Machine Learning Applications in Engineering Education and Management

ISSN: ***Applied***

Volume ***02*** *Issue* ***01 Year 2022*** *Page* ***20:29***

Intrusion Detection System Attack Detection and Classification Model with Feed-Forward LSTM Gate in Conventional Dataset

[1]Dr. Pravin R. Kshirsagar, [2]Dr. Rakesh Kumar Yadav, [3]Dr. Nitin Namdeo Patil, [4]Mali Makarand L

[1]G.H. Raisoni College of Engineering, Nagpur
[2]Department of Computer Science & Engineering, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Lucknow,
[3]Associate Professor, R. C. Patel Institute of Technology, Shirpur
[4]R C Patel Institute of Technology Shirpur
[1]pravinrk88@yahoo.com, [2]rkyiftmuniversity@yahoo.com, [3]er.nitinpatil@gmail.com, [4]malimakarand1@gmail.com

Article History

Received: 22 January 2022
Revised: 14 April 2022
Accepted: 19 May 2022

Abstract

With the increased network scale, intrusion detection is more frequent, advanced, and volatile for capturing large scale is challenging. The increased malicious attacks in the network system affect the security tool in the network causing illegal users, reliability, and robustness for network security. Recently, network security is increased with the illegal intrusion detection system for the security in each occasion for the sensitive users, governments, enterprises and governments. Network Intrusion Detection (NIDS) exhibits a reliable and effective technological form for the packets in the network, unauthorized users, and traffic monitoring for the computer network. The incorporation of the machine learning model exhibits effective performance for network traffic monitoring. Additionally, the NIDS model exhibits effective attack detection and traffic malicious activities in the network. Through intelligent capability, the machine learning model comprises of intrusion detection based on rule-based solution for the network attacks. This paper proposed a Long Short Term Memory Gate Recurrent Neural Network (LSTMgateRNN). The constructed LSTMgateRNN model comprises of the LSTM features for the attribute evaluation for the attack data processing. The incorporation of the gate function within the network the incorporated gate function increases the evaluation of the attributes in the network. Finally, the processed data is examined with the RNN model to perform the attack detection and classification. The proposed LSTMgateRNN model performance is evaluated for the three different datasets such as KDD'99, NSL-KDD and UNSW-SW15. Simulation analysis exhibited that proposed LSTMgateRNN model achieves an attack detection rate of 99%. The proposed LSTMgateRNN is comparatively examined with the with the existing model and achieves the ~6 – 12% improved performance.

Keywords: Intrusion Detection System (IDS), Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), Attacks, Machine Learning

1. Introduction

In the present scenario, significant advancement of computer systems completely changed our daily lives and made our existence dependant on them [1]. From small companies to large enterprises, individuals to government agencies, many of their activities are performed through network services. With the tremendous growth of the use of Internet, our computer systems are exposed to elevate high number of threats [2]. Any vulnerability in the network devices and computing platforms can expose the network system under various attacks and may lead to catastrophic consequences. However, it is a nightmare for organizations and corporation's security managers to prevent their networks from being attacked and to preserve their secretes and sensitive information of their customers from leaking out [3]. Conventional network intrusion detection systems (NIDS) are signature or rule-based approaches that have not been adequate for the fast-growing network and unable to deal with attacks of their growing volume, complexity, and deflation [4].

The firewall is built to protect the entire network or systems from unauthorized access. The firewall and its variants have been shown that it could be easily bypassed by intruders, for instance, by using false source address [5]. It also failed to detect so many attacks such as DoS and DDoS. To resolve the limitation associated with the security scheme Intrusion Detection System (IDS) is deigned [6]. IDS involved in the process monitoring for the computer system for the examination of the possible events in the network to compute the anomaly activities in the network through the effective security policies or regulatory schemes. The anomaly events comprise of the malicious code to access the system through the utilization of the Internet or privileged users for the maximized privileges [7]. An intrusion detection system (IDS) is software that maintains the mechanism of intrusion detection. The IDS is concentrated primarily on the detection of potential incidents. That is, IDS could identify when an intruder has adeptly breached a system by exploiting system vulnerability [8]. Many IDS can be equipped with a collection of firewalls rules-such as settings, encouraging them to detect network traffic that breaches the security or permissible use policies of the organization. Some IDSs can supervise data transmission and recognize suspicious ones, such as copying a massive database to a user's machine [9].

