IJIRMET ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering, and Technology
Vol. 8, Issue 3, March 2023

# INTRUSION DETECTION SYSTEM USING DEEP LEARNING (LSTM) INNETWORK SECURITY

[1] Manikandan,[2] Darwin Arun Doss I,[3] Mukesh Kumar M,[4] Rajesh S,[5] Vijay A

[1] MENTOR,AP/IT, Department of Information Technology Hindusthan Institute of Technology

[2][3][4][5] Department of Information Technology Hindusthan Institute of Technology.

***Abstract:** Nowadays, large numbers of people were affected by data infringes and cyber-attacks due to dependency on internet. India is lager country for any resource use or consumer. Over the past ten years, the average cost of a data breach has increased by 12%. Hacking in India is take share of 2.3% of global criminal activity. To prevent such malicious activity, the network requires a system that detects anomaly andinform to the admin or service operator for taking an action according to the alert. System used for intrusion detection (IDS) is software that helps to identify and observes a network or systems for malicious, anomaly or policy violation. Deep learning algorithm techniques is an advanced method for detect intrusion in network. In this paper, intrusion detection model is train and test by NSL-KDD dataset which is enhanced version of KDD99 dataset. Proposed method operations are done by Long Short-Term Memory (LSTM) and detect attack. So admin can take action according to alert for prevent such activity. This method is used for binary and multiclass classification of data for binary classification it gives 99.2% accuracy and for multiclass classification it gives 96.9% accuracy.*

***Keywords— Intrusion detection; Deep Learning Method; LSTM algorithm; Network Security, NSL- KDD dataset.***

## 1. INTRODUCTION

Security of data is very important aspect of internet in recent years. For illegal right to use or information from network, intruder made an intrusion in system. An intrusion is nothing but attack, hacking, packet sniffing or stilling of data. Attacks are an aim to tear down system privacy or networks in way to extort money, other malicious intentions or acquiring essential records. Intrusion modify program, data or logic in computer by the use of malicious code resulting in difficulty a few consequences that can give and take the institutes private data to formulate it accessible for cybercriminal. Many different attacks come under Cyber attacks which consist of hacking of data, Denial of services, Malware, Phishing and theft. The percentage of cyber attackers or illegal activities increases in the world and defender of cyber-security are experience a lot of threats from these cyber attacker. It could probably leave in to enormous and a major impact on human lives for that to take security measures are important. And these measures can be done by intrusion detection system (IDS). Intrusion Detection can be done by collecting of data packets, analyzing it and detecting any unwanted, suspicious or malicious things in traffic to inform administrator. This device is prepared for securing our data from any attack or unwanted use.

The digital world is especially vulnerable to security threats. Hackers are gradually more hacked websites for various reasons. That creates many security threats that had made numerous companies re-evaluate their security measures. Hackers ascertain the loopholes in the website to break the system and achieve their offender ideas. Intrusion detection system also knows as security information and event management system. Two methods are generally used ie. Signature based and anomaly based. And some types are based on network intrusion, host based, perimeter, VM based intrusion detection system. The system detect network ie. A data packet travels from one to another destination. This step is useful for protection of data, information and other losses due to attack.

The reminder of this proposed paper is arranged as follows: Section II covers related work with intrusion detection. Section III gives detail description of Algorithm used in the paper which is Long Short-Term Algorithm ie. LSTM. Next section Iv related to NSL-KDD dataset. Section v includes proposed system description. After that, section vI having tentative results and last one is the conclusion of paper in section vII.

## II. RELATED WORK

This section includes recent development in intrusion detection system. Many methods of machine learning are used for detection of anomalies. As development in technology the techniques also upgrade to accomplish requirements. And now those techniques used machine learning that converted in deep learning methods for more precision and accuracy.

