Intrusion Detection and Prevention System Using Deep Learning

Akhil Krishna
Computer Science and Engineering
Saintgits college of Engineering
Kerala, India
akhil.krishna1620@saintgits.org

Ashik Lal M A
Computer Science and Engineering
Saintgits college of Engineering
Kerala, India
ashik.lal1620@saintgits.org

Athul Joe Mathewkutty
Computer Science and Engineering
Saintgits college of Engineering
Kerala, India
athul.joe1620@saintgits.org

Dhanya Sarah Jacob
Computer Science and Engineering
Saintgits college of Engineering
Kerala, India
dhanya.sarah1620@saintgits.org

Hari M
Assistant Professor
Computer Science and Engineering
Saintgits college of Engineering
Kerala, India
hari.m@saintgits.org

Abstract- As technology is developing day by day and the number of networked digital devices is increasing manifold, the number of intruders and the type of attacks are also increasing. So there arises a need to detect and prevent these attacks. Hence this work is focused to implement an Intrusion detection and prevention system using Deep Learning that can immediately detect the attacks such as DOS, Probe, R2L and U2R and prevent the same. The intrusion when arises is detected using a Deep Learning model called Multi-Layer Perceptron trained by the dataset kddcup99 with high accuracy. Appropriate data from network is captured and it is stored as a csv file and is fed to the implemented Deep learning model to predict the attack in a real time manner, thus detection is achieved. In second phase, the intrusion is prevented using a script that runs in the background. The script is developed to perform the prevention phase by taking appropriate decision on the different prevention function to be performed for different types of attacks. The decision can be made by using the data from the classification part achieved through the Multi-Layer Perceptron model. In this paper both the separate Intrusion Detection System and the Intrusion Prevention system are combined as a single system to achieve the aim of intrusion detection and prevention tasks in a faster and efficient manner.

Keywords: Deep Learning; Intrusion Detection System; MLP; Prevention; Network.

1. INTRODUCTION

Intrusion Detection and Prevention System (IDPS) is defined as a system or software application that monitors network and/or system activity and determines if any malicious activity occurs and thus generates an immediate response to it. As stated that Information is wealth so, the hackers use various forms of attacks to gain useful information[15]. Many of the attacks can be detected using intrusion detection techniques and their prevention will create a blocking effect for Intrusions. The key aspect is to provide a comprehensive analysis on intrusion detection, intrusion forms and their detection and to establish an immediate response to intrusions, challenges and finally to build the IDPS Research Tool, which will be able to detect and prevent intrusions from intruders.

Over the past few years, as the development and proliferation of infinite communication paradigm and massive increase in the number of networked digital devices, there is considerable concern about cyber security that attempts to maintain the system's information and communication technology. Attackers identify and create new attacks on a daily basis, so attacks need to be correctly detected by the intrusion detection systems (IDSs) and appropriate responses should be provided, that are the primary objective of IDPS .IDSs, which play a very important role in network security, comprise three main components: data collection, feature selection/conversion and decision engine.

Deep learning offers low training time and a high accuracy rate with distinctive learning method for using Big Data. As a result, use of IDPS systems has started. The aim of this paper is to research in-deep learning-based intrusion detection and prevention approach through comparative literature work and by giving a better understanding of IDSs or in the deep learning algorithms.

Earlier, developers were using different machine learning algorithms to classify and distinguish anomaly traffic from normal traffic without prior knowledge of the attack pattern. Extensive research on machine learning recently made a major breakthrough in imitating the human brain.

The breakthrough in machine learning comes from deep learning that has been expected to bring about a significant change in artificial intelligence field and if both cyber security and deep learning are integrated it can give us phenomenal results. Earlier researchers adopted various machine learning approaches to detect as well as prevent threats.

2. RELATED WORKS

Some projects related to Intrusion Detection and Prevention System in various fields was studied. Several ideas and technologies related to the fields were understood and tried to utilize those concepts in this paper.

