Machine Learning and Deep Learning based Cyber Attack Detection In Industrial Automation And Control Systems

Mohammed Mohaideen.J, AnanjanVikash.R.K, Ashik Elahi Khan.S

(Electronics and Communication Engineering)

K.L.N.College of Engineering,Sivagangai,Tamilnadu

*Mrs.R.Thilagavathy, B.E,M.E,
AssistantProfessor(Sr.Gr),
K.L.N.College of Engineering,Sivagangai,Tamilnadu

Abstract–The proposed model is aimed at detecting intrusions by classifying as benign or malicious in the data set (KDD Cup 99 & CIDCD) has been used to train and test.Then data preprocessing will happen to remove null values and redundancy in the dataset. k means algorithm is used to clustering the dataset into three. Machine learning algorithm called Random Forest algorithm is used to find the accuracy and also to calculate the confusion matrix.Then,Implemented the deep learning algorithm using Long Short Term Memory algorithm to find the accuracy and also to calculate the confusion matrix. Compare both the accuracy of the Random forest algorithm and Long Short Term algorithm to conclude that the Long Short Term Algorithm is more than Random Forest. Finally send the details of attacked data to the user by email using SMTP

Keywords— Attacks, Random Forest, LSTM, accuracy, confusion matrix.

INTRODUCTION

In this period of technological advancement, there is an explosion of new technologies.
prospects and cost-effective potential resources.
Organisations have formed, but these have also emerged.
Threats to the economy have arisen as a result of technological advancements. In such a case,
In this scenario, effective security measures are critical. Now, Hacking has been a frequent technique in recent years. In order to steal data and information from them. This emphasises the necessity for a reliable system to identify and respond to threats to thwart fraudulent activity. It's all about the data when it comes to cyber security.

Cyberspace security for systems, networks, and data.

Malware is still one of the most dangerous security threats.
Internet-based dangers Malware is a term used to describe malicious software signal that the file or programmes are harmful. These are the ones unwelcome initiatives because they affect the environment.

To provide a new detective machine to predict the attacked information in the facts set containing lots of data the use of a device learning & advanced deep learning method.
We are thinking about KDD cup 99 dataset for education and CIDCD dataset for checking out and preprocessing takes place for this two records set to put off null values, redundancy values, repetition of facts from the dataset then characteristic extraction need to be executed to switch uncooked data into numerical values before applying Machine Learning and Deep learning algorithms to get the higher results, then by means of using random woodland set of rules and long quick term memory algorithm (LSTM) we will get the accuracy, f1 score, precision, recall & confusion matrix.

EXISTING SYSTEM

A . The EnPEO-DBN Method :

We supply a novel ensemble technique to decorate the detection performance of cyber-attacks in IACS primarily based on the PEO-DBN detection technique in this section. The framework of the EnPEO-DBN is given in Algorithm Algorithm 1. Firstly, a random subspace-based total features segment [2] is used to construct the organisation functions Xk from the SCADA network. Then, Mbase classifiers are obtained based on Xk. In other words, after schooling is completed, M one of a kind PEO-DBN-based classifiers are received. Finally, these class consequences are incorporated by the majority vote casting scheme noted . The structure of the proposed EnPEO-DBN detection approach for cyber-attacks in IACS Network site visitors can be transmitted from cyber layer to bodily layer or vice-versa, which can be monitored through the secure shape. And the cyber-assaults detection technique can obtain any response from PLC/RTU to master terminal unit (MTU) or question from MTU to PLC/RTU. The fundamental components of technique
for detecting cyber-attacks are given as follows.
1) PEO set of rules, a complicated optimizer, is applied to optimise the adjustable parameters, e.g., the gaining knowledge of price.The length of mini-batch and the number of hidden layers in DBN with the aid of minimising the health function in Equation (eight). The details of proposed PEO-DBN are given in Section III.B.