IDSs are mainly concentrating on detecting possible incidents. The IDS can make report to security administrators, who can instantly start incident response actions to minimize the effect caused by the incident [10]. The IDS also manage log information that can be used by system administrators. Numerous Intrusion Detection systems are configured to identify the infringements of security policies. IDS is now an important component of computer security for detecting attacks before they cause extensive damage and the era of intrusion detection has got considerable attention in the recent years [11]. Intrusion detection scheme aimed to provides the confidentiality, availability and integrity for the computer resources in the untrusted manner [12]. Similarly, those incidents are breach based on the prevented authorized user access for the service resources within the computer. IDS observe the instances for the monitoring of the incidents for the analysis of the network intrusions. An IDS is a software or hardware that streamlines the mechanism of monitoring and analysis of incidents. IDS monitors the inbound and outbound traffic for the purpose of suspicious ones. IDS can be categorized regarding its placement or the technique it uses to detect abnormal activities [13]. With respect to its placement, IDS could be located at terminals to protect them from being attacked hence it is called Host-based IDS (HIDS). The IDS monitors incoming and outgoing packets at network entry to detect malicious ones in order to protect the whole network is called Network-based IDS (NIDS).

In this paper proposed an effective attack detection and classification model for the machine learning model. The developed model is defined as the LSTMgateRNN model for the network attack detection and classification. The proposed LSTMgateRNN model uses the autoencoder LSTM model uses the machine learning model RNN model for the dataset attack classification and detection. The LSTMgateRNN model is evaluated for the consideration of three different datasets such as KDD'99, NSL-KDD and UNSW-SW15. The comparative analysis expressed that proposed LSTMgateRNN model achieves the higher accuracy value of 99%. This paper is presented as follows: Section 2 provides the related works focused on the existing machine learning model for the attack classification. Section 3 the proposed LSTMgateRNN model for the attack processing is presented. In section 4 the proposed LSTMgateRNN model results are presented for the different datasets and overall conclusion is presented in section 5.

2. Related Works

In [14] proposed Hidden naïve Bayes data mining model that can be applied to intrusion detection problems which are affected by high dimensionality, high related features and high network data quantity. In this experiment they used two prominent variation techniques such as reduction of the entropy in the discretized manner with the k-interval level for the effective performance in the KDD'99 dataset. The developed model comprises of the selection of features with the three different filter those are consistency, correlation and Interact for the selection of features. These techniques help to obtain good results in proposed method on KDD'99 dataset. The model shows overall better result in terms of detection accuracy, error rate and misclassification cost.

In [15] implemented novel methodology known as FCANN, based on artificial neural network and fuzzy clustering. The given data is partitioned into clusters to maintain homogeneity within the clusters and heterogeneity between the clusters. The process of the clustering module process incorporates the reduction of the complexity and size in the training sequences for the efficiency and effectiveness in the ANN. The intrusion detection prediction is achieved with the ANN based feed-forwards network with the back propagation model. In the final stage, fuzzy is adopted for the computation of the different NN in the minimization of the errors. The experimental results evaluated using KDD'99 dataset that demonstrates effectiveness especially in low frequent attack detection i.e. R2L and U2R attacks in terms of precision and detection stability.

In [16] proposed a model for the anomaly detection with the hybrid intrusion detection module in the decomposition structure. The developed model incorporates the C4.5 decision making algorithm for the regular training and manageable subsets for the processing of data. The anomaly detection is implemented with the support vector machine with the 1-class model for the decomposition. The performance of the dataset is evaluated with the NS-KDD model for the classification with the 1-class SVM for the decomposition. The developed model exhibits the reduced time for the anomaly detection with the improved training and testing.