One technology uses both static detection and dynamic detection methods for malware detection. This uses an ensemble learning approach that blends software and hardware features, extracts malware call sequence APIs, hardware output counters, and memory dump as detector features, and constructs various forms of feature vectors. Whereby the software features compensate for the lack of precision in hardware detection features and those software compensation features are vulnerable to evasion. An existing neural network with excellent detection performance is used as a detector [1]. In another one honeypots are installed within the programs of the firewall. Whatever is assigned as a honeypot, its aim is to test, attack and possibly misuse the system. Instead of evasion, the honeypot is a response and detection tool. After doing so, the defenders will respond to this confirmation by building better resistance against future security threats and counter measures [2]. When referred with yet another technology it was studied that they collect and use information from recognized attacks by using IDS and figure out if someone is attempting to attack the network / host. The model they used is a hybrid model for cloud infrastructure intrusion detection and prevention [3]. Another technology uses both network-based and host-based IDPS as a hybrid intrusion detection and prevention system to help detect maximum network attacks and can detect all signature-based network attacks, anomaly-based network attacks and configuration rules for different host operating systems. This system also handles types of attacks known and unknown [4]. Description about another system uses intrusion-based network approach. In this system they allocate part of the network to a database node. To send some data to any node in the network first send it to the server and then the server will redirect the data to their original destination. To detect an intrusion, the client has the system installed in it. So, if it is an intrusion, the server will detect it and discard the information. Otherwise, the checked data will be sent to the node of destination [5].

3. OBJECTIVE

The main challenge of the 21st century which uses technology at its peak level is to ensure its cyber security. Day by day new attackers and new types of attacks through the exploitation of vulnerability is sprouting. Through these types of attacks, untold miseries may occur to the organization, personal devices, systems etc. It is necessary to protect them from such attacks by ensuring the integrity and confidentiality of the data. For that, innovative methodology is required. The objective of this paper is to build network security software that tracks malicious activities in network or system and protects any organization, personal devices; system etc. from a subset of attacks namely DOS, R2L, U2R and probe. The attacks are detected using the Intrusion Detection System obtained from Multi-Layer Perceptron Deep Learning model trained using KDDCup99 dataset. The malicious activity is blocked using the Intrusion Prevention System acquired from a script.

In a nutshell the system aims to catch the attack features as soon as it comes to the system and detect corresponding attack and then perform prevention and thus ensuring cyber security to the system as a whole. The main functions are spotting, collection, reporting, planning to block or stop the malicious activities. Intrusion Prevention System is the augmentation to Intrusion Detection System and both are blended to single software in this paper. Through the software one will be able to use his devices without having the fear of being attacked by intruders and will also be able to protect his privacy.

4. METHODOLOGY

The entire IDPS system architecture comprises of two different phases namely the detection phase and prevention phase.

In the detection phase a deep learning model is created for detecting intrusions and any possible threats that may encounter in our network, this is done with a sequence of steps which make our model with maximum possible accuracy and negligible loss. The IDS phase first starts with the suitable data set collection, here KDDCup99 dataset. The dataset collection is followed by preprocessing using One Hot Encoding, in which (one-of-K) is used to transform all categorical features into binary features which is proceeded with feature scaling to standardize the independent features present within a fixed range, here the values are scaled with the distribution centered at 0 with a standard deviation of 1.Now the input data is ready to be fed for creation of a pre-trained model using Multi-Layer Perceptron consisting of 2 dense layers with Relu and Softmax activation functions, and this model is tested with the testing data made to run at specific number of epochs and this marks the end of detection phase. The real time testing of data is done using wire shark, in which data is stored as a csv file and then fed into the developed high accuracy Multi-Layer Perceptron model and intrusions are detected. IDS in figure 1 explain this process.