2) PEO-DBN with one of a kind functions are employed to examine the implicit dating among community site visitors statistics and attack sorts. Then, a majority balloting scheme is implemented to aggregate the distinct class effects obtained with the aid of PEO-DBN to triumph over the weak spot of single technique.
3) Several cyber-attacks detection strategies are regarded as the competitors to demonstrate the detecting overall performance of PEO-DBN and EnPEO-DBN in line with specific assessment metrics.
An original group technique to upgrade the location execution of digital assaults in IACS in light of the PEO-DBN recognition strategy in this segment. The structure of the EnPEO-DBN is given in Algorithms. Right off the bat, irregular subspace-based highlights are utilised to develop k-the gathering highlights Xk from the SCADA organisation. Then, M base classifiers are obtained in view of Xk. As such, after the preparation interaction is achieved, M different PEO-DBN-based classifiers are obtained. At last, these characterization results are coordinated by the larger part casting a ballot conspire referenced in.

The construction of the proposed EnPEO-DBN discovery technique for digital assaults in IACS.Network traffic can be sent from digital layer to actual layer or the other way around,

B . The PEO-based DBN Method :

There is no current clear information to assist customers set the DBN's adjustable parameters. These parameters encompass the size of mini-batch, mastering price and the wide variety of hidden
layers [8]. Many researchers decide these parameters via trial-and-error, which manually requires substantial knowledge and can not be used efficiently. Additionally, PEO has been established in managing a number of complex optimization problems, however it has no longer been employed in optimising DBN. Thus, we use the PEO because it is the seek engine for computerised parameter optimization of DBN to enhance the ability of detecting cyberassaults. The distinct fitness characteristic is designed to tune the parameters of DBN,
F = 1 − gacc(f (tr x, tr y, Nhid1, Nhid2, Mbt, ε1, ε2),
tr x, tr y)
gacc =T P +T N /T P +T N+F P +F N.

The performance of detection methods are justified according to two commonly evaluation metrics, i.e., accuracy (ACC) and false positive rate (FPR),

I. DEEP LEARNING METHOD

Deep mastering is an AI feature that mimics the workings of the human brain in processing facts for use in detecting objects, spotting speech, translating languages, and making
selections. Deep mastering AI is able to research without human supervision, drawing from information that is each unstructured and unlabeled.Deep studying applications are utilised in industries from automated riding to clinical gadgets. Automated Driving: Automotive researchers are the use of deep learning to robotically detect gadgets including forestall symptoms and site visitors lighting fixtures. In addition, deep mastering is used to come across pedestrians,which helps decrease accidents.Various styles of deep mastering approach is given beneath:

• Convolutional Neural Networks (CNNs)
• Long Short Term Memory Networks (LSTMs)
• Recurrent Neural Networks (RNNs)
• Generative Adversarial Networks (GANs)
• Radial Basis Function Networks (RBFNs)
• Multilayer Perceptrons (MLPs)
• Self-Organising Maps (SOMs)
• Deep Belief Networks (DBNs).

II. MACHINE LEARNING TECHNIQUES

Machine learning (ML) is a type of artificial intelligence (AI) that allows software applications to become more accurate at predicting outcomes without being explicitly programmed to do so. Machine learning algorithms use historical data as input to predict new output values.

- SVM algorithm
- Naive Bayes algorithm
- KNN algorithm
- K-means
- Random forest algorithm.

