International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Network Intrusion Detection System

[1]Rashmika. R, [2]Sujithra. M

[1]Department of Computing, Coimbatore Institute of Technology, Coimbatore, India
[2]Assistant Professor, Department of Computing, Coimbatore Institute of Technology, Coimbatore, India

ABSTRACT—

Intrusion detection system (IDS) has become an essential layer in all the latest ICT system due to an urge towards cyber safety in the day-to-day world. Reasons including uncertainty in finding the types of attacks and increased the complexity of advanced cyber attacks. In this project , Deep Learning models have been utilized to predict the attacks on Network Intrusion Detection System (N-IDS). The models are Linear Discriminant Analysis , Multi layer perceptron and Auto encoder . KDDCup-'99' dataset has been used for training and bench- marking the network. The results were compared and concluded that MLP classifier has superior performance over all the other algorithms.

***Index Terms*—Intrusion detection, deep learning , multi layer perceptron**

1. INTRODUCTION

In the modern world, the fast-paced technological advancements have encouraged every organization to adopt the integration of information and communication technology (ICT). Hence creating an environment where every action is routed through that system making the organization vulnerable if the security of the ICT system is compromised. Therefore, this call for a multilayered detection and protection scheme that can handle truly novel attacks on the system as well as able autonomously adapt to the new data.

Intrusion Detect Systems (IDSs) are a range of cybersecurity based technology initially developed to detect vulnerabilities and exploits against a target host. The sole use of the IDS is to detect threats. Therefore it is located out-of-band on the infrastructure of the network and is not in the actual real-time communication passage between the sender and receiver of data. Instead, they solutions will often make use of a TAP or SPAN ports to analyze the inline traffic stream's copy and will try to predict the attack based on a previously trained algorithm, hence making the need of a human intervention trivial.

Therefore it becomes obvious that Deep Learning and IDSs, when combined together, can work at a superhuman level. Also, since the IDSs are out-of-band on the infrastructure, common attacks like DoS which primarily aims at choking the network band to gain access of the host, cannot bottleneck the performance of it, hence this security layer cannot tamper with ease.

2. ENVIRONMENT

2.1 ANACONDA:

Anaconda is a free open source distribution environment using Python and R programming languages for large-scale data processing, predictive analytics and scientific computing that mainly aims to simplify package management and deployment. Package versions are managed by the package management system.

2.2 JUPYTER NOTEBOOK :

In Anaconda environment it is easy to install python, the jupyter notebook and spyder is mainly used to run python programs and other commonly used packages for scientific computing and data science . Jupyter notebook runs code in many programming languages , but python is mainly used for the requirement of installing the jupyter notebook . It can be executed on a local desktop, requiring no internet access or can be installed on a remote server and accessed through the internet.

3. DATASET DESCRIPTION

The DARPA's ID evaluation group, accumulated network based data of IDS by simulation of an air force base LAN by over 1000s of UNIX nodes and for continuously 9 weeks, 100s of users at a given time in Lincoln Labs which was then divided into 7 and 2 weeks of training and testing respectively to extract the raw dump data TCP. MIT's lab with extensive financial support from DARPA and AFRL, used Windows and UNIX nodes for almost all of the inbound intrusions from an alienated LAN unlike other OS nodes. For the purpose of dataset, 7 distinct scenarios and 32 distinct attacks which totals up to 300 attacks were simulated.

Since the year of release of KDD-'99' dataset, it is the most vastly utilized data for evaluating several IDSs. This dataset is grouped together by almost 4,900,000 individual connections which includes a feature count of 41. The simulated attacks were categorized broadly as given below :

- **Denial-of-Service-Attack (DoS):** Intrusion where a per- son aims to make a host inaccessible to its actual purpose by briefly or sometimes permanently disrupting services by flooding the target machine with enormous amounts of requests and hence overloading the host [35].
- **User-to-Root-Attack (U2R):** A category of commonly used maneuver by the perpetrator start by trying to gain access to a user's pre-existing access and exploiting the holes to obtain root control.
- **Remote-to-Local-Attack (R2L):** The intrusion in which the attacker can send data packets to the target but has no user account on that machine itself, tries to exploit one vulnerability to obtain local access cloaking themselves as the existing user of the target machine.
- **Probing-Attack:** The type in which the perpetrator tries to gather information about the computers of the network and the ultimate aim for doing so is to get past the firewall and gaining root access.