In [17] developed a novel integrated principal component analysis (PCA) and Support vector machine (SVM) with the kernel pattern for the selection of the feature attributes. The defined KDD dataset is provided for the training and testing process for the elimination of the attacks in the network with the U2R and R2L features. In the minimal state the PCA is implemented for the selection of attributes for repetitive features. The computation is based on the threshold variance to achieve the higher value for the vector features. Secondly, the features are processed with the PCA based training and testing for the classification with the SVM for the minimized time for the overhead.

In [18] proposed feature selection approach based on mathematical intersection principle. In this technique, three different types of 34 feature selection techniques are applied. Correlation based feature selection (CFS) method with Genetic Algorithm (GA) applied. After CFS using GA method for the combination of the generated population. The filtered approach is utilized those to achieve the information gain and the correlation attribute evaluation in the pre-processing of the dataset for the ranking features. Naïve Bayes and J48 classifiers applied to classify the testing features. The results are evaluated on NSL-KDD dataset in terms of accuracy, run time and selected number features.

In [19] proposed hybrid intrusion detection model by integrating the principal component analysis (PCA) and Support Vector Machine (SVM). The PCA generated eigen vectors for every feature, to obtain the optimal feature subset highest eigen values retained in respective eigen vectors. The SVM classifier is used to predict the class label. In training stage identifies the class labels from the feature matrix. In testing stage obtains the learning rules from the training phase to identify the pattern of the unknown traffic. SVM classifier uses optimization of kernel parameters to select automatic parameters. This method optimizes the punishment factor (C) and kernel parameter (γ), thereby enhancing the accuracy and reducing the train and test time. The model evaluated results are on NSL-KDD dataset.

In [20] proposed discriminant SVM technique is used to differentiate the features of intrusions. Rough set theory selects the features and reduced dimensionality of dataset. The scaling method avoids attributes in wider numeric ranges compared to those in smaller numeric ranges. SVM based kernels 35 classify the intrusions efficiently for heterogeneous type KDD'99 dataset. Scaling process improves the performance of classification. The combination of scaling and rough set feature selection techniques increases the overall performance and minimized detection time.

3. Improved LSTMgateRNN model for the attack detection and classification in IDS

LSTMgateRNN model uses the traditional feed forward neural network for the transmission of information in the forward direction. The data transmission between input and the hidden nodes in the output layer of the network. In the developed LSTMgateRNN model the hidden nodes are optional for the RNN network. The proposed LSTMgateRNN model comprises of the weighted matrices and activation function estimation. The input sequence vector, hidden vector and output vector represented as X, H and Y. The sequence of the input vector is denoted as $X = (x_1, x_2, \dots\dots, x_T)$ for the calculated hidden vector RNN is represented as $H = (h_1, h_2, \dots\dots, h_T)$ with the output vector sequence is denoted as $Y = (y_1, y_2, \dots\dots, y_T)$ as in equation (1) and (2)

$$s_t = \sigma(W_{xh}x_t + W_{hh}x_{t-1} + b_h) \quad (1)$$

$$e_t = W_{hy}s_t + b_y \quad (2)$$

Where logistics function is denoted as σ, bias vector b, bias term weighted matrix is represented as W. The network hidden layer t-time steps are computed based on the output of the hidden layer. LSTMgateRNN model comprises of the dependence sequence prediction for the LSTM in RNN. Every cell in LSTM network comprises of the input gate W_{xm}, forget gate as W_{hm} and output gate denoted as W_{cm} represented as in equation (3) - (5)