III. PROPOSED PROBLEM

Intrusion Detection is a hassle of identifying unauthorised users on a pc device. It is also described because the hassle of protecting laptop network structures from being compromised. The first posted renowned literature on laptop network security is [2] where Denning discussed diverse security worries, supplied a definition of Intrusion Detection and discussed exclusive kinds of Intrusion Detection. An intrusion detection system is software program and/or hardware designed to hit upon unauthorised tries at accessing,manipulating, and/or disabling a laptop machine, particularly through a network, which includes the internet. One of the principle demanding situations within the security management of massive-scale excessive speed networks is the detection of anomalies in network visitors.
A secure community ought to provide the subsequent:

• Confidentiality: Data which are being transferred through the community have to be accessible simplest to those which have been well legal.
• Integrity: Data should hold their integrity from the moment they're transmitted to the instant they are really acquired. No corruption or facts loss is familiar both from random occasions or malicious pastime.
• Availability: The network needs to be resilient to Denial of Service assaults.A laptop has to offer confidentiality, integrity and guarantee in opposition to the exceptional sorts of attacks. However, because of improved load and connectivity, increasingly the system is subjected to assault with the aid of intruders and malicious users. They try to take advantage of

flaw or loop holes inside the working gadget as well as within the utility applications.

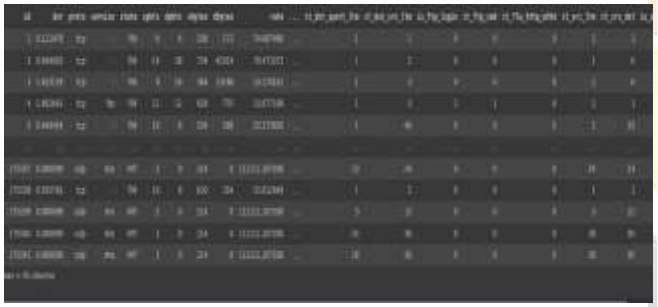
We can use the cryptographic techniques to secure the system however they have got their personal issues as password can be easily cracked, customers can lose their passwords and complete crypto-device can be damaged. We want to secure the system against unauthorised access by means of malicious consumers or hackers. So we need a machine that's actual time, that is We would like to locate them as quickly as feasible and take suitable movement. This is what an intrusion detection gadget does. We tried to construct a machine which created clusters from its input statistics with the aid of labelling clusters as everyday or anomalous fact instances and in the end used these clusters to classify unseen network information times as both everyday or anomalous [4]. Both education and trying out became the use of a special subset of KDD Cup 99[9] facts that is used as an training dataset and CIDCD 2019 is used as an testing dataset.

PROPOSED METHOD

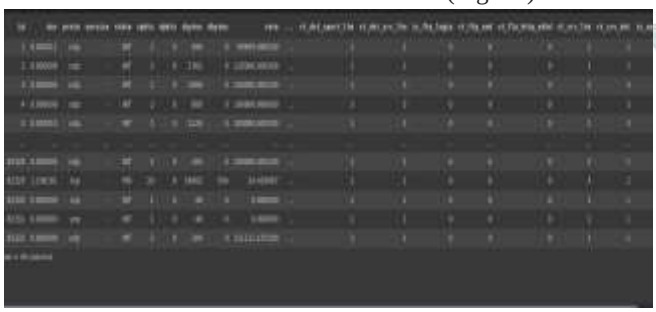
A. Dataset :

A data set is a collection of related, discrete items of related data that may be accessed individually or in combination or managed as a whole entity.A data set is organised into some type of data structure.

In this we are using KDDcup 99 for training and CIDCD 2019 for testing



TRAINING DATASET (Fig 1.1)



TESTING DATASET (Fig 1.2)

A. Data Preprocessing :

We used Label encoder to preprocess the data set, Label Encoding refers to **converting the labels into a numeric form so as to convert them into the machine-readable form**. Machine learning algorithms can then decide in a better way how those labels must be operated. It is an important preprocessing step for the structured dataset in supervised learning.

Data preprocessing is **a process of preparing the raw data and making it suitable for a machine learning model**. It is the first and crucial step while creating a machine learning model. When creating a machine learning project, it is not always the case that we come across clean and formatted data.

Steps to preprocess the dataset :

- Data quality assessment.
- Data cleaning.
- Data transformation.
- Data reduction.

After preprocessing the datasets we process the datasets (fig 1.1 & 1.2) under feature extraction using the K Means algorithm.