Anish Halimaa and Dr. K.Sundarakantham [1] used SVM and Naïve bayes method for intrusion detection. This paper shows comparative analysis of SVM and Naïve bayes with the help of NLS-KDD dataset. Both methods used for solving the classification problem. Accuracy and misclassification rate get calculated and on that basis SVM works better than Naïve bayes. Normalization and feature reduction are also applied to makes comparative analysis. Performance of model is depends on accuracy, main motive is to reduce false alarm rate (FAR) and to increase detection rate by increasing accuracy. SVM algorithm is used for image processing and pattern reorganization application on the other hand Naïve data, classification according to set of rules and result evolution on the base of method used.

Mohammed Ishaque et al [2] used deep learning which is an region of Machine Learning research. Deep learning approach is used to selecting a subset of relevant feature from unknown information. These types of property are useful in analysing highly complex information to detect anomaly from data present on internet or web system. Deep learning method is used for feature extraction to reduce dimensionality of the dataset obtained from the web system. This paper used unlabeled training data and web system data are given to pre- processing unit then this data is compared with the help of stacked denoising autoencoder, after this data will be split into attacking and normal traffic.

Jin Yang et al [3] proposed the method to address the challenge of unbalanced positive and negative learning samples, we propose 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. This paper applies long short-term memory (LSTM) to automatically learn the features of network intrusion behaviours. To remove such dependency and enable intrusion detection in real time, we propose a simple recurrent unit based (SRU)-based model. The proposed model in this paper was verified by wide-ranging experiments on the standard datasets for intrusion detection which is KDD'99 and NSL-KDD that effectively recognizes normal and malicious network activities. It achieves 99.73% accuracy for the KDD'99 dataset and 99.62% on the NSL-KDD dataset.

Gozde Karatas et al [4] this paper aimed to survey deep learning based intrusion detection system approach by making a comparative work of the literature contains three main components: data collection, feature selection/ conversion and decision engine. To extend the pliability of the system, rather than signature-based detection, it's required to implement the system as anomaly detection with a learning system. Therefore, during this paper, it's aimed to supply a brief survey of deep learning-based intrusion detection systems with the overview of varied aspects of intrusion detection and deep learning algorithms. Additionally, this work lists and provides details about some publicly available datasets with their characteristics and shortcomings.

Dimitar Nikolov et al [5] this paper presents the effects of problem based learning project on a high-school student in Technology school. The intrusion detection system is predicated on a recurrent neural network classifier namely long-short term memory units. The intrusion detection system (IDS) consists of three modules: monitoring, processing and learning module. Learning module creates the LSTM recurrent neural network and finds the necessary structure, weights and biases. For learning, the dataset consisting of system call sequences is used.

Brian Lee et al [6] this paper presents a comparative evaluation of deep learning approaches to network intrusion detection. The paper present a comparative evaluation of deep learning approaches to network intrusion detection. Their performance is evaluated using the network intrusion dataset provided by Knowledge Discovery in Databases

(KDD). The results of the analysis between the deep learning models suggests that the utilization of deep learning in NIDS would be a appropriate solution to improving detection accuracy on unclean data; however, building an environment that is specifically designed for this purpose would go a long way to further improve and could greatly impact the decision on which model would work best in a given environment.

## III. LSTM: LONG SHORT-TERM ALGORITHM

Long short-term memory (LSTM) is special sort or superior version of a man-made recurrent neural network (RNN) architecture utilized within in the sector of deep learning. LSTM has feedback connections and design to avoid long term dependencies. It can't only process only data points, but also whole sequences of knowledge. For instance, LSTM is applicable to tasks like unsegmented data, connected recognition pattern, speech recognition and anomaly detection in network traffic or IDS's (intrusion detection systems). A common LSTM unit consists four main parts: 1) cell, 2) input gate, 3) output gate and 4) forget gate. The cell memories values over random time intervals and therefore the three gates standardize the flow of data or information into and out of the cell.

LSTM networks are complementary to classifying, processing and makingpredictions based on time series data, since there are often lags of unknown duration between important events in a time series. LSTMs were developed to affect the vanishing gradient problem that can be encountered when training traditional RNNs. Relative insensitivity to gap length is a plus of LSTM over RNNs, hidden Markov models and other sequence learning methods in numerous applications. LSTM having foru stages in it's cell structure as shown in fig.1.

