International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-5, September 2021
https://doi.org/10.21276/ijircst.2021.9.5.2
Article ID IRP1204, Pages 14-23
www.ijircst.org

Use of Smart Intrusion Detection System for Enhancing the Security in Hierarchical Wireless Sensor Network

Rahul Das[1], and Dr. Mona Dwivedi[2]

[1]Research Scholar, Department of Computer Science, Mansarovar Global University, Madhya Pradesh, India.
[2]Associate Professor, Department of Computer Science, Mansarovar Global University, Madhya Pradesh, India.

Correspondence should be addressed to Rahul Das; rahul.rr.das@gmail.com

ABSTRACT- Trusted environment provides safety measures for the sensor network. There are many problems that occur during the management of resources. Memory management and computation overhead or CPU usage are the major issues. Security issues is another problem in Wireless sensor network.. The three types of issues like issues of memory, computation overhead and intrusion detection is considered in this proposed research. The proposed model has provided a mechanism for resource management in a wireless sensor network. This model would also resolve one diff type of issue like computation overhead. The proposed work is capable to classify IDS attacks using a deep learning model. For improving accuracy a Network model is proposed during intrusion detection using a recurring neural network. The network model is used for testing by the help of a confusion matrix to calculate The accuracy, precision, recall and fscore. For clustered wireless sensor networks the advanced adaptive and dual data communication trust scheme (adct) have been used. Research is able to handle untrustworthy nodes inefficient manner. A function that is used in this research to assess direct trust among nodes is called Adaptive trust function. In intracluster as well as intercluster this Trust mechanism ADCT is used. With the help of compression mechanism Packets have been compressed for reducing the computation overhead. For security in Intrusion, this proposed model would also be capable. Moreover, research work would also deal with selfish nodes and malicious nodes to provide better of service for network lifetime for different network sizes.

KEYWORDS-Wireless Sensor Network, IDS, intrusion detection system, Trust management, LSTM.

I. INTRODUCTION

There are several existing researches that have contributed in field of Trust management in wireless sensor. On other hand there have been various mechanism to improve the security of Trusted using IDS. It has been observed that previous researches have made use of Fuzzy logic, Genetic algorithm, Machine learning mechanism, KNN [9] classification, LSTM model. More over previous researches have make use of NDL-KDD [12] dataset for training. But these researches are suffering from accuracy issues. Moreover the time consumption during training of network model is more. These researches have motivated to develop a model that should be trained fast as compared to previous models. Moreover previous researches have also motivated to increase the accuracy using two layer LSTM model considering hidden layer. The proposed research are supposed in provide fast training to dataset and more accurate predication as compared to previous researches.

A. Trust Management To Secure Wsn

Traditional security mechanisms cannot be used in Wireless Sensors Networks (WSNs) because they are susceptible to many security threats. Recently Trust management models is an effective security mechanism for WSNs. Considerable research has been done on modelling and managing trust by increasing security. In this paper, attacks such as IDS against trust models are considered. Moreover, the intelligent system has been proposed to predict the intrusion for trust best practices that are essential for developing a robust trust model for WSNs.

B. Trusted Network

Trust models in WSN are classified into two categories that are node trust models and data trust models. There are two categories: centralized and distributed models in trust model. In centralized trust models, a particular trusted intermediary or base station is used to calculate trust values of sensor nodes. In distributed trust models, sensor nodes calculate trust values by themselves. Trust of a sensor node is the neighbor nodes belief about its future behaviors. Given a reputation metricR_{ij}, the trust metric T_{ij} is obtained by:

$$T_{ij} = E[R_{ij}] = E[Beta(\alpha_j, \beta_j)] = \frac{\alpha_j}{\alpha_j + \beta_j}$$

In RFSN, an aging mechanism is proposed for trust updating, thus a node's trustworthiness is revaluated continuously. However, RFSN assumes that each node has enough interactions with neighbour nodes so that reputation can reach a stationary state Reputation information will not stabilize If the movement speed of a sensor node is higher. RFSN scheme only propagates good reputation information about other nodes In regards to bad mouthing attacks. In this case, sensor nodes cannot resist against conflicting behaviour attack because they cannot share their bad reputation information with each other. Parameterized and Localized trust management Scheme (PLUS) is another distributed trust computation scheme is proposed in. In

PLUS, personal reference and recommendation are used to build reasonable trust relationship among sensor the personal reference value $T_{pr(i)}$ of node i is computed based on the node's availability and the proportion of correct packets. The recommendation value $T_{r(i)}$ is calculated based on neighbor nodes' trust values and the number of neighbor nodes. Therefore, the trustworthiness of node i can be expressed as:

$$T_{(i)} = T_{pr(i)} * W_{pr} + T_{r(i)} * W_r \, , Where \, W_{pr} + W_r = 1$$

C. Intrusion Detection System

An intrusion detection system [2] has been considered as application which is capable to view network in case of any malicious operation as well as violation of given policies. Intrusion detection is playing significant role to assure the data protection of information. The main mechanism used is capable to check different types attack over network in accurate manner. Network-dependent system have been found capable to check network-connected operation such as volume of traffic, remote IP addresses, ports used, and utilized protocols. Intrusion Detection System is known as a system which is monitoring network traffic to trace suspicious activity. It also issues alerts as activity has been detected. This is known as a software application that is capable to check network. It checks system for harmful operation as well as any breach of policy. The intrusion detection system has been composed of various components. One component is sensors that are utilized to produce security events. It is triggering intrusion detection system. Another component is console. Intrusion detection systems [3] are operating by either considering signs of known attacks/deviations during usual operations. Such deviations/anomalies are pushed up stack and checked at protocol and application layer.

D. Types Of Ids

IDS are classified into 5 types:

- Network IDS
- Host IDS
- Protocol dependent IDS
- Application Protocol dependent IDS
- Hybrid IDS

E. Detection Method of IDS

Detection mechanism utilized by IDS [9] has been signature dependent and anomaly dependent.