KDDCup-'99' set is classified into the following three groups: Basic features: Attributes obtained from a connection of TCP/IP comes from this group. Majority of these features results in implicitly delaying the detection. Traffic features: Features computed w.r.t. a window of time is categorized under this group. This can be further subdivided into 2 groups:

- **"Same host" features:** The connections that has identical end host as the connection under consideration for the continuously 2 seconds fall into this category and serves the purpose of calculating the statistics of protocol behaviour, etc.
- **"Same service" features:** The connections that are only having identical services to the present connection for the last two seconds fall under this category.
- **Content features:** Generally probing attacks and DoS attacks have at least some kind of frequent sequential intrusion patterns unlike R2L and U2R attacks. This is due to the reason that they involve multiple connections to a single set of a host(s) under short span of time while the other 2 intrusions are integrated into the packets of data partitions in which generally only one connection is involved. For the detection of these types of attacks, we need some unique features by which we will be able to search for some irregular behaviour. These are called content features.

NSL-KDD	Total	Normal	Dos	Probe	R2L	U2R
KDD train+	125973	67343	45927	11656	995	52
KDD test+	18793	9710	5741	1106	2199	37

Table 1: Details of the NSL-KDD dataset

4. METHODOLOGY

Firstly, the NSL - KDD dataset is cleaned from outliers and min-max normalization technique is used to scale data within the range 0 and 1. Afterwards, the one-hot-encoding is applied to convert symbolic (or categorical) features into numeric values. Then, the 38 numeric attributes are analyzed statistically in order to select the most correlated features. Finally, shallow MLP, and deep AE, LSTM networks are developed to measure the detection performance both in binary and multi-classification scenario.

4.1 DATA PREPROCESSING

The proposed preprocessing stage arranges data to be proccessed by the next modules properly. It includes three units: outliers analysis , data normalization and one-hot encoding. Outliers analysis The NSL-KDD dataset is filtered from inconsistent values (outliers) as it has proven to be an important operation before data normalization. Indeed, outliers can interfere with the learning process causing miss detection in the proposed intrusion systems. Here, the outliers are identified using the Median Absolute Deviation Estimator (MADE).

4.2 ONE-HOT-ENCODING :

The three categorical features protocol type, service, flag (z2, z3, z4, respectively) were transformed into numerical values using the one-hot-encoding technique. Specifically, each categorical attribute is represented by binary values.

For example, the z2 feature (protocol type) has three attributes: tcp, udp and icmp. Applying the one-hot-encoding technique they were converted into binary vectors: [1,0,0],[0,1,0],[0,0,1], respectively. Similarly, also z3 and z4 features (service and flag) were converted into one-hot-encoding vectors. Overall, the 41- dimensional features were mapped into 122-dimensional features (38 continuous and 84 with binary values related to the features z2, z3, z4).

4.3 FEATURE EXTRACTION :

This processing module extracts the most correlated features. For each continuous feature, the percentage of zeros is evaluated both for KDD Train+ and KDDTest set.. In this work, feature vectors with number of zeros higher than 80% are excluded from subsequent elaborations. Specifically, 20 variables are discarded; whereas, the remaining 18 continuous features are combined with 84 one-hot-encoding vectors for a grand total of 102-dimensional features vector. Such vector is the input of the proposed classifiers.

5. DEEP LEARNING MODELS

5.1 MLP CLASSIFIER:

MLP is a feed-forward neural network and uses supervising learning algorithm for training . It is to be noted that, for fair comparison, MLP and AE architectures have the same structure. Indeed, the MLP classifier consists of one hidden layer with 50 neurons and a softmax output layer for classification tasks.

5.2 LDA CLASSIFIER:

DA is a statistical method typically used in machine learning. The goal of DA is to reduce the dimensionality and keep good separability among classes. Specifically, it projects the data samples onto a lower-dimensional space so that the class-separability is maximum and the dispersion of the samples belonging to the same class is minimum.

In this study, a discriminant classifier with linear function (LDA) is implemented.

5.3 AUTO ENCODER :

An AE architecture consists of an encoder and decoder operation: first, it transforms the input data vector into a typically lower representation (encoder); then, it attempts to reconstruct the original input from the compressed vector (decoder). The AE is trained in unsupervised fashion and is able to capture significant features from unlabeled data .

6. CONCLUSION

The strengths and effectiveness of the proposed IDS were evaluated using standard measurements including precision, recall, F1 score and accuracy. The most correlated features were extracted through statistical analysis which were used as input to AE, MLP and LDA. Moreover, both the binary (Normal vs Abnomal) and multi-classification (Normal vs Dos vs R2L vs Probe) were performed. The experimental results showed that the MLP classifier achieved the best performances for both binary (83.15% accuracy) and multi-class discrimination (83.65% accuracy), as compared with AE and LDA classifiers.

REFERENCES

[1] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelffl´e, Vision and challenges for realising the internet of things, Cluster of European Research Projects on the Internet of Things, European Commision 3 (3) (2010) 34–36.

[2] S. Goel, K. Williams, E. Dincelli, Got phished? internet security and human vulnerability, Journal of the Association for Information Systems 18 (1) (2017) 22.

[3] https://www.sciencedirect.com/science/article/pii/S0925231219315759