$$m_t = \sigma(W_{xm}x_t + W_{hm}x_{t-1} + W_{cm}x_{t-1} + b_m) \quad (3)$$

$$n_t = \sigma(W_{xn}x_t + W_{hn}x_{t-1} + W_{cn}x_{t-1} + b_n) \quad (4)$$

$$r_t = \sigma(W_{xr}x_t + W_{hr}x_{t-1} + W_{cr}x_{t-1} + b_r) \quad (5)$$

The cell state in the model is computed based on the forget network model with the gate function estimated from the previous output and input. The gate control is defined as a_t with the cell state represented as g_t and i_t in equation (6) and (7)

$$a_t = g_t © a_{t-1} + i_t © \tanh(W_{ax}x_{t-1} + b_a) \quad (6)$$

$$i_t = r_t © tanh(a_t) \quad (7)$$

In the above equation the input, hidden and cell state are denoted as m_t, n_t and r_t for the cell time t. The bias state of the input, forget, cell and output gate are represented as a_t, g_t, r_t and b_a. The sigmoidal function is denoted as σ with the element -wise multiplication denoted as © for the weighted matrix W for the connected input, forget, cell and output are represented as W_{xm}, W_{hm}, W_{cm} and W_{xr}.

3.1 LSTM Optimization with Machine Learning

LSTMgateRNN uses the gradient descent optimization model with the neural network. The gradient operator in the model uses the learning rate for the optimization of the LSTM network for the parameter $\theta_{t,i}$ for the time step t. The objective function for the LSTMgateRNN model is presented in equation (8)

$$S_{t,i} = \nabla_\theta J(\theta_{t,i}) \quad (8)$$

The incorporated intrusion detection system updates the information about parameter in the time step t defined as the θ_i given in equation (9)

$$\emptyset_{t+1,i} = \theta_{t,i} - \rho . g_{t,i} \quad (9)$$

Through the update rule general rate of learning is represented as $\emptyset$ for the time step t in the parameter θ_i computed as in equation (10)

$$\emptyset_{t+1,i} = \theta_{t,i} - \frac{\rho}{\sqrt{G_{t,ii}+\epsilon}} . g_{t,i} \quad (10)$$

The diagonal matrix element in the gradient square is represented as the $Gt \in R\ d \times d$ with respect to the time step t integrated with the smoothing variable ϵ those learning rate is defined as the 0.01. The process of dimensionality reduction in the feature extraction process is estimated based on the two steps for the input data X and the mapping process is defined as in equation (11) and (12)

$$H = s(UX + b) \tag{11}$$

$$\widehat{G} = s(U'y + b') \tag{12}$$

The hidden layer neuron activation function is denoted as H and $\widehat{G}$ with the output neuron respectively. The bias vector is denoted as the b and b' represents the encoder and decoder process with the weighted matrices value U and U'. The mean square error (MSE) of the LSTMgateRNN model is estimated using the equation (13)

$$MSE = \frac{1}{M}\sum_{i=1}^{N} x_i + x_i'^2 \tag{13}$$

With regularization the non-differentiable parameters are computed based on the optimization function with the smoothing labelled process as defined in equation (14)

$$s_u(t) = \begin{cases} \frac{t^2}{2\mu}, & if\ |t| \le \mu \\ |t| - \frac{\mu}{2}, & otherwise \end{cases} \tag{14}$$

The hyper-parameter values are computed as $\mu > 0$ for the smoothened and regularization process in the RNN model. The induced sparsity is defined as the $s_u(t)$ with the average output in the hidden unit is denoted as t_j denoted in equation (15)

$$t_j = \frac{1}{n}\sum_{i=1}^{m} a_j^{(i)} \tag{15}$$

In above equation (15) the $a_j^{(i)}$ denotes the hidden unit input and output through the smoothed regularization for the sparsity divergence. The process involved in the intrusion detection system for the attack detection is presented in figure 1. The designed model predicts the multi-class malicious activity to compute the performance characteristics.