In cell state, the horizontal topmost line running in cell that indicates cell state. The LSTM does have the ability to eliminate or incorporate information to the cell state, carefully regulated by structures called gates. The cell has series like structure in it. Step 1: The first step in LSTM is to identify that information that are not necessary and make a decision of what information is going to throw away from the cell state. This decision is formed by a sigmoid layer called the ‘forget gate layer’.

$$f_t = \sigma (W_f \; .[h_{t-1} \; , \; _t] + b_f) \qquad \text{--(1)}$$

where; $ht-1$= output from previous time stamp, $xt$ = new input, $bf$ = bais

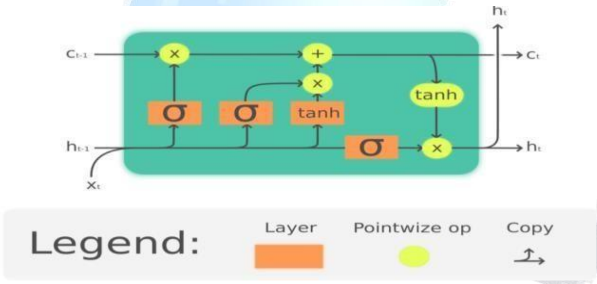


Fig.1: LSTM cell

Step 2: The next step is to make a decision what new information were going to store in the cell state. This comprise two parts: One - a ‘sigmoid layer’ called the “input gate layer” decides which values will update, second- a ‘tanh layer’ creates a vector of new contender values , that could be added to the state. In the next step is to combine these two to create an update to the state.

$$i_t = \sigma (W \; .[h_{t-1} , \; _t] + b_i) \qquad .(2)$$

~

$$C_t = \tanh(W_C \, .[h_{t-1} \, , x_t] + b_C) \qquad .(3)$$

Step 3: It is now time to update the old cell state C(t-1), into the new cell state. The previous steps already decided what to do, actually just need to do it. First- The old state multiplies by, forgetting the things that we decided to forget previous. Second- Then, add to cell state. This is the new candidate values, scaled by what proportion for decided to update each state value.

$$C_t = f_t * C_t + i_t * C_t \qquad (4)$$

Step 4: Final stage is output stage. This output are going to be supported our cell state, but will be a filtered version. First, run a sigmoid layer which decides what parts of the cell state going to output. Then, put the cell state through tanh (to push the values to be between −1 and 1) and multiply it by the output of the sigmoid gate, so that only output the parts decided to.

$$o_t = \sigma(W_o . [h_{t-1}, x_t] + b_o) \qquad ...(5)$$

$$h_t = o_t * \tanh\,(C_t) \qquad ..(6)$$

IJIRMET

## IV. DATASET: NSL-KDD

Intelligent intrusion detection systems can only be built if there's availability of an efficient data set. A data set with a large amount of quality data which mimics the important time can only help to coach and test an intrusion detection system. The NSL-KDD data set may be a refined version of its predecessor KDD‟99 data set. In this paper the NSL-KDD data set is analysed and wont to study the effectiveness of the varied classification algorithms in detecting the anomalies within the network traffic patterns.

NSL-KDD dataset may be a data set suggested to unravel a number of the inherent problems of the KDD'99 data. This advantage makes it affordable to run the experiments on the entire set without the necessity to randomly select a little portion.

Furthermore, the amount of records within the NSL-KDD train and test sets are reasonable. This advantage makes it affordable to run the experiments on the entire set without the necessity to randomly select a little portion. Consequently, evaluation results of various research works are going to be consistent and comparable.

The NSL-KDD data set has the subsequent advantages over the first KDD data set:

- It doesn't include redundant records within the play thing; therefore the classifiers won't be biased towards more frequent records.
- There is not any duplicate records within the proposed test sets; therefore, the performance of the learners aren't biased

by the methods which have better detection rates on the frequent records.

- The number of selected records from each difficulty level group is inversely proportional to the share of records within the original KDD data set. As a result, the classification rates of distinct machine learning methods vary during a wider range, which makes it more efficient to possess an accurate evaluation of various learning techniques.