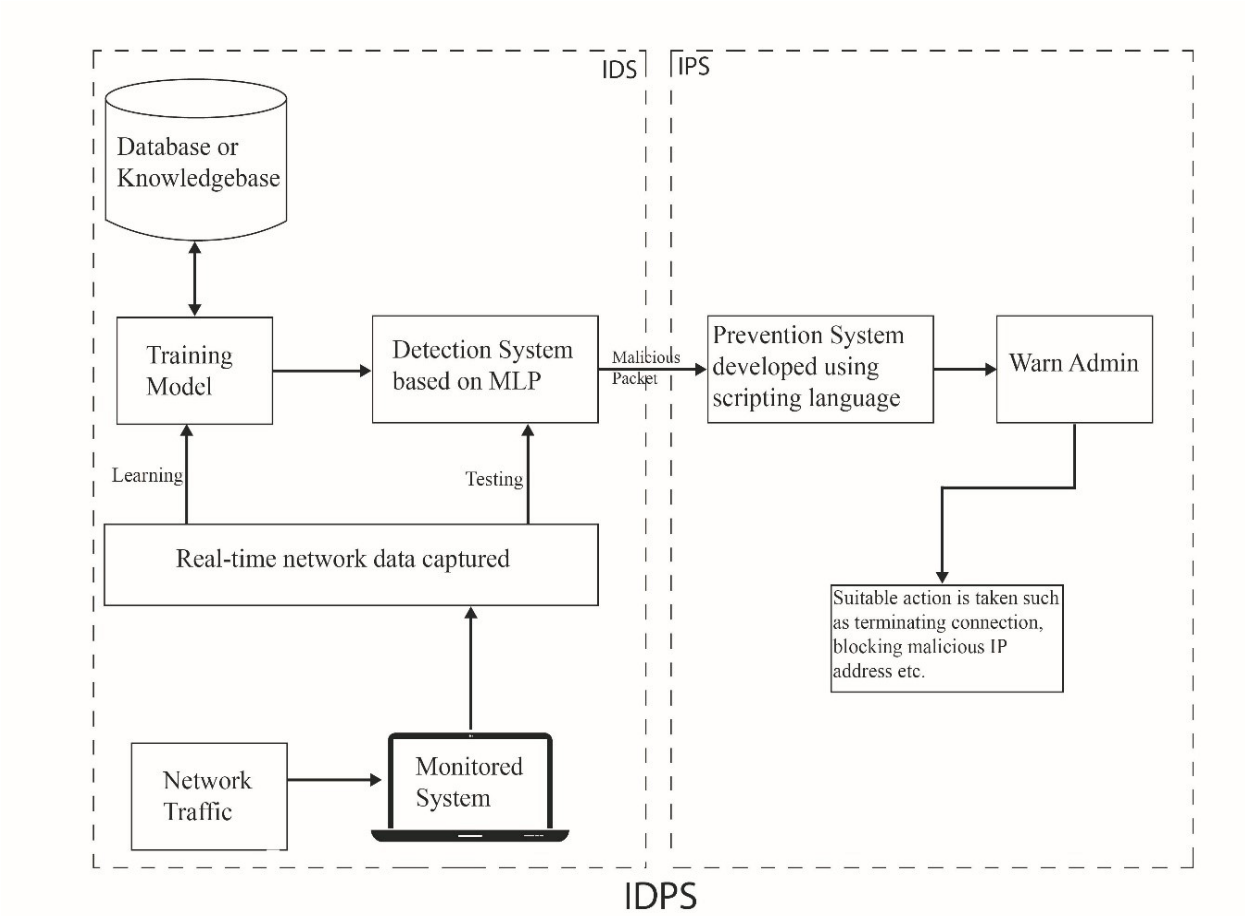

IDS
IPS
Database or Knowledgebase
Training Model
Detection System based on MLP
Malicious Packet
Prevention System developed using scripting language
Warn Admin
Learning
Testing
Real-time network data captured
Suitable action is taken such as terminating connection, blocking malicious IP address etc.
Network Traffic
Monitored System
IDPS

Figure 1 Intrusion Detection and Prevention System Architecture

In the second phase the intrusion is prevented using a script that runs in the background, using all the admin privileges. The script is developed in such a manner that it prevents any malicious requests such as those of DOS attack, by terminating the connection and informing the admin about the occurrence of the malicious event and this sets the top of prevention phase. Both the detection and prevention phase is integrated and deployed as software. This work aims to detect only the attacks such as DOS, U2R, R2L, probe and prevents the same. IPS in figure 1 explains this process.

4.1 Intrusion Detection System (IDS)

Deep learning may be defined as a special sort of technique in machine learning for the extraction of features, better learning, and perception of machines. Deep learning uses multiple consecutive layers for their algorithmic operations. The layers are connected in an interlinked fashion where each layer receives input as the output of the previous layer. This is an efficient algorithmic usage with excellent advantage for the hierarchical extraction of features that are best in representing data rather than features that are manual in deep learning aspects [14]. It uses specified architectures of Artificial Neural Network namely Multilayer perceptron. Convolutional Neural Networks, Recurrent Neural Networks etc.

Here, the system uses Multi-Layer Perceptron. It is a type of neural network that constitutes of one or more layers of neurons. Data is fed to the input layer, it's going to contain one or more hidden layers providing levels of abstraction, and predictions are made on the output layer, also called the visible layer. A multilayer perceptron (MLP) may be a class of feed forward artificial neural network.