B. Feature Extraction :

Feature extraction for machine learning and deep learning. Feature extraction refers to the process of transforming raw data into numerical features that can be processed while preserving the information in the original data set. It yields better results than applying machine learning directly to the raw data. Feature extraction helps to reduce the amount of redundant data from the data set. In the end, the reduction of the data helps to build the model with less machine effort and also increases the speed of learning and generalisation steps in the machine learning process.

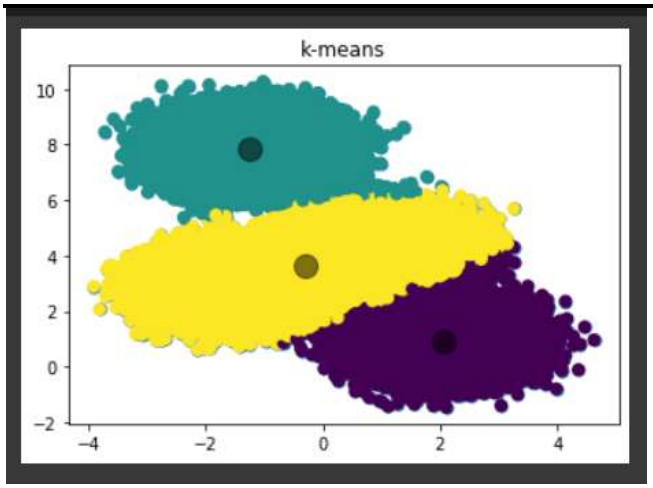
C. K Means Algorithm :

K-Means Clustering is an Unsupervised Learning algorithm, which groups the unlabeled dataset into different clusters. Here K defines the number of predefined clusters that need to be created in the process, as if K=3, there will be three clusters. It is an iterative algorithm that divides the unlabeled dataset into k different clusters in such a way that each dataset belongs to only one group that has similar properties. It is a centroid-based algorithm, where each cluster is associated with a centroid. The main aim of this algorithm is to minimise the sum of distances between the data point and their corresponding clusters. The algorithm takes the unlabeled dataset as input, divides the dataset into k-number of clusters, and repeats the process until it does not find the best clusters. The value of k should be predetermined in this algorithm.

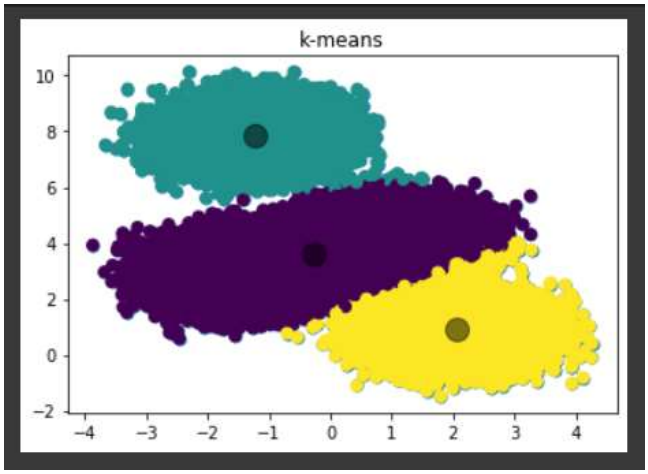
The k-means clustering algorithm mainly performs two tasks:

- Determines the best value for K centre points or centroids by an iterative process.
- Assigns each data point to its closest k-centre. Those data points which are near to the particular k-centre, create a cluster.

In this proposed method we used the k-means algorithm to cluster the datasets(KDDcup & CIDCD) into three and pass the clustered data into both Machine learning and Deep learning algorithms.



CLUSTERED TRAINING DATASET (Fig 1.3)



CLUSTERED TESTING DATASET (Fig 1.4)

The Proposed Random Forest Algorithm :

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of **ensemble learning,** which is a process of *combining multiple classifiers to solve a complex problem and to improve the performance of the model.*

Random Forest works in two-phase first is to create the random forest by combining N decision trees, and second is to make predictions for each tree created in the first phase.