- The number of records within the train and test sets is reasonable, which makes it affordable to run the experiments on the entire set without the necessity to randomly select a little portion. Consequently, evaluation results of various research works are going to be consistent and comparable

Total 126620 samples were available for NSL-KDD training module, along with 41 features each (similar to KDD99) it will consider normal traffic or attack of special type. The features are categories as main four types:

- Basic feature: Each resource obtained from the TCP/IP connection, such as service, duration and protocol type.
- Time-based traffic features: such as Rerror rate, srv count and count.
- Content features: In order to access the TCP packets, these resources use domain knowledge.
- Host-based traffic features: Each attack longer than two seconds that share the equal destination host as the present connections are accessed utilised these kinds of features.

The NSL-KDD labels are sub-divided in four categories of attack and one normal traffic category. The attack categories are:

- DOS (Denial of Service): try to block network resources and/or services in network and computer network.
- Probe: attack that attempts to obtain information or find vulnerabilities in a network.
- R2L (Remote to Local): attack that want to generate remote, non-authorized access to a network.
- U2R (User to Root): special kind of attempts to obtain access as root user or admin.

## V. PROPOSED SYSTEM

The paper used deep learning LSTM algorithm for detection of intrusion in network. This method has several steps as shown in fig.2. NSL-KDD dataset is used for training as well as testing of LSTM model. The Model used for two types of classification of output. One is for Binary classification: that detect malicious and normal data for testing. And second is for Multiclass classification of data: which give five output like- DOS, U2R, R2L, Probe, Normal data.

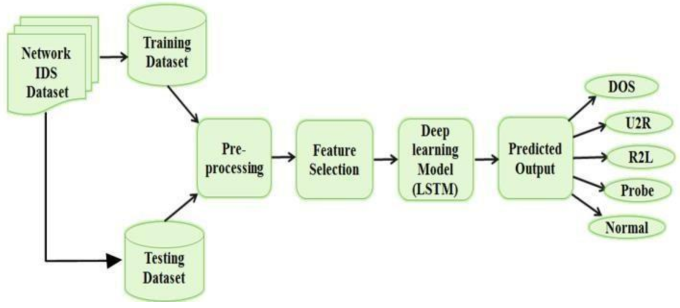


Fig.2: Proposed Methodology

Network Intrusion Detection System (IDS) dataset:
There are many types of datasets available on internet for intrusion detection in network. But the KDD99 dataset is most popular and mostly used by many researchers for their work on intrusion detection. The KDD data set is used to modify the detection module and many updated versions of KDD dataset is available for IDS. In proposed work NSL- KDD dataset is used for detection of intrusion in network (which is newer version of KDD99 CUP dataset).
.

### A. Training / Testing Dataset:

NSL-KDDtrain and NSL-KDDtest dataset is used for training as well as testing of LSTM model. It divided into 60-40 ratio, that meance 60% of dataset is used for training and 40% of data for testing of model. The ration of training and testing can be varying according to researcher and application.

### B. Preprocessing

The pre-processing step is to produce data which is practical for detection of intrusion. Pre-processing mainly focus on the general operations, like converting the data into readable form and also into another format. Also eliminating the redundant data into dataset, this is taking from training dataset to model or test the data that is input data. This data is then given as input to the feature extraction for feature selection. Some of this having no values in columns that will be eliminated, to avoided confusion in learning as well as testing.
This also includes normalization of data, which normalized values of matrix for LSTM model, to convert data into same format or type.
Normalization of data:

Features = Features - f
***min*** $f_{max}$ - $f_{min}$

### C. Feature Selection

Feature extraction is the process where important information. It is one of many factors which are used to increase the effectiveness of a detection system. NSL-KDD dataset having 41 features and one 42 feature column is for data label. The 41 features are like as Duration, protocol_type, service, flag, etc. Last column (ie. 42 column) is xAttack[17].
This label converted into two categories:
Binary Classification- (0; 1), 0 = normal traffic, 1 = malicious traffic.
Multiclass classification- Attacks were assigned with real values in new field called xAttack: dos = [1], u2r = [2], r2l = [3], probe = [4], normal = [5], unknown = [6]
D. Deep learning Classification
By using LSTM deep learning algorithm (special sort of RNN) the data will classify into normal data, malicious / suspicious data also in other attack types. Five different types of attacks are included in this analysis: DOS, U2R, R2L and Probe attack. Which type of specific attack occur on network,

that also recognized by the algorithm for multiclass classification of data.