- **Signature dependent Mechanisms**

Signature-based IDS is finding attacks over the basis of particular patterns like the number of bytes or count of 1 or count of 0 in network traffic. This is detecting according to considered invalid instruction sequences. Such sequences are utilized by malware. Found patterns in IDS have been considered as signatures. The Signature dependent IDS [10] could find attacks easily where the pattern is already present in the system. This is complex to find the latest malware attacks because such signatures are unknown.

- **Anomaly-based Mechanisms**

Anomaly-based IDS [14] has been frequently used to find unknown malware attacks because the latest malware is produced at a rapid speed. There is the utilization of machine learning to develop a significant and faithful activity model in anomaly-based IDS. Anything that is coming inside is compared to this model. These things are declared suspicious these are not present in the model. It has been observed that the Machine learning-dependent mechanism is having better features as compared to signature or pattern dependent IDS [15] system. This is because these models are trained as per the configuration of applications and hardware.

F. Deep Neural Network

A deep neural network has been considered as artificial neural network. It has several layers inside input as well as output layers. The DNN is detecting valid mathematical manipulation to product output as per input. There might be a linear relationship as well as a non-linear relationship. This is well known deep structured learning that could be utilized for hierarchical learning for IDS [18] detection. This has been considered a portion of a broader family of machine learning mechanisms. These mechanisms are dependent on artificial neural networks. Research has utilized deep thinking and quick learning for Viable AI.

G. Reinforcement Learning

Reinforcement Learning has been determined as Machine Learning. It is a branch of AI. Reinforcement Learning has been considered as a category of Machine Learning. It is also considered a branch of AI. Exactly permitter presentative of hardware and computer program to mechanically identify perfect attitude in particular circumstances, for maximizing its efficiency. Exactly a type of Machine learning method which permits representative of hardware and computer program to mechanically identified perfect attitude within a particular circumstance, for maximizing its efficiency.

H. Recurrent Neural Network

Such network has been considered as class of neural networks where interconnectivity among nodes is forming directed graph. It is also creating a temporal sequence which is allowing it to show temporal dynamic behaviour. RNNs is capable to utilize their memory to process variable length sequences of inputs as these are derived from feed forward neural networks. It is making them enable to implement operations like unsegmented as well as interconnected consideration. RNN has been utilized to take in account two different broad categories of networks that are supporting usual structure. Here one is having finite impulse. But another one is having impulse which is infinite. Such categories of networks have exhibited the runtime actions those are not permanent.

I. Long Short-Term Memory

LSTM [22] has been considered as well known artificial RNN. Such is frequently utilized in the area of deep learning. LSTM [23] is having feedback interconnection. It is not like general feed forward neural network. This is not just processing single data points such as graphics. It is also completing sequences of information like audio and video. The LSTM [24] networks are considered suitable to perform classification. It is performing processing as well as making predictions on the bases of time series information. This is because there might be lags of duration that is not known in significant events during time series. Long Short-Term Memory networks have been considered as category of recurrent

neural network. This is found capable to get taught order dependence in case of sequence prediction problem. This is a behavior needed in case of complicated issue domains like translation by machine. Long Short-Term Memory have been considered complicated field of deep learning. This is difficult to understand Long Short-Term Memory. There have been little work in field of Long Short-Term Memory.

J. Need of Research

The intrusion detection system has been considered as crucial for network security in order to improve the security of trust model. They are enabling users to find and reply to malicious traffic. The major need for intrusion detection system is to assure IT personnel is notified during attack or network intrusion is in execution. The proposed system is required to train IDS system that should be capable to predict with maximum accuracy. The trained model for intrusion detection would be made with support of LSTM and simulated in a Matlab environment. Existing researches have provided limited accuracy with limited precision, f-score, and recall value. The implementation of such a model is quite challenging but such research opens doors for innovations.

II. LITERATURE REVIEW

There are several types of research in area of trust management, intrusion detection and deep learning. Research work has focus on trust management, training and testing of IDS system with support of LSTM model. The various research papers interconnected to IDS and deep learning have been considered to accomplish objectives. The researches that have been considered during proposed work are explained in this section.

S. No	Author	Year	Title	Methodology
1.	Momani,	2010	Survey of trust models in different network domains	Trust model
2.	Han,	2014	Management and applications of trust in Wireless Sensor Networks: A survey	Trust management for WSN
3.	Karthik,	2011	Trust management techniques in wireless sensor networks: an evaluation	Trust management for WSN
4.	Dhulipala,	2017	Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review	Trust management for WSN
5.	Bao,	2012	Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection	Trust management for WSN
6.	Ullah, Imtiaz,	2020	A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks	Anomalous activity detection
7.	Buczak, Anna L.,	2015	A survey of data mining and machine learning methods for cyber security intrusion detection and Erhan Guven.	IDS
8.	A.Javaid,	2016	A deep learning approach for network intrusion detection system	Deep learning for IDS
9.	Tang, Tuan A.,	2016	Deep learning approach for network intrusion detection in software defined networking	Deep learning for IDS
10.	M. Sheikhan,	2012	Intrusion detection with support of reduced-size RNN dependent on feature grouping	IDS using RNN
11.	Tavallaee,	2009	A detailed analysis of the KDD CUP 99 data set	IDS
12.	Revathi,	2013	A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection	IDS
13.	Paulauskas,	2017	Analysis of data pre-processing influence on intrusion detection using NSL-KDD dataset	IDS
14.	Bhattacharje e,	2017	Intrusion detection system for NSL-KDD data set using vectorised fitness function in genetic algorithm	IDS
15.	Ashfaq,	2017	Fuzziness based semi-supervised learning approach for intrusion detection system	Fuzzy logic

III. PROPOSED WORK

The proposed trust model is using LSTM mechanism to train seventy percent of the dataset and testing on thirty percent of the dataset.