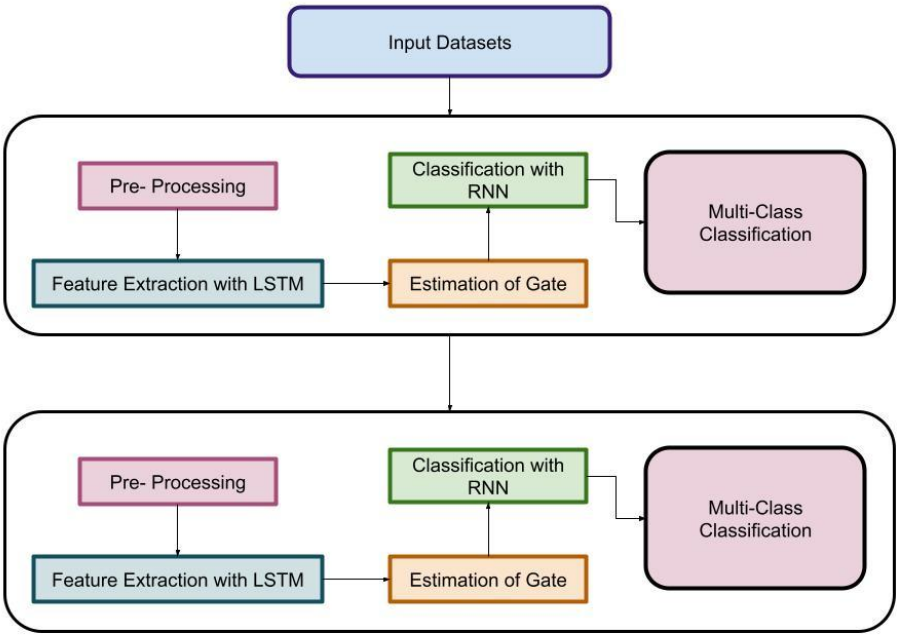


Figure 1: Architecture of LSTMgateRNN

The developed LSTMgateRNN model comprises of the two-stage deep learning process for the acquired datasets. Initially, the acquired data is represented with the targeted label those are related to the unlabelled data. The proposed model belongs to the class of unsupervised feature learning process for the processing of the labelled and unlabelled data. The attack labels are processed and classified based on the supervised algorithm for the attack classification in the network. Through the PCA based feature learning process the dimensionality reduction is employed for the input and output layers of the network. The algorithm for the proposed LSTMgateRNN model is presented as follows:

Algorithm 1: LSTMgateRNN model for attack detection and Classification
Input Train and evaluate the test intrusion dataset Output Compute the multi-class attacks Step 1: Start Step 2: initialize h, g, w, w', b, b' Step 3: Evaluate the reconstruction error function Step 4: Add smoothed with estimation of the cost function in the LSTM Step 5: Train Network Step 6: obtain reconstruction representation of the input x' Step 7: Classification of the attacks using the RNN network Step 8: Stop

3.2 Dataset

The developed LSTMgateRNN model performance is evaluated in the intrusion detection system based on the consideration of different datasets such as KDD'99, NSL-KDD and UNSW-NB15 datasets. The KDD dataset comprises of the 4,87.674 and 22,345 for the training and testing. Also, the NSL-KDD dataset comprises of the records 1,32,684 and 22,378 for the data training and testing.

4. Results and Discussions

The efficiency of the developed LSTMgateRNN model comprises of the sparse encoder with the unsupervised deep learning classifier for the intrusion detection system for the training and testing phases. The proposed LSTMgateRNN model is comparatively examined with the RNN and LSTM model for the different datasets such as KDD'99, NSL-KDD and UNSW-SW15. The table 1 provides the classification performance for the developed LSTMgateRNN model is presented.