The Working process can be explained in the below steps and diagram:

Step-1: Select random K data points from the training set.

Step-2: Build the decision trees associated with the selected data points (Subsets).

Step-3: Choose the number N for decision trees that you want to build.

Step-4: Repeat Step 1 & 2.

Step-5: For new data points, find the predictions of each decision tree, and assign the new data points to the category that wins the majority votes.

We used the clustered dataset in the random forest algorithm to find the confusion matrix and accuracy.

Also we are calculating the precision, recall & F1 score.

CONFUSION MATRIX :

Confusion Matrix is **a useful machine learning method which allows you to measure Recall, Precision, Accuracy, and AUC-ROC curve**. Below given is an example to know the terms True Positive, True Negative, False Negative, and True Negative. True Positive: You projected positive and its turned out to be true.

CONFUSION MATRIX FORMULAS :

Precision :

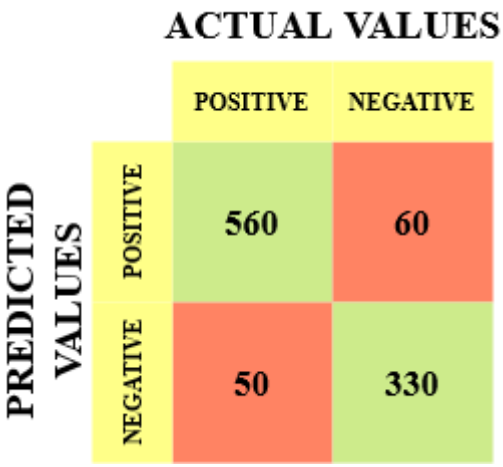
- Precision = TruePositives / (TruePositives + FalsePositives)

Recall :

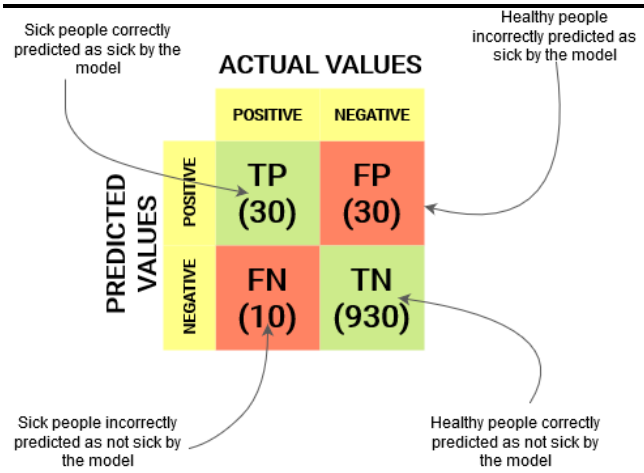
- Recall = TruePositives / (TruePositives + FalseNegatives)

f1 Score :

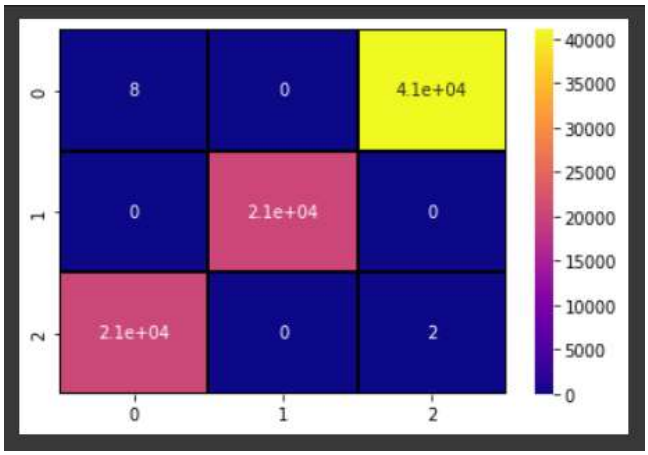
- F1 score = 2*((precision*recall)/(precision+recall))