A. Process Flow of Deep LSTM IDS to increase security of Trust Model

Deep LSTM IDS is powerful tool to secure the network. It makes use of different deep learning techniques to train our network. There are various steps with different techniques involves in making an IDS. The proposed work deals with various phases

- Dataset selection
- Preprocessing
- Training
- Testing

a) Dataset

The first phase deals with the selection of the dataset. The Dataset is a group of records also known as a group of data. The data set is corresponding to one or more database tables for tabular data. Every column of a table is presenting a particular variable. Here every row is corresponding to a given record of data set. These records stored in the dataset are representing information of the entity. The entity is an object regarding which dataset has been created. There is the existence of multiple columns also known as an attribute to represent the feature of an entity. Multiple similar records with a group of the attribute are stored in the dataset. In IDS data set is consisting of eighty network characteristics along with three label characteristics. The label characteristics are binary, category, and sub-category. In the dataset, records are stored vertically while attributes are presented horizontally. Datasets have been considered as a basic requirement to foster the development of multiple computational fields. It is providing scope, robustness to results. Datasets are becoming famous with the advent of AI, machine learning along deep learning. Then some portion dataset has been utilized during testing. During testing, the dataset portion is processed with a network model to get a confusion matrix. The confusion matrix is also depending on the dataset.

b) Preprocessing

In the previous phase after selecting the dataset, there is a need to clean the data, also known as preprocessing. It is very important to preprocess the dataset before training. During preprocessing useless attributes that are not playing any significant role in decision making is eliminated. Also, it takes care of the missing value. The Shapiro–Wilk [64] algorithm has been utilized to eliminate such attributes considering their significance. Data preprocessing is a process that is performed on raw data before training it. This algorithm has been utilized to eliminate attributes. The Shapiro-Wilk algorithm [64] checks regularity of distribution of occurrences to characteristics& removed characteristics with less than a .5 ranking score. Thus it is helping in eliminating attributes utilized in the dataset based on their ranking score. On the other hand, attributes that are consisting of common value are also eliminated. The preprocessing helps in reducing useless attributes to speed up the training process. Moreover, accuracy is also increased if attributes with significant characteristics are kept. The data preprocessing is performing the following operations .Eliminating attributes with less ranking score with support of Shapiro wilk algorithm.

c) Neutral Network Based Ids

It is one of the important fields that deals set up of the neural network .Neural network models are performing supervised learning operation. It is building knowledge from IDS data sets. It is considering the right answer that has been provided in advance. Networks are then learning by tuning themselves to detect the right answer by themselves. These are trying to increase accuracy during predictions. These neural networks could be utilized to solve several issues. These issues might be interconnected to network security like intrusion detection. These issues may be interconnected to other applications like sales forecasting, customer research. Other issues are the validation of data along with the management of risk.

B. LSTM and Its Training Mechanism

The trained network "net" is stored in the system for further testing. The LSTM has been implemented with two LSTM layers to produce a trained network. The proposed model is making use of two LSTM layer along with drop out layer during a training operation. To perform training 70% dataset is considered for training and the remaining 30% to perform the test. Based on feature LSTM dependent neural is trained. The factors that are influencing the time of training are batch size. The hidden layers and dropout layers are playing a significant role in increasing accuracy. After getting a dataset of IDS the selection of characteristics is performed to train the dataset. The ratio of training and testing is set then LSTM1 layer with 12 hidden layers and LSTM2 layer with 5 hidden layers. Dropout layers are used to resolve the issue of overfitting then fully connected layer and softmax layer are applied. Classification operation is performed to perform decision making to predict intrusion.

C. LSTM layer

In our research, the LSTM mechanism is being considered to train the network which uses deep learning and it makes use of feedback interconnection. In the proposed model, LSTM networks have been used to perform the classification of IDS attack with the support of hidden layers, dropout layers, fully connected, and classification layers. LSTM mechanism has been used to perform processing as well as making predictions based on the given IDS dataset. Different anomalies that are classified by the trained model. Two LSTM has been used to the model the IDS & they have been joined consecutively. Each has different hidden layers i.e. 12 and 5 respectively. These hidden layers have increased the accuracy but cause the issue of overfitting. The issue of overfitting arises during the training of the neural network model. If the training is continued then the model will adopt idiosyncrasies. These layers have a learning long-term dependencies. It learns from different time steps lying in time series along sequence contents. It performs additive interactions. The layers are supposed to enhance gradient flow in long sequences during training.

International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-5, September 2021
https://doi.org/10.21276/ijircst.2021.9.5.2
Article ID IRP1204, Pages 14-23
www.ijircst.org