A MLP contains a total of three node layers: an input layer, a hidden layer, and an output layer. Besides the input nodes, each node may be a neuron using a nonlinear activation function. MLP uses a guided learning method for teaching which is called back propagation. The multiple layers and nonlinear activation distinguish MLP from a linear perceptron [9]. It can distinguish data that's not linearly separable.

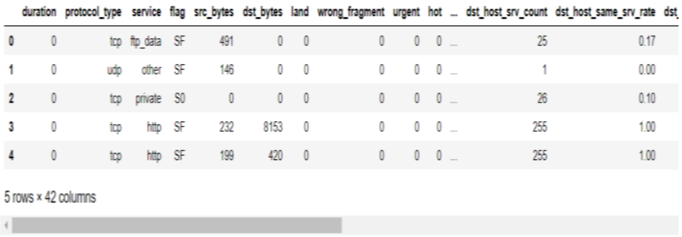
4.1.1 Dataset Analysis

This dataset was collected by simulating a typical U.S Air force local area network (LAN), operated like a real environment and being blasted with multiple attacks [8]. The kddcup99 dataset is divided into two parts such as the training and the testing set. The training set consists of 4,900,000 single connection vectors in which each has 41 features capable of detecting mainly two activities such as distinguishing an activity as normal or as an attack. The four attack types are Dos, U2R, R2L and probe [11].The summary statistics of the training and testing subsets is as follows:[10]

Type	No. of Records in Training Set	No. of Records in Testing Set
Attack	3,925,650	250,436
Normal	972,781	60,591
Total	4,898,431	311,027

Table 1: summary statistics of the training and testing subsets

The procedure of kddcup99 dataset helping in the process of intrusion detection is as follows: The multi-layer perceptron model is trained using the preprocessed kddcup99 dataset. The preprocessing step converts all types of data into numerical values. The model is trained in such a way that it is able to predict the activity as either normal or as an attack through the analysis of the variations in the corresponding values of the 41 features. So in real time whenever an attack or a normal activity is taking place the input to the model is a preprocessed data and the model will predict the corresponding activity through the comparison of the trained variations with the variations in the values achieved in real time. Thus the process of intrusion detection is achieved efficiently through kddcup99 dataset. Every TCP/IP link with features such as duration, protocol type, DST host service count etc.is also called normal with an exact form of attack. First five rows of the dataset are shown in the figure 2.



	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	...	dst_host_srv_count	dst_host_same_srv_rate	dst_
0	0	tcp	ftp_data	SF	491	0	0	0	0	0	...	25	0.17	
1	0	udp	other	SF	146	0	0	0	0	0	...	1	0.00	
2	0	tcp	private	S0	0	0	0	0	0	0	...	26	0.10	
3	0	tcp	http	SF	232	8153	0	0	0	0	...	255	1.00	
4	0	tcp	http	SF	199	420	0	0	0	0	...	255	1.00	

5 rows × 42 columns

Figure 2 KddCup99 Dataset

4.1.2 Pre-processing and Feature Scaling

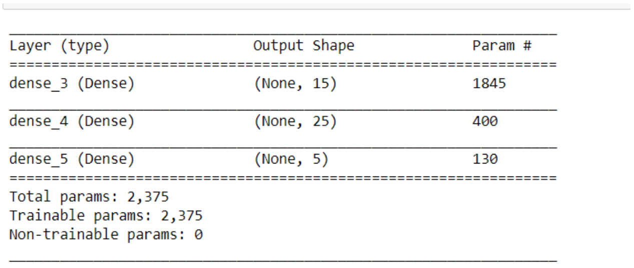
Pre-processing refers to all the transformations on the raw data before it is fed to the machine learning or deep learning algorithm. In pre-processing all the features are made a numerical value using One Hot Encoding which (one-of-K) is used to transform all categorical features into binary features. "The input to the present transformer should be a matrix of integers, denoting the values taken on by categorical (discrete) features [7]. The outputs are going to be a sparse matrix where each column corresponds to at least one possible value of 1 feature. It's assumed that input features combat values within the range [0, n values).".

The features are scaled using feature scaling to standardize the independent features present within a fixed range; here feature scaling is done at the time of data pre-processing with standard scalar in which the values are scaled with the distribution centred at 0 with a standard deviation of 1.