Table 1: Attack Classification

	KDD'99			**NSL-KDD**			**UNSW-SW15**		
Methodology	**RNN**	**LSTM**	**LSTMgateRNN**	**RNN**	**LSTM**	**LSTMgateRNN**	**RNN**	**LSTM**	**LSTMgateRNN**
Accuracy	91.34	94.52	99.48	90.45	95.43	98.79	93.45	94.63	99.37
Recall	90.46	93.48	99.35	98.56	98.76	99.35	93.67	94.67	99.84
Precision	94.62	94.68	99.84	93.58	94.68	99.84	94.77	95.63	99.84
F1	94.68	94.83	99.84	92.57	93.63	99.83	95.63	96.73	99.14
FPR	0.18	0.05	0.03	0.23	0.29	0.15	0.32	0.27	0.13

The proposed LSTMgateRNN model is evaluated with the conventional LSTM and RNN model for the performance evaluation. The comparative analysis observed that the proposed

LSTMgateRNN model archives the accuracy value of 99.48% for the KDD'99, 98.79% for the NSL-KDD and 99.37% for the UNSW-SW15 datasets. The table 2 provides the attack classification rate for the KDD'99 and NSL-KDD model is presented. In table 3 the attack classification rate for the UNSW-SW15 model classification rate for the dataset is presented.

Table 2: Attack Classification with KDD'99 and NSL-KDD

Dataset	Model	DoS	Probe	R2L	U2R	Normal
KDD'99	RNN	90.45	91.37	91.38	91.34	92.35
	LSTM	92.35	91.84	93.42	92.48	94.59
	LSTMgateRNN	98.67	98.47	99.03	99.04	99.04
NSL-KDD	RNN	94.52	95.63	94.83	95.61	97.53
	LSTM	96.93	96.83	95.73	96.74	97.59
	LSTMgateRNN	99.13	99.46	99.28	98.48	99.24

Table 3: Attack Classification with UNSW-NB15 dataset.

Dataset	Model	Exploits	Reconnaissance	Backdoor	DoS	Analysis	Fuzzers	Worms	Shellcode	Generic	Normal
UNSW-SW15	RNN	89.56	90.45	94.51	92.72	92.78	92.57	93.69	93.63	94.62	93.84
	LSTM	90.34	90.36	95.74	91.84	94.63	93.61	94.64	95.75	96.74	91.74
	LSTMgateRNN	98.74	98.74	99.13	99.45	99.57	99.85	98.94	98.83	99.63	99.05

The comparative analysis expressed that proposed LSTMgateRNN model achieves the classification accuracy of the 99% for the all three datasets considered for the analysis. Through the comparative analysis it can be concluded that LSTMgateRNN model achieves the higher detection rate compared with the existing LSTM and RNN model. Similarly, for the proposed LSTMgateRNN model detection rate for the KDD'99 and NSL-KDD model is presented in table 4 and table 5 provides the detection rate of UNSW-NB15 dataset.

Table 4: Detection Rate for KDD'99 and NSL-KDD

Dataset	Model	DoS	Probe	R2L	U2R	Normal
KDD'99	RNN	97.84	96.84	89.04	86.93	91.89
	LSTM	97.94	97.56	94.57	88.56	93.47
	LSTMgateRNN	99.04	99.37	98.73	98.76	98.73
NSL-KDD	RNN	98.67	95.68	94.93	95.67	94.86
	LSTM	98.94	97.83	96.73	98.52	97.82
	LSTMgateRNN	99.28	99.34	99.42	99.18	99.37