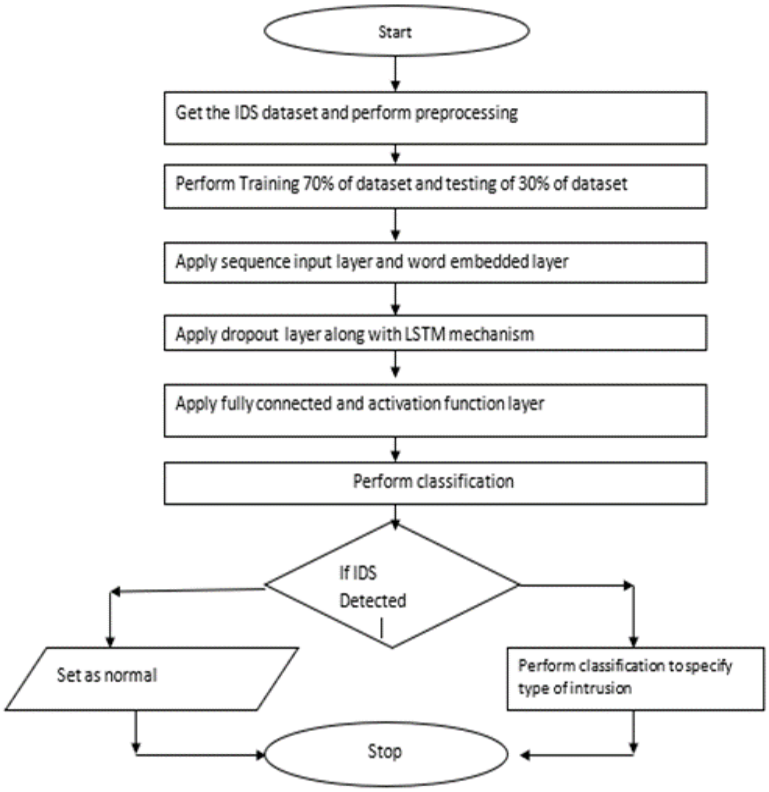


Fig. 1: Flowchart of Proposed work to enhance security of trusted model

D. *Testing Phase*

The testing phase where the accuracy of the trained model is checked. The sample dataset is taken to test the accuracy of the model. The network model trained by the previous dataset is process processed with various datasets to perform prediction. The testing face presents the reliability of the model. In the testing phase trained network is considered is supervised. Then the dataset for testing is taken. The data considered for testing is then processed with a trained network to find accuracy, f-score, and precision considering new test values. For our analysis, let train model on first 70% of data and test it on remaining 30%.

IV. RESULT AND ANALYSIS

In the proposed work MATLAB (2020 a) has been used as a simulation tool. MATLAB is used in different sectors of education such as mathematics, academies. It is mostly useful in Universities for research purposes. MATLAB allows the execution of computationally tasks quicker as compare to other languages. It has several toolboxes such as image toolbox, Simulink, simscape, etc. Matlab is allowing performing tasks rapidly. It is performing better than languages. Other Programming languages allow the user to perform tasks at a time. On the other hand, MATLAB offers to work within complete matrices quickly & easily. In the proposed work the training of the network has been performed using the IDS dataset. Two LSTM layers have been used in the proposed simulation environment. The hidden layers, Batch size parameters are also defined simulation. The following figure is showing a simulation environment MATLAB to implement the proposed LSTM model.

A. Deployment Model

To simulate the deployment model that considers the training of a dataset that is consisting record related to IDS. The model has been used to perform accurate classification in IDS. Before the training network model, there is a need for dataset pre-processing. Then data is classified as 70% for training and 30% for testing. In the proposed deployed model two LSTM layers are used. 12 hidden layers are used in the first LSTM layer and 5 hidden layers are used in the second LSTM layer. However hidden layer has a quality of retaining the previous value but it also raises a problem overfitting that network will not be robust and will increase the loss function, it will make network to be useless when there is need for new dataset or new values of data thus there is need of improvement in the network. Classification layers are used to perform different predictions of different attacks in IDS. After the training of the network model, testing is performed on the dataset. 30% of the dataset has been used for the testing of IDS. Afterward, a confusion matrix is produced considering predicted and actual value to get True positive, False positive, True negative, False negative. The accuracy, precision, recall, f-score is obtained to get overall accuracy.

- ***Performance Parameters***

The confusion matrix is produced presenting True positive (TP), True negative(TN),False positive(FP), False negative(FN).

True positives: True positive have been considered as predicted positive data. It is the value of the actual class that is found true and the result of the predicted class has been also true.

True negatives: True Negatives have been known as predicted negative values that are correct. This means the value of the real class is has been found no and the result of the predicted class has been also no. False positives and false negatives, such values are occurring when the real class result is not matching with the result of the predicted class.

False positives: It is the case when the real class is no but the output of the predicted class has been found yes.

False negatives: It is the case where the real class is yes on the other hand predicted class is saying no. The parameters utilized for verifying results are accuracy, precision, recall, and f-score that are discussed below:

- ***Accuracy***

It is considered the most intuitive measurement of performance. This is known as the proportion of the right predicted findings to total findings. It is considered that if the accuracy of the model is high then the model is best. Accuracy has been considered as a good measure. The condition is that users should have symmetric datasets. Here values of false-positive, as well as false negatives, are mostly equal.

Accuracy (A) = True positive + True Negative/ True positive + False positive + False negative + True Negative

Precision: It has been considered as a proportion ratio of right predicted positive results with overall predicted positive findings.

Precision (P) = True positive / True positive + False positive

Recall: It is representing sensitivity and is considered as a proportion of right predicted positive findings to all findings in real class true.

Recall (R) = True Positive / True Positive + False Negative

F-score: It has been considered as a weighted average of precision as well as recall. So, the score is considering false positives and false negatives both. The significance of F-score is considered more as compare to accuracy.

F-score = 2 x (R x P) / (R + P)

- Simulation
- Simulation Of Proposed Lstm

The training is one of the important steps in IDS. Gradually the progress of the model is increasing. The progress simulation has been the following figure.