CONFUSION MATRIX



ARCHITECTURAL DIAGRAM OF CONFUSION MATRIX



CONFUSION MATRIX OF RANDOM FOREST

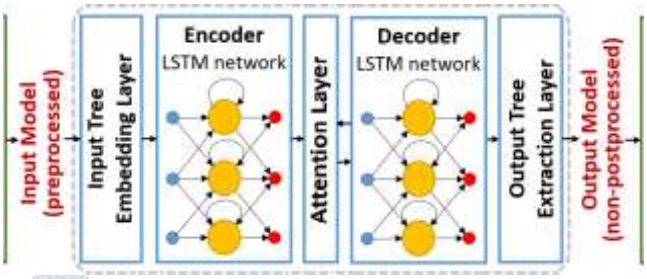
The Proposed Long Short Term Memory Algorithm :

Long short-term memory (LSTM) is an artificial recurrent neural network (RNN) architecture used in the field of deep learning. It was proposed in 1997 by **Sepp Hochreiter** and **Jurgen schmidhuber**. Unlike standard feed-forward neural networks, LSTM has feedback connections. It can process not only single data points (such as images) but also entire sequences of data (such as speech or video).

Long Short- Term Memory (LSTM) networks are a modified version of recurrent neural networks, which makes it easier to remember past data in memory

We will set up a function to build the LSTM layers to handle the number of layers and sizes dynamically. The service will take a list of LSTM sizes, which can indicate the number of LSTM layers based on the list's length (e.g., our example will use a list of length 2, containing the sizes 128 and 64, indicating a two-layered LSTM network where the first layer size 128 and the second layer has hidden layer size 64).First, we call each of the tasks we have described to build a network and call a TensorFlow session to train the model with a predefined number of epochs using mini-batches. At the end of each period, we will print losses, training accuracy, and precision accuracy to monitor results as we train the model.

- The current long-term memory of the network — known as the *cell state*
- The output at the previous point in time — known as the previous *hidden state*
- The input data at the current time step.
-



LSTM ARCHITECTURAL DIAGRAM

$$\tilde{c}_t = tanh(w_c[h_{t-1}, x_t] + b_c)$$
$$c_t = f_t * c_{t-1} + i_t * \tilde{c}_t$$
$$h_t = o_t * tanh(c^t)$$

$c_t \rightarrow cell\ state(memory)\ at\ timestamp(t).$
$\tilde{c}_t \rightarrow represents\ candidate\ for\ cell\ state\ at\ timestamp(t).$
$note^*\ others\ are\ same\ as\ above.$

Equations for the cell state, candidate cell state and the final.

Max pooling 2D :

Max pooling operation for 2D spatial data. Downsamples the input along its spatial dimensions (height and width) by taking the maximum value over an input window (of size defined by pool_size) for each channel of the input. The window is shifted by strides along each dimension.

Conv 2D :

2D convolution layer (e.g. spatial convolution over images). **This layer creates a convolution kernel that is convolved with the layer input to produce a tensor of outputs**. If use_bias is True, a bias vector is created and added to the outputs. Finally, if activation is not None , it is applied to the outputs as well.

Dropout :

"dropout" refers to **dropping out units (both hidden and visible) in a neural network**. Simply put, dropout refers to ignoring units (i.e. neurons) during the training phase of a certain set of neurons which is chosen at random.

Activation Layer:

A neural network without an activation function is essentially just a linear regression model. **The activation function does the non-linear transformation to the input making it capable to learn and perform more complex tasks**. a(1) is the vectorized form of any linear function

Dense Layer :

A dense layer is **a layer that is deeply connected with its preceding layer** which means the neurons of the layer are connected to every neuron of its preceding layer. This layer is the most commonly used layer in artificial neural network networks.