Table 5: Detection Rate for the UNSW-NB15

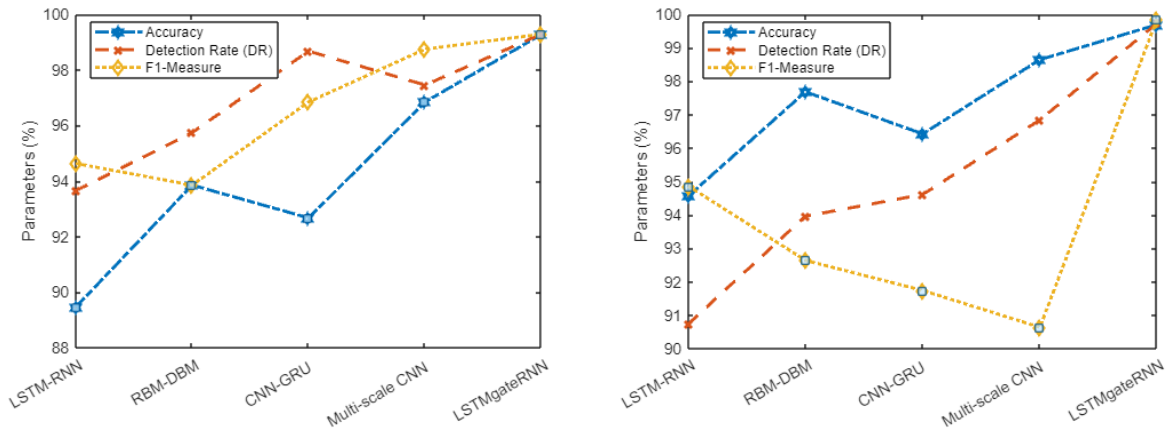
Dataset	Model	Exploits	Reconnaissance	Backdoor	DoS	Analysis	Fuzzers	Worms	Shellcode	Generic	Normal
UNSW-SW15	RNN	94.61	92.75	94.72	96.93	94.91	93.86	91.48	92.84	92.75	94.63
	LSTM	96.84	94.79	96.03	98.71	96.82	96.84	92.86	93.86	93.69	97.63
	LSTMgateRNN	98.94	99.07	99.13	99.05	98.95	99.28	98.71	99.74	99.74	99.46

Like the classification accuracy the proposed LSTMgateLSTM model achieves the maximal detection rate of 99% which is significantly higher for the existing LSTM and RNN model. The table 6 provides the comparison of proposed LSTMgateRNN model with the existing classification models for the different datasets.

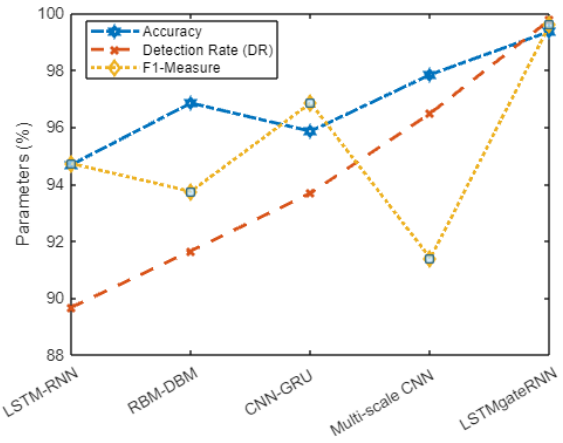
Table 6: Comparison of Parameters for datasets

KDD'99				
Method	**Accuracy**	**DR**	**F1**	**FPR**
LSTM-RNN [12]	89.46	93.65	94.63	2.87
RBM-DBN [5]	93.85	95.74	93.85	2.59
CNN-GRU [6]	92.67	98.67	96.84	1.59
Multi-scale CNN [11]	96.84	97.45	98.74	1.28
LSTMgateRNN	99.27	99.28	99.28	0.14
NSL-KDD				
Method	**Accuracy**	**DR**	**F1**	**FPR**
LSTM-RNN [12	94.56	90.74	94.86	1.78
RBM-DBN [5]	97.68	93.96	92.64	1.29
CNN-GRU [6]	96.42	94.61	91.74	0.98
Multi-scale CNN [11]	98.64	96.84	90.64	0.64
LSTMgateRNN	99.69	99.73	99.86	0.29
UNSW-NB15				
Method	**Accuracy**	**DR**	**F1**	**FPR**
LSTM-RNN [12]	94.67	89.67	94.72	2.78
RBM-DBN [5]	96.84	91.65	93.74	2.17
CNN-GRU [6]	95.85	93.68	96.84	1.85
Multi-scale CNN [11]	97.84	96.48	91.39	1.36
LSTMgateRNN	99.36	99.77	99.63	0.8

The figure 2 provides the comparative analysis of the LSTMgateRNN model with the existing model characteristics for the three different datasets are presented.