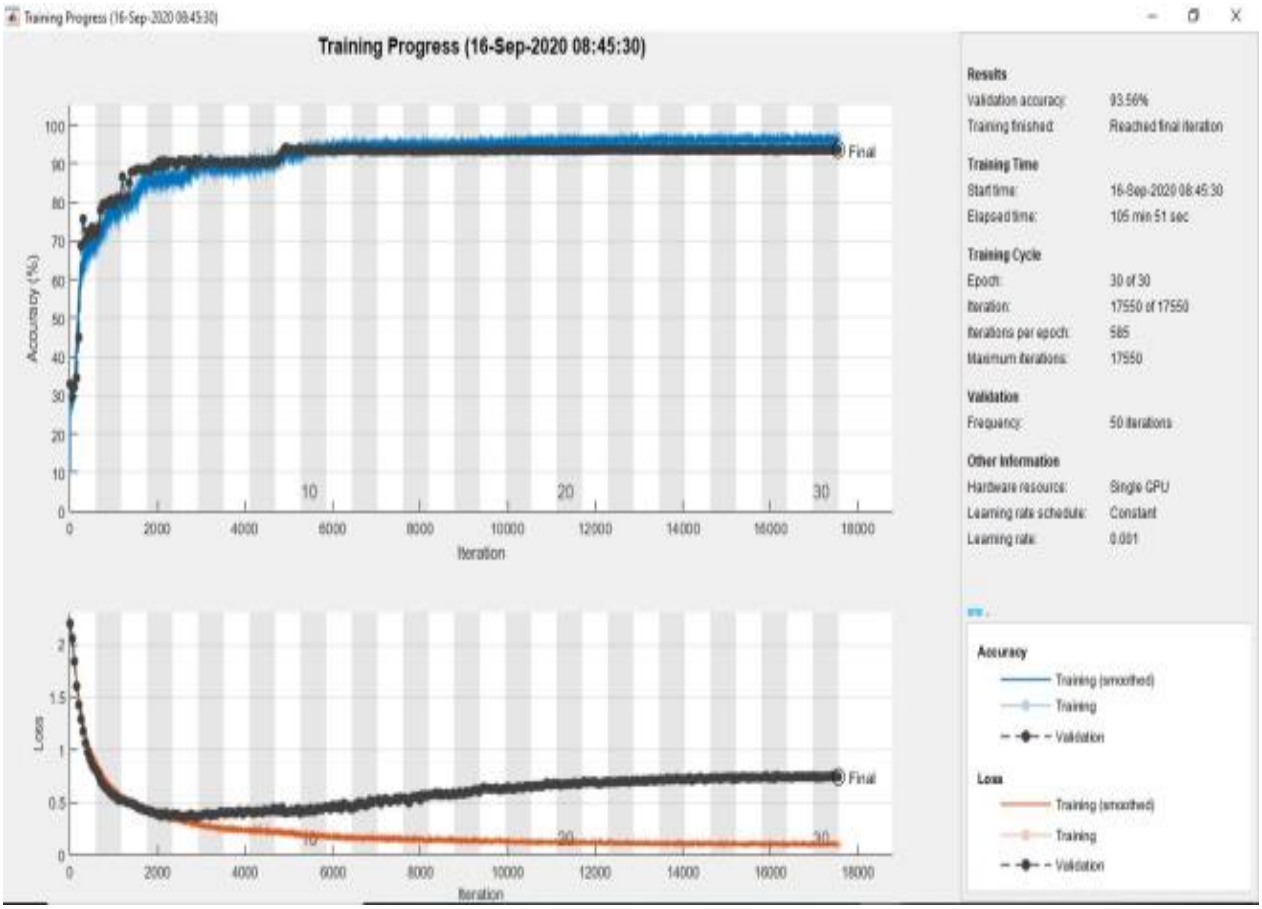


Fig. 2: Progress simulation

- ***Confusion matrix***

After training of the dataset testing module is run then the confusion matrix is generated. The following confusion matrix is considering 9 attributes. The true classes are presented on the y-axis and predicted classes are presented on the x-axis. With the help of this matrix we can calculate

different parameters to the efficiency of the system also we can compare them

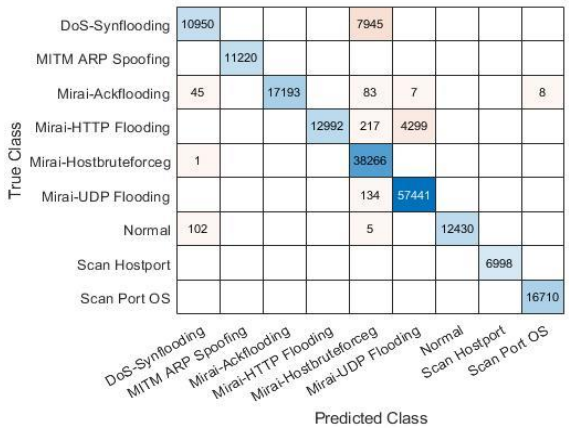


Fig. 3: Confusion Matrix of proposed model

B. Result

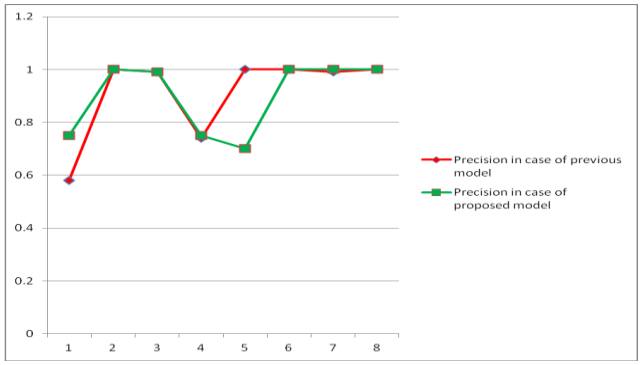
Considering the above confusion matrix chart presenting accuracy, precision, recall value, and f-score is generated. The accuracy chart in the case of existing work is presented below(table 1).

Table 1: Accuracy chart of proposed model

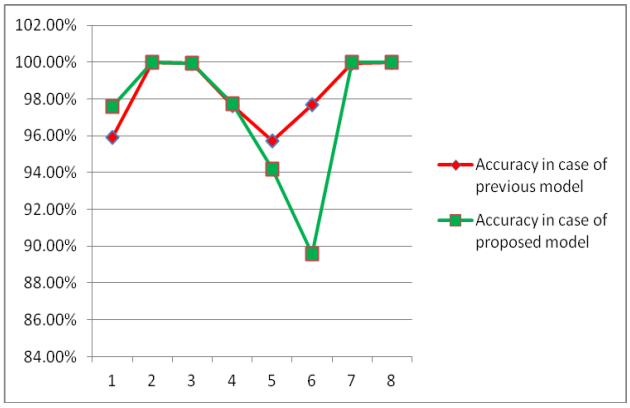
Class	n (truth)	n(classified)	Accuracy	Precision	Recall	F-Score
1	4246	5674	97.5%	0.75	1.0	0.86
2	3370	3370	100.0%	1.00	1.0	1.0
3	5177	5207	99.9%	0.99	1.0	1.0
4	3926	5258	97.7%	0.75	1.0	0.85
5	8127	11490	94.1%	0.70	0.99	0.82
6	23454	17289	89.5%	1.00	0.74	0.85
7	3744	3756	99.9%	1.00	1.0	1.0
8	2101	2101	100.00%	1.00	1.0	1.0
9	5018	5018	100.00%	1.00	1.0	1.0