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 lstm (LSTM)                 (None, 2, 10)             480

 dropout (Dropout)           (None, 2, 10)             0

 conv1d (Conv1D)             (None, 2, 64)             1984

 max_pooling1d (MaxPooling1D  (None, 1, 64)            0
 )

 lstm_1 (LSTM)               (None, 50)                23000

 dropout_1 (Dropout)         (None, 50)                0

 dense (Dense)               (None, 1)                 51

 activation (Activation)     (None, 1)                 0

=================================================================
Total params: 25,515
Trainable params: 25,515
Non-trainable params: 0
```

LSTM LAYERS & IT'S CALCULATIONS.

SIMULATION AND RESULT ANALYSIS:

Accuracy is a metric used in classification problems used to tell the percentage of accurate predictions. We calculate it by **dividing the number of correct predictions by the total number of predictions**. This formula provides an easy-to-understand definition that assumes a binary classification problem.It is calculated as **the ratio between the number of correct predictions to the total number of predictions**.

KDDCup'99 dataset
This is a data set used by Third International Competition for Information Acquisition and Data Mining, held in partnership with KDD-99 The Fifth International Conference on Access to Information and Data Mining [9]. The task of the competition was to build a network intrusion detector, a capable forecasting model to distinguish between `` bad " communication, called input or attacks, and `` good " common communication [9]. The database contains a standard set of data to be tested, including a a variety of interference made on a military network nature.
In 1998, the DARPA access control system, a the fixed location was set to detect the raw TCP / IP discard local area network (LAN) data by MIT Lincoln Comparison performance appraisal lab for various interventions methods [9]. It worked like a real environment, but to be exploded with mass attacks and gained more attention in the research community of dynamic interventions adoption.
In the KDD99 database [9], each example represents class value attribute in network data flow, and each the class is marked as normal or aggressive.
Classes in the KDD99 database [9] can be divided into 5 large classes (one standard class and four main interventions classes: probe, DOS, U2R, and R2L)

```
Random Forest
              precision    recall  f1-score   support

           0       0.00      0.00      0.00     41032
           1       1.00      1.00      1.00     20613
           2       0.00      0.00      0.00     20687

    accuracy                           0.25     82332
   macro avg       0.33      0.33      0.33     82332
weighted avg       0.25      0.25      0.25     82332


Random Forest Accuracy is: 25.048583782733324 %

Confusion Matrix:
[[    8     0 41024]
 [    0 20613     0]
 [20685     0     2]]
```

RANDOM FOREST ACCURACY CALCULATION

```
LSTM
              precision    recall  f1-score   support

           0       0.00      0.00      0.00     41032
           1       0.33      1.00      0.50     20613
           2       0.00      0.00      0.00     20687

    accuracy                           0.25     82332
   macro avg       0.11      0.33      0.17     82332
weighted avg       0.08      0.25      0.13     82332


