.Muthukumar "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach" Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.191

[12] Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan "Intrusion Detection System" International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com, Volume 5, Issue 2 (March – April 2017), PP.38-44.

[13] Saurabh Kumar, Joy Pal, Abhijeet Giri, Aditya Raj, Ritu Raj, Mangayarkarasi R "Intrusion Detection System using Random Forest" 2019

[14] Tao Wu, Honghui Fan, Hongjin Zhu, Congzhe You, Hongyan Zhou and Xianzhen Hua
"Intrusion detection system combined enhanced random forest with SMOTE algorithm". EURASIP Journal on Advances in Signal Processing(2022)2022:39 doi.org/ 10.1186/ s13634-022-00871-6

[15] Mehrnaz Mazini, Babak Shirazi, Iraj Mahdavi "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms" doi.org/10.1016/j.jksuci.2018.03.0111319-1578/ 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.