E. Proposed Output:
The output of model gives two types of classification. This method gives binary and multiclass classification of test data. Binary class classification is used for binary output which is for malicious and normal data. Multiclass classifier gives five output: DOS, U2R, R2L, Probe and normal data.
F. Output (Network attack type):
After classification, it gives output that detects network attack type. The deep learning algorithm is used for the detection of intrusion. If the malicious data is found, then the alert is given to the system admin to act according on the alert.
G. Training values:
The time requires for training or testing data is calculated as evaluation time of model. For binary classification or multiclass classification training evaluation time is depends on system parameters and specification. Because, the deep learning is require latest specification for better executions of task. So, the evaluation time of testing or binary classification is 8.28 sec and 3.25 sec for multiclass classification.

### H. Performance Statistical Measure

The values are obtain from confusion matrix, used for calculation of different parameters .These parameters are nothing but performance measures of model.

This section includes performance measure of binary classifier: which is having values for malicious data and normal data. And Multiclass classifier: includes values for four specific attack and normal data. Table-I gives parameters for Binary Classification.

TABLE I. PARAMETER VALUES OF BINARY CLASSFICATION

| | |
|---|---|
| **True Positive** | 12739 |
| **False Negative** | 94 |
| **True Negative** | 9615 |
| **False Positive** | 95 |
| **Accuracy** | 99.1616 |
| **Error Rate** | 0.8484 |
| **Sensitivity (Recall)** | 99.2675 |
| **Specificity** | 99.0216 |
| **F-Score** | 99.2613 |
| **Positive Predictive Rate (Precision) (PPR)** | 99.2598 |
| **False Positive Rate (FPR)** | 0.97837 |
| **Matthews Correlation Coefficient (MCC)** | 98.2904 |

IJIRMET

## VI. EXPERIMENTAL RESULT

Confusion Matrix

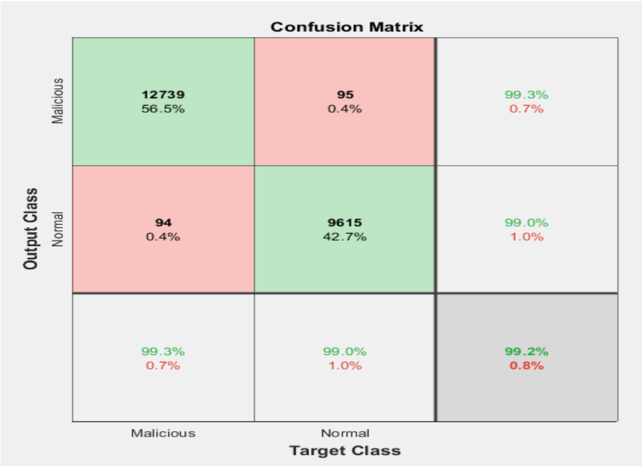
1. Binary classifier

Data classification is performed by LSTM model for separating malicious data/ traffic from normal data/traffic. Binary confusion matrix, separate data into four parts ie.TP, TN, FP, FN. Green blocks shows positive values of matrix

and red blocks shows negative values of Matrix. Malicious across malicious block shows true positive value, same for normal and normal across malicious shows negative values. The accuracy depends on how efficiently it classifies values, gives across that rows and columns.