(a) (b)



(c)

Figure 2: Comparison of LSTMgateRNN for different datasets (a) KDD'99 (b) NSL-KDD (c) UNSW-NB15

The comparative analysis expressed that the LSTMgateRNN model achieves the higher accuracy value of the 99% which is significantly higher than the existing model for the attack detection and classification in the IDS. The comparative analysis confirmed that LSTMgateRNN model exhibits the improved performance than the existing RNN and LSTM model for the classification.

5. Conclusion

This paper presented a LSTMgateRNN model for the attack detection and classification in the Intrusion Detection System. The developed model comprises of the gate function applied over the Recurrent Neural Network for the attack detection. With the LSTMgateRNN model the features of the attacks are smoothed and regularized for the minimal dimensional features. The developed model is comparatively examined with the conventional classifier model for the attack detection and classification. The comparative analysis expressed that developed LSTMgateRNN model achieves the higher0020accuracy of the 99% which is significantly higher compared with the existing classifier. The performance of the LSTMgateRNN model is ~6-12% higher than the existing classification model.

References

[1] Kunang, Y. N., Nurmaini, S., Stiawan, D., & Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. *Journal of Information Security and Applications*, *58*, 102804.

[2] Shrestha, R., Omidkar, A., Roudi, S. A., Abbas, R., & Kim, S. (2021). Machine-learning-enabled intrusion detection system for cellular connected UAV networks. *Electronics*, *10*(13), 1549.

[3] Alzahrani, A. O., & Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. *Future Internet*, *13*(5), 111.

[4] Liu, C., Gu, Z., & Wang, J. (2021). A hybrid intrusion detection system based on scalable K-Means+ random forest and deep learning. *IEEE Access*, *9*, 75729-75740.

[5] Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly-based intrusion detection systems in the CICIDS2017 dataset. *IEEE access*, *9*, 22351-22370.

[6] Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., ... & Buchanan, W. J. (2021). A deep learning-based intrusion detection system for mqtt enabled iot. *Sensors*, *21*(21), 7016.

[7] Imrana, Y., Xiang, Y., Ali, L., & Abdul-Rauf, Z. (2021). A bidirectional LSTM deep learning approach for intrusion detection. *Expert Systems with Applications*, *185*, 115524.

[8] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150.

[9] Mendonça, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., & Farouk, A. (2022). A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Systems*, *39*(5), e12917.

[10] Ashiku, L., & Dagli, C. (2021). Network intrusion detection system using deep learning. *Procedia Computer Science*, *185*, 239-247.

[11] Ramaiah, M., Chandrasekaran, V., Ravi, V., & Kumar, N. (2021). An intrusion detection system using optimized deep neural network architecture. *Transactions on Emerging Telecommunications Technologies*, *32*(4), e4221.

[12] Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied Sciences*, *11*(18), 8383.

[13] Sethi, K., Madhav, Y. V., Kumar, R., & Bera, P. (2021). Attention based multi-agent intrusion detection systems using reinforcement learning. *Journal of Information Security and Applications*, *61*, 102923.

[14] Rao, K. N., Rao, K. V., & PVGD, P. R. (2021). A hybrid intrusion detection system based on sparse autoencoder and deep neural network. *Computer Communications*, *180*, 77-88.

[15] Wani, A., & Khaliq, R. (2021). SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). *CAAI Transactions on Intelligence Technology*, *6*(3), 281-290.

[16] Kanna, P. R., & Santhi, P. (2021). Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features. *Knowledge-Based Systems*, *226*, 107132.

[17] Disha, R. A., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. *Cybersecurity*, *5*(1), 1-22.

[18] Hammad, M., Hewahi, N., & Elmedany, W. (2021). T-SNERF: A novel high accuracy machine learning approach for Intrusion Detection Systems. *IET Information Security*, *15*(2), 178-190.

[19] Disha, R. A., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. *Cybersecurity*, *5*(1), 1-22.

[20] Singh, G., & Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, *44*(7), 659-669.