V. COMPARISON IN CASE OF PREVIOUS AND PROPOSED WORK

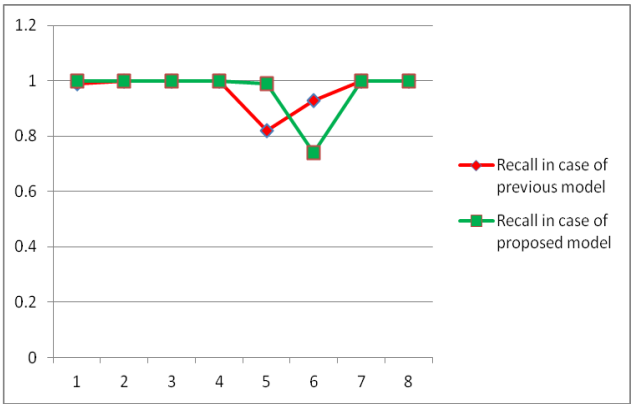
The comparison of the proposed work and traditional LSTM model with a single layer is presented below. The following chart is presenting that the proposed work has more accuracy, precision value, recall value, and F-scores value as compare to previous LSTM. The comparison chart for accuracy in case of previous and proposed is shown below:



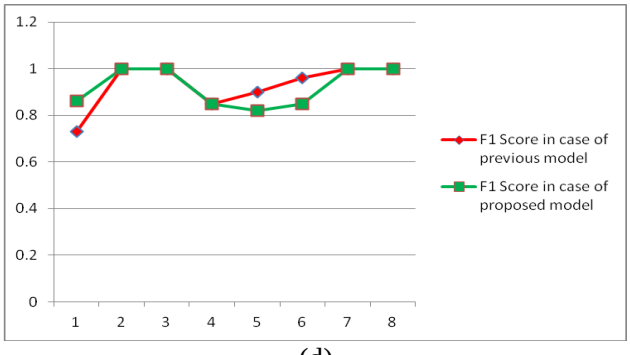
(a)



(b)



(c)



(d)

Fig. 4: Comparison of Proposed and previous in case of Accuracy, Precision, Recall value, F1 Score

Following chart is presenting comparison of accuracy, precision, recall and F-score in case of previous and proposed LSTM model. It has been observed that there is

slight change in recall value but there is significant difference in F1score.

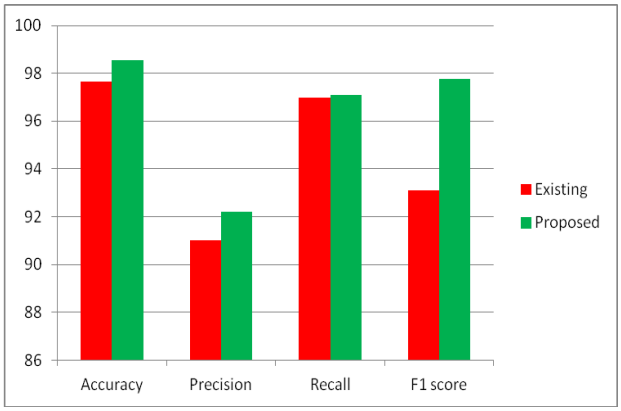


Fig. 5: Comparison of Proposed and previous LSTM model

VI. CONCLUSION

It has been concluded that the proposed IDS model has increased the security of Trust model. Research has made comparison among previous and proposed work. Results are presenting that accuracy of proposed model has been increased significantly. Accuracy is intuitive measurement of performance while precision is presenting the proportion ratio of right predicted positive results. Recall is representing sensitivity and is considered as a proportion of right predicted positive findings to all findings in real class true. F-score is weighted average of precision as well as recall.

VII. SCOPE OF RESEARCH

The research would play a significant role in predicting IDS with high accuracy in order to build trusted model. The proposed work has provided a scalable and flexible approach to perform IDS detection considering the training model. The probability of error would be less while calculating overall accuracy as the proposed model has made use of a huge dataset for training and utilized the LSTM model with multiple layers. Future research could have the benefit of rapid training from this research.

REFERENCE

[1] Momani, M., & Challa, S. (2010). Survey of trust models in different network domains. arXiv preprint arXiv:1010.0168.

[2] Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.

[3] Karthik, S., Vanitha, K., & Radhamani, G. (2011, February). Trust management techniques in wireless sensor networks: an evaluation. In 2011 International Conference on Communications and Signal Processing (pp. 328-330). IEEE.

[4] Dhulipala, V. S., & Karthik, N. (2017). Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. CSI Transactions on ICT, 5(3), 281-294.

[5] Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management, 9(2), 169-183.

[6] Li, Wenchao, Ping Yi, Yue Wu, Li Pan, and Jianhua Li. "A new intrusion detection system based on KNN classification algorithm in wireless sensor network." Journal of Electrical and Computer Engineering 2014 (2014).

[7] Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications surveys & tutorials 18, no. 2 (2015): 1153-1176.

[8] A.Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. "A deep learning approach for network intrusion detection system." In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26. 2016.

[9] Tang, Tuan A., Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, and Mounir Ghogho. "Deep learning approach for network intrusion detection in software defined networking." In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 258-263. IEEE, 2016.

[10] M. Sheikhan, Z. Jadidi, and A. Farrokhi, ‘‘Intrusion detection with support of reduced-size RNN dependent on feature grouping,’’NeuralComput. Appl.,vol. 21, no. 6, pp. 1185–1190, Sep. 2012.

[11] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6. IEEE, 2009..

[12] Revathi, S., and A. Malathi. "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection." International Journal of Engineering Research & Technology (IJERT) 2, no. 12 (2013): 1848-1853..

[13] Paulauskas, Nerijus, and Juozas Auskalnis. "Analysis of data pre-processing influence on intrusion detection using NSL-KDD dataset." In 2017 open conference of electrical, electronic and information sciences (eStream), pp. 1-5. IEEE, 2017..