4.1.3 Training and Testing

In the Training the received data after pre-processing is used to create the pre-trained model by feeding the present output to the selected Deep Neural Network consisting of 2 dense layers other than input and output layer with Relu and Softmax activation functions and train our data with the described model in Figure 3.

The input shape is 122 and the total parameter for the input is 122*15+15 which gives 1845. Similarly other values of the dense network can be calculated as such. This is an original MLP model with total trainable parameters of 2375. In the output layer it consists of 5 nodes which represent the five classes of attack type i.e., DOS, Probe, U2R, R2L and Normal.



```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
dense_3 (Dense)              (None, 15)                1845
_________________________________________________________________
dense_4 (Dense)              (None, 25)                400
_________________________________________________________________
dense_5 (Dense)              (None, 5)                 130
=================================================================
Total params: 2,375
Trainable params: 2,375
Non-trainable params: 0
_________________________________________________________________
```

Figure 3 MLP Model Summaries

In testing, the data is fed to the trained model and run at 100 epochs gives 91.41 accuracy and the model converges to a loss of 1.192 .Then finalize the pre-trained model trained on a large benchmark dataset by considering the feasible computational cost and maximum obtained accuracy and this model marks the end of Intrusion Detection System.

The plot of model accuracy and the model loss are also shown in the figure 4 can be used to identify the progress and ability of the neural network model. This plot of learning curve shows a best fit model because the plot of training loss decreases to a point of stability and the plot of validation loss decreases to a point of stability and has a small gap with the training loss.

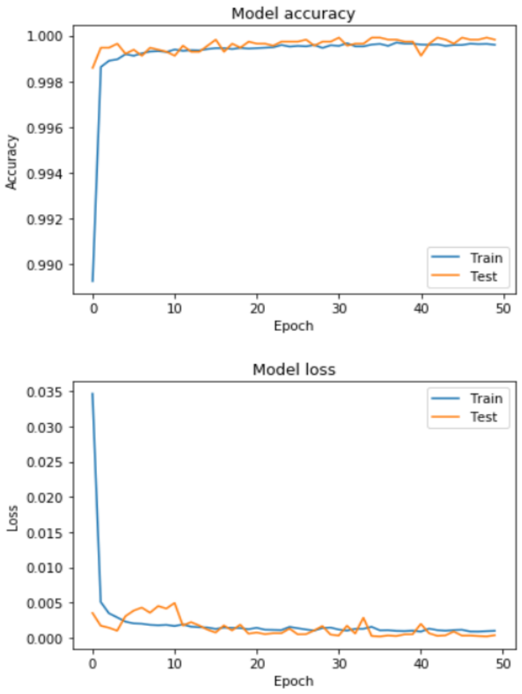


Figure 4 Plots of Model Accuracy and Loss

4.2 Intrusion Prevention System (IPS)

In intrusion prevention, the attack which is detected by the deep learning method as part of Intrusion detection is prevented using the iptable (command operations based on Linux) ,in which the network data packets are blocked using the iptable with regard to the prevention method needed for a specific attack[12].
When network attacks are detected, the system drives in through an input from the classification part in order to specify the attack corresponding to which the prevention operation is selected e.g., if probe attack takes place the IP address of both sender and attacker are taken and all packets from the attacker IP is either dropped or blocked, similarly if a DOS attack takes place then the system records the connection port number which was attacked and simultaneously blocks all the packets going through that port number and does nothing if the output of detection part is normal[13].
Thus, an intrusion is prevented using a script that runs in the background, using all the admin privileges. A script is developed in such a manner that it prevents any type of attack by counter triggering the type of prevention that is needed to save our system from that corresponding attack and thereby making our system safe from any kind of intrusion that may occur in our network.

5. RESULTS

The first attempt was a machine learning model with decision tree algorithm but the accuracy was only about 74% at around 100 epochs which was customized into another Supervised Machine Learning model namely SVM(Support Vector Machine) with linear kernel and random state 1.The newly generated SVM model was tested at 100 epochs and accuracy of 83% was obtained. To make the model more accurate deep learning MLP (Multi-Layer Perceptron) model with keras high level API was selected consisting of 2 dense layers having activation functions such as relu and softmax. The loss used is sparse categorical cross entropy with Adam optimizer with a batch size of 16 that has been run for about 100 epochs. In the end an accuracy of 91.4% has been got and the model for intrusion detection system was finalized. A wireshark tool was used to obtain real time network packet data and was exported into a csv file consisting of values needed for our model. Features like the IP address and the port number were considered for preventing the user from further malicious activities by using the administrative privileges and was established through a script.