2. Multiclass Classifier

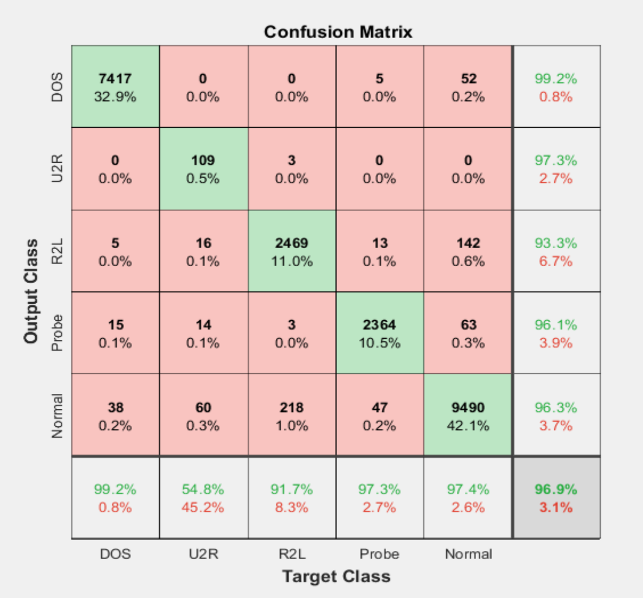
Multiclass confusion matrix gives values same like green for positive and red in negative values. Only thing changes in multi class is that, it give very large number of values for each class and very difficult for manual calculations of parameters. The complexity of formula for multiclass confusion matrix is increased as compare with binary confusion matrix.DOS across DOS having positive values and other all values are consider as negative for DOS class, same for other class



Confusion Matrix

| Output Class \ Target Class | Malicious | Normal | |
|---|---|---|---|
| Malicious | 12739<br>56.5% | 95<br>0.4% | 99.3%<br>0.7% |
| Normal | 94<br>0.4% | 9615<br>42.7% | 99.0%<br>1.0% |
| | 99.3%<br>0.7% | 99.0%<br>1.0% | 99.2%<br>0.8% |

Fig. 1. Confusion Matrix of Binary Classifier



Confusion Matrix

| Output Class \ Target Class | DOS | U2R | R2L | Probe | Normal | |
|---|---|---|---|---|---|---|
| DOS | 7417<br>32.9% | 0<br>0.0% | 0<br>0.0% | 5<br>0.0% | 52<br>0.2% | 99.2%<br>0.8% |
| U2R | 0<br>0.0% | 109<br>0.5% | 3<br>0.0% | 0<br>0.0% | 0<br>0.0% | 97.3%<br>2.7% |
| R2L | 5<br>0.0% | 16<br>0.1% | 2469<br>11.0% | 13<br>0.1% | 142<br>0.6% | 93.3%<br>6.7% |
| Probe | 15<br>0.1% | 14<br>0.1% | 3<br>0.0% | 2364<br>10.5% | 63<br>0.3% | 96.1%<br>3.9% |
| Normal | 38<br>0.2% | 60<br>0.3% | 218<br>1.0% | 47<br>0.2% | 9490<br>42.1% | 96.3%<br>3.7% |
| | 99.2%<br>0.8% | 54.8%<br>45.2% | 91.7%<br>8.3% | 97.3%<br>2.7% | 97.4%<br>2.6% | 96.9%<br>3.1% |

fig. 2. Confusion Matrix of Multiclass Classifier

IJIRMET

## VII. CONCLUSION

This paper proposed Long Short-Term Memory algorithm for intrusion detection in network security based on anomaly detection. The method comprises binary as well multiclass classification for detection. Multiclass categories attack into four main types which are including in NSL- KDD dataset. The need for detecting attack very precisely can be fulfill by using deep learning method for intrusion detection. This paper gives 99.2% accuracy for binary classifier and 96.9% accuracy for multiclass classifier. Different parameters calculated to see model effectiveness for detection of intrusion like: Sensitivity is 99.26 %, 99.26 % Specificity and
0.97 False Positive Rate. By using an algorithm of deep learning in MATLAB (2019b) software, intrusion detection can be done more effectively in network security.

ACKNOWLEDGMENT
I would like to express my gratitude towards the mentor who inspires me for taking this subject for a research and also thankful to the Electronics department of Government College of Engineering, Amravati for provided facilities, environment and support.

## 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.

IJIRMET