[14] Bhattacharjee, Partha Sarathi, Abul Kashim Md Fujail, and Shahin Ara Begum. "Intrusion detection system for NSL-KDD data set using vectorised fitness function in genetic algorithm." Adv. Comput. Sci. Technol. 10, no. 2 (2017): 235-246..

[15] Ashfaq, Rana Aamir Raza, Xi-Zhao Wang, Joshua Zhexue Huang, Haider Abbas, and Yu-Lin He. "Fuzziness based semi-supervised learning approach for intrusion detection system." Information Sciences 378 (2017): 484-497..

[16] Martens, James, and Ilya Sutskever. "Learning recurrent neural networks with hessian-free optimization." In Proceedings of the 28th international conference on machine learning (ICML-11), pp. 1033-1040. 2011..

[17] Pichotta, Karl, and Raymond J. Mooney. "Learning Statistical Scripts with LSTM Recurrent Neural Networks." In AAAI, pp. 2800-2806. 2016.

[18] Khan, Muhammad Ashfaq, Md Karim, and Yangwoo Kim. "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network." Symmetry 11, no. 4 (2019): 583..

[19] Althubiti, S. A., Jones, E. M., & Roy, K. (2018, November). Lstm for anomaly-dependent network intrusion detection. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-3). IEEE.

[20] Kim, Chanho, Fuxin Li, and James M. Rehg. "Multi-object tracking with neural gating using bilinear lstm." In Proceedings of the European Conference on Computer Vision (ECCV), pp. 200-215. 2018.

[21] Bansal, Ashu. "Ddr scheme and lstm rnn algorithm for building an efficient ids." PhD diss., 2018..

[22] Zhao, Zheng, Weihai Chen, Xingming Wu, Peter CY Chen, and Jingmeng Liu. "LSTM network: a deep learning

approach for short-term traffic forecast." IET Intelligent Transport Systems 11, no. 2 (2017): 68-75..
[23] Tan, Ming, Cicero dos Santos, Bing Xiang, and Bowen Zhou. "Lstm-based deep learning models for non-factoid answer selection." arXiv preprint arXiv:1511.04108 (2015)..
[24] Gensler, André, Janosch Henze, Bernhard Sick, and Nils Raabe. "Deep Learning for solar power forecasting—An approach using AutoEncoder and LSTM Neural Networks." In 2016 IEEE international conference on systems, man, and cybernetics (SMC), pp. 002858-002865. IEEE, 2016..
[25] Sun, Lei, Jun Du, Li-Rong Dai, and Chin-Hui Lee. "Multiple-target deep learning for LSTM-RNN based speech enhancement." In 2017 Hands-free Speech Communications and Microphone Arrays (HSCMA), pp. 136-140. IEEE, 2017..
[26] Li, Peisong, and Ying Zhang. "A Novel Intrusion Detection Method for Internet of Things." In 2019 Chinese Control And Decision Conference (CCDC), pp. 4761-4765. IEEE, 2019..
[27] Yin, Chuanlong, Yuefei Zhu, Jinlong Fei, and Xinzheng He. "A deep learning approach for intrusion detection using recurrent neural networks." Ieee Access 5 (2017): 21954-21961..
[28] Dong, Bo, and Xue Wang. "Comparison deep learning method to traditional methods using for network intrusion detection." In 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), pp. 581-585. IEEE, 2016.
[29] Althubiti, Sara A., Eric Marcell Jones, and Kaushik Roy. "Lstm for anomaly-based network intrusion detection." In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-3. IEEE, 2018..
[30] Li, Wenchao, Ping Yi, Yue Wu, Li Pan, and Jianhua Li. "A new intrusion detection system based on KNN classification algorithm in wireless sensor network." Journal of Electrical and Computer Engineering 2014 (2014)..
[31] Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications surveys & tutorials 18, no. 2 (2015): 1153-1176..
[32] Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. "A deep learning approach for network intrusion detection system." In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26. 2016..
[33] Tang, Tuan A., Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, and Mounir Ghogho. "Deep learning approach for network intrusion detection in software defined networking." In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 258-263. IEEE, 2016..
[34] M. Sheikhan, Z. Jadidi, and A. Farrokhi, ‘‘Intrusion detection with support of reduced-size RNN dependent on feature grouping,’’NeuralComput. Appl.,vol. 21, no. 6, pp. 1185–1190, Sep. 2012.
[35] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6. IEEE, 2009..
[36] Revathi, S., and A. Malathi. "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection." International Journal of Engineering Research & Technology (IJERT) 2, no. 12 (2013): 1848-1853..
[37] Paulauskas, Nerijus, and Juozas Auskalnis. "Analysis of data pre-processing influence on intrusion detection using NSL-KDD dataset." In 2017 open conference of electrical, electronic and information sciences (eStream), pp. 1-5. IEEE, 2017..
[38] Bhattacharjee, Partha Sarathi, Abul Kashim Md Fujail, and Shahin Ara Begum. "Intrusion detection system for NSL-KDD data set using vectorised fitness function in genetic algorithm." Adv. Comput. Sci. Technol. 10, no. 2 (2017): 235-246..
[39] Ashfaq, Rana Aamir Raza, Xi-Zhao Wang, Joshua Zhexue Huang, Haider Abbas, and Yu-Lin He. "Fuzziness based semi-supervised learning approach for intrusion detection system." Information Sciences 378 (2017): 484-497..
[40] Martens, James, and Ilya Sutskever. "Learning recurrent neural networks with hessian-free optimization." In Proceedings of the 28th international conference on machine learning (ICML-11), pp. 1033-1040. 2011..
[41] Song, S., Huang, H., &Ruan, T. (2019). Abstractive text summarization with support of LSTM-CNN dependent deep learning. Multimedia Tools and Applications, 78(1), 857-875.
[42] Liu, Hui, Xiwei Mi, and Yanfei Li. "Smart multi-step deep learning model for wind speed forecasting based on variational mode decomposition, singular spectrum analysis, LSTM network and ELM." Energy Conversion and Management 159 (2018): 54-64..
[43] Lu, Na, Yidan Wu, Li Feng, and Jinbo Song. "Deep learning for fall detection: Three-dimensional CNN combined with LSTM on video kinematic data." IEEE journal of biomedical and health informatics 23, no. 1 (2018): 314-323..
[44] Mohan, Arvind T., and Datta V. Gaitonde. "A deep learning based approach to reduced order modeling for turbulent flow control using LSTM neural networks." arXiv preprint arXiv:1804.09269 (2018)..
[45] Reddy, Bhargava K., and Dursun Delen. "Predicting hospital readmission for lupus patients: An RNN-LSTM-based deep-learning methodology." Computers in biology and medicine 101 (2018): 199-209..
[46] Mohan, Arvind, Don Daniel, Michael Chertkov, and Daniel Livescu. "Compressed convolutional LSTM: An efficient deep learning framework to model high fidelity 3D turbulence." arXiv preprint arXiv:1903.00033 (2019)..
[47] Chen, Jinyin, Jian Zhang, Xuanheng Xu, Chenbo Fu, Dan Zhang, Qingpeng Zhang, and Qi Xuan. "E-lstm-d: A deep learning framework for dynamic network link prediction." IEEE Transactions on Systems, Man, and Cybernetics: Systems (2019)..
[48] Abdullah, Malak, Mirsad Hadzikadicy, and Samira Shaikhz. "SEDAT: sentiment and emotion detection in Arabic text using CNN-LSTM deep learning." In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 835-840. IEEE, 2018..
[49] Balouji, Ebrahim, Irene YH Gu, Math HJ Bollen, Azam Bagheri, and Mahmood Nazari. "A LSTM-based deep learning method with application to voltage dip classification." In 2018 18th International Conference on Harmonics and Quality of Power (ICHQP), pp. 1-5. IEEE, 2018...
[50] Shen, Shui-Long, Pierre Guy Atangana Njock, Annan Zhou, and Hai-Min Lyu. "Dynamic prediction of jet grouted column diameter in soft soil using Bi-LSTM deep learning." Acta Geotechnica (2020): 1-13..
[51] Prakash, Aaditya, Sadid A. Hasan, Kathy Lee, Vivek Datla, Ashequl Qadir, Joey Liu, and Oladimeji Farri. "Neural paraphrase generation with stacked residual lstm networks." arXiv preprint arXiv:1610.03098 (2016)..
[52] Tong, Weitian, Lixin Li, Xiaolu Zhou, Andrew Hamilton, and Kai Zhang. "Deep learning PM 2.5 concentrations with bidirectional LSTM RNN." Air Quality, Atmosphere & Health 12, no. 4 (2019): 411-423..
[53] Mohan, Arvind, Don Daniel, Michael Chertkov, and Daniel Livescu. "Compressed convolutional LSTM: An efficient deep learning framework to model high fidelity 3D turbulence." arXiv preprint arXiv:1903.00033 (2019)..
[54] Wang, Fei, Yili Yu, Zhanyao Zhang, Jie Li, Zhao Zhen, and Kangping Li. "Wavelet decomposition and convolutional LSTM networks based improved deep learning model for