LSTM Accuracy is: 49.92842376232147 %

Confusion Matrix:
[[    0 41032     0]
 [    0 20613     0]
 [20496   191     0]]
```

LSTM ACCURACY CALCULATION

Finally, the Long short term memory algorithm has the more accuracy values than in the Random forest algorithm.

Insert all the attacked data in an array and attached those it into an csv file or by getting an id as an input from the use and find that the id is attacked or not. If it's attacked,we send an alert mail to the user using SMTP (Simple Mail Transfer Protocol).

The id no 78 was attacked recently, kindly check now to fix it

MAIL THREAD THROUGH GMAIL

CONCLUSION

In this project, We are finding an attacked and not attacked data set using Random Forest and LSTM. In our proposed method we are preprocessing the data set and doing feature extraction by Kmeans algorithm and then finding accuracy using Random forest and LSTM algorithm and calculating confusion matrix, etc. If the data is attacked we send an alert message to the user by mentioning the attacked data Id. In Future work, we can use real time data set to detect the attack in the files.

REFERENCES

[1] Pathan A-SK, Azad S, Khan R, et al. Security mechanisms and data access protocols in innovative wireless networks. London: Sage; 2018.

[2] Yong-xiong Z, Liang-ming W, Lu-xia Y. A network attack discovery algorithm based on unbalanced sampling vehicle evolution strategy for intrusion detection. Int J Comput Appl. 2017: 1–9.

[3] Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEE Commun Surv Tutorials. 2013;15(4):2046–2069.

[4] Toledo AL, Wang X. Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks. IEEE Trans Inf Forensics Secur. 2008;3(3):347–358.

[5] Guo Y, Ten CW, Hu S, et al. Modeling distributed denial of service attack in advanced metering infrastructure. 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT); 2015. p. 1–5

[6] Dwivedi S, Vardhan M, Tripathi S, et al. Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection. Evol Intell. 2019: 1–15.

[7] Kumar N, Singh AK, Srivastava S. Feature selection for interest flooding attack in named data networking. Int J Comput Appl. 2019:1–10.

[8] Xu W, Hu G, Ho DWC, et al. Distributed secure cooperative control under denial-of-service attacks from multiple ADVERSARIES. IEEE Trans Cybern. 2019: 1–10

[9]Generations of Machine Learning in Cybersecurity, LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.Kapratwar, A. (2016). Static and Dynamic Analysis for Android Malware Detection.

[10] Intrusion detection research," in International Conference on Critical Infrastructure Protection. Springer, 2014, pp. 65–78. DOI: 10.1007/978–3–662–45 355–1.

[12] T. N. Sainath, O. Vinyals, A. Senior, and H. Sak, "Convolutional, long short-term memory, fully connected deep neural networks," in 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2015, pp. 4580–4584. DOI:10.1109/ICASSP.2015.7 178 838.

[13] U. Adhikari, S. Pan, T. Morris, R. Borges, and J. Beave, "Industrial control system (ICS) cyber attack datasets," Accessed: Apr., 2020, https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.

[14] J. Alcala-Fdez, L. Sanchez, S. Garcia, M. J. del Jesus, S. Ventura, J. M. Garrell, J. Otero, C. Romero, J. Bacardit, V. M. Rivas et al.,"Keel: a software tool to assess evolutionary algorithms for data mining problems," Soft Computing, vol. 13, no. 3, pp. 307–318, 2009. DOI:10.1007/s00500-008-0323-y.

[15] M. Jaderberg, W. M. Czarnecki, I. Dunning, L. Marris, G. Lever, A.G.Castaneda, C. Beattie, N. C. Rabinowitz, A. S. Morcos, A. Rudermanetal., "Human-level performance in 3D multiplayer games with population-based reinforcement learning," Science, vol. 364, no. 6443,pp. 859–865, 2019. DOI: 10.1126/science.aau6249.

[16] D. Ho, E. Liang, X. Chen, I. Stoica, and P. Abbeel, "Population based augmentation: Efficient learning of augmentation policy schedules," in International Conference on Machine Learning. PMLR, 2019, pp.2731–2741.

[17] Dwivedi S, Vardhan M, Tripathi S, et al. Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection. Evol Intell. 2019: 1–15.

[18] Kumar N, Singh AK, Srivastava S. Feature selection for interest flooding attack in named data networking. Int J Comput Appl. 2019:1–10.

[19] Xu W, Hu G, Ho DWC, et al. Distributed secure cooperative control under denial-of-service attacks from multiple ADVERSARIES. IEEE Trans Cybern. 2019: 1–10

[20] A. Gumaei, M. M. Hassan, S. Huda, M. R. Hassan, G. Fortino, D.Camacho, and J. Del Ser, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," Applied Soft Computing, p. 106658, 2020. DOI: 10.1016/j.asoc.2020.106658