ACCURACY	Decision Tree	SVM	MLP
DOS	74.63	83.06	91.41
Probe	74.57	82.84	90.56
R2L	73.9.	83.31	91.32
U2R	74.66	83.56	90.39

Table 2: Comparison of Results

6. CONCLUSION

To prevent attacks to the networks, an intrusion detection and prevention system plays a crucial role in the cyber security domain. In order to improve the system's versatility, it is necessary to implement the system as anomaly detection with a learning framework instead of signature-based detection. One of the newest training and classification techniques, which are executed in this engine, is emerged as deep learning. These intrusion detection instruments utilize a few strategies to assist them decide what qualifies as an interruption versus normal traffic. If a program uses anomaly detection, misuse detection, target monitoring, or stealth probes, they usually fall into one of two categories: network or host [6]. Each category has its own strengths and weaknesses that should be evaluated against the needs for different targets. After implementing this IDS model using deep learning, the script for the prevention is generated. It would be able to prevent all the unknown attacks and intrusions based on the deep learning model.

7. REFERENCES

[1] Dai, Y., Li, H., Qian, Y., Yang, R., & Zheng, M. (2019). *SMASH: A Malware Detection Method Based on Multi-feature Ensemble Learning. IEEE Access, 1–1.* doi:10.1109/access.2019.2934012

[2] Ravji, S., & Ali, M. (2018). *Integrated Intrusion Detection and Prevention System with Honeypot in Cloud Computing. 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE).* doi:10.1109/iccecome.2018.8658593

[3] Sunita Kumawat., Anil Kumar Sharma., Anjali Kumawat. (2016). Intrusion detection and prevention system using K-learning classification in cloud. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). doi.10.1109/indiacom.2016.7724378

[4] Vasudeo, S. H., Patil, P., & Kumar, R. V. (2015). *IMMIX-intrusion detection and prevention system. 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM).* doi:10.1109/icstm.2015.7225396

[5] Ahmed, M., Pal, R., Hossain, M. M., Bikas, M. A. N., & Hasan, M. K. (2009). *NIDS: A Network Based Approach to Intrusion Detection and Prevention. 2009 International Association of Computer Science and Information Technology - Spring Conference.* doi:10.1109/iacsit-sc.2009.96

[6] "Multi Layer Perceptron (MLP) Models On Real World Banking Data". *Medium*, 2020, https://becominghuman.ai/multi-layer-perceptron-mlp-models-on-real-world-banking-data-f6dd3d7e998f?gi=7057648ed14f.

[7] "Sklearn.Preprocessing.Onehotencoder — Scikit-Learn 0.22.1 Documentation". *Scikit-Learn.Org*, 2020, https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.OneHotEncoder.html.

[8] Network, Intrusion. "Intrusion Detection Using Artificial Neural Network - Docshare.Tips". *Docshare.Tips*, 2020, http://docshare.tips/intrusion-detection-using-artificial-neural-network_584e6fd3b6d87f49628b524f.html.

[9] "An Introduction To IDS | Symantec Connect". Symantec.Com,2020,https://www.symantec.com/connect/articles/introduction-ids.

[10] Sonali Rathore, Prof. Amit Saxena, and Dr. Manish Manoria. "Intrusion Detection System on KDDCup99 Dataset: A Survey." *IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 6, no. 4, 2015.

[11] Modi Urvashi, and Prof. Anurag Jain. "A Survey of IDS Classification Using KDD CUP 99 Dataset in WEKA ." *International Journal of Scientific & Engineering Research*, vol. 6, no. 11, Nov. 2015.

[12] Musawi, Bahaa. (2012). Mitigating DoS/DDoS attacks using iptables. International Journal Of Engineering & Technology. 12. 101-111.

[13] Wattanapongsakorn, N., et al. "A Practical Network-Based Intrusion Detection and Prevention System." *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, doi:10.1109/trustcom.2012.46.

[14] Ge, Mengmeng, et al. "Deep Learning-Based Intrusion Detection for IoT Networks." *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2019, doi:10.1109/prdc47002.2019.00056.

[15] Patel, Ahmed & Qassim, Qais & Wills, Christopher. (2010). Survey of Intrusion Detection and Prevention Systems. Information Management and Computer Security. 18. 10.1108/09685221011079199.