solar irradiance forecasting." Applied Sciences 8, no. 8 (2018): 1286..
[55] Bouktif, Salah, Ali Fiaz, Ali Ouni, and Mohamed Adel Serhani. "Multi-sequence LSTM-RNN deep learning and metaheuristics for electric load forecasting." Energies 13, no. 2 (2020): 391..
[56] Wang, Ziyi, Aiying Yang, Peng Guo, and Pinjing He. "OSNR and nonlinear noise power estimation for optical fiber communication systems using LSTM based deep learning technique." Optics express 26, no. 16 (2018): 21346-21357..
[57] Liu, Yangdong, Yizhe Wang, Xiaoguang Yang, and Linan Zhang. "Short-term travel time prediction by deep learning: a comparison of different LSTM-DNN models." In 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), pp. 1-8. IEEE, 2017..
[58] Kumar, Sumit, Lasani Hussain, Sekhar Banarjee, and Motahar Reza. "Energy load forecasting using deep learning approach-LSTM and GRU in spark cluster." In 2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT), pp. 1-4. IEEE, 2018..
[59] Yuan, Xiaofeng, Lin Li, Yuri Shardt, Yalin Wang, and Chunhua Yang. "Deep learning with spatiotemporal attention-based LSTM for industrial soft sensor model development." IEEE Transactions on Industrial Electronics (2020)..
[60] https://datasilk.com/intrusion-detection-prevention
[61] https://towardsdatascience.com/training-deep-neural-networks-9fdb1964b964
[62] https://adventuresinmachinelearning.com/keras-lstm-tutorial
[63] https://www.researchgate.net/profile/Syariful_Shamsudin/publication/299390844/figure/fig5/AS:650029635235894@1531990550259/The-representation-of-neural-network-training-process.png
[64] Royston, Patrick. "Approximating the Shapiro-Wilk W-test for non-normality." Statistics and computing 2, no. 3 (1992): 117-119.

ABOUT THE AUTHORS

Rahul Das is a Research Scholar in Computer Science Department, Mansarovar Global University. Billkisganj, Sehore, Madhya Pradesh-466001.He is currently working as a teacher in the Department of Computer Science, Raja Narendralal Khan Women's college, Paschim Medinipur, West Bengal. He has received BCA degree in 2005 and Master's (MCA) under Vidyasagar University,2009 and B. Ed degree. He has 10 Years of teaching Experience in College. His research interest Security in Wireless Sensor Network.

Dr. Mona Dwivedi is currently working as an Assistant Professor in the Department of Computer Science at Mansarovar Global University, Billkisganj, Sehore, Madhya Pradesh, India. She received her M.Sc. and M.Phil. degree from Barkatullah University, Bhopal, M.P., India. Dr Dwivedi received her Ph.D. degree from Maulana Azad National Institute of Technology, Bhopal, India. Her research interest includes Green Computing, High Performance Computing, Wireless Sensor Networks, Numerical Analysis and Computational Modeling.