Efficient Intrusion Detection in Patient Health Records Based on LSTM-Based RNN

Nikita Sharma[1], Hajare Hirendra Ramesh[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India*

KEYWORDS

Intrusion Detection Systems, Deep Learning, attacks, classification, LSTM based RNN.

ABSTRACT

Advancements in Information and Communication Technology applications play an important role in the field of healthcare and bio-medical engineering. The process of image processing and analysis starts from receiving visual information to giving out the description of the scene for improving the visual appearance of the human viewer and extract the features of the data. Moreover, IDS can be deployed along with other security mechanisms as a line of defence to ensure security of system and network resources. There have been various efforts in designing IDS using Machine Learning (ML) techniques. Additionally, by developing a hybrid strategy for intrusion detection and classification and using feature engineering approaches to extract significant features for learning, among other things, efforts have been made to improve the classification performance of ML-based IDS. However, as networking technology have advanced, attack types have evolved as well. For this reason, an efficient and successful intrusion detection and classification system must be created. To address the issue and achieve good generalization ability for intrusion detection and classification, the paper presents empirical analysis of LSTM based RNN classifiers. The suggested methods' effectiveness is assessed using a range of performance metrics, such as recall, f-score, accuracy, precision, and False Positive Rate (FPR). The LSTM based RNN method recognize attacks with 99.2% accuracy with minimum time complexity (5 s).

1. Introduction

An whole new realm of information and communication technologies known as the Internet of Things (IoT) refers to a networked system of interconnected, interdependent things that may gather and share data without the need for human intervention. One of the most significant technologies of the twenty-first century is the Internet of Things (IoT). Various IoT standards and technologies have been established recently for a variety of application scenarios, including smart homes, smart cities, agriculture, healthcare, and so on. IoT devices have embedded transceivers, actuators, CPUs, and sensors that can send data over other networks or the internet. These components are configured for specific uses [1]. Intrusion detection and classification system is designed to analyse network data samples and extract patterns to identify normal network traffic and attack network traffic. ML techniques are applied to perform prediction and classification for the underlying application problem, wherein patterns are learned through experience [4]. Various ML approaches adopt different learning strategy to derive patterns for intrusion detection and classification. The basic task of ML techniques is prediction, for which varied data samples are used and presented to the underlying technique that learns patterns from the data and predicts based on the learning. Furthermore, one of the important considerations while applying learning technique is its ability to handle data. There has been multitude of research work in the field of ML-based IDS, wherein various aspects such as data pre-processing, feature engineering, learning approach, and performance measures have been taken into consideration for demonstrating the performance of ML-based IDS [2]. By taking into account different aspects like good generalisation ability, enhanced feature engineering capability, improved learning capability, effortless handling of high-dimensional data, and handling class imbalance in intrusion detection datasets, our work focuses on proposing LSTM based RNN approaches for enhancing attack classification capability of designed IDS [16]. The following is a summary of the research's principal contributions. Research gaps and findings are derived and studied to foster the need to design IDS with enhanced attack detection and classification capability. Empirical analysis of DL techniques is performed for intrusion detection and classification and solutions proposed to address research gaps for performance improvement of IDS. Enhanced techniques LSTM based RNN are designed that can resonate with performance improvement for attack classification. Designed solutions are evaluated for

attack classification using different intrusion detection datasets to ensure assorted performance of proposed solutions. In this instance, section 1 of the paper examines the introduction, whereas section 2 examines the relevant literature. Section 3 provides an explanation of the planned work, Section 4 presents the work's outcomes, and Section 5 concludes the project.

2. Literature Review

Using Autoencoder and Isolation Forest as Auto-IF, Sadaf & Sultana (2020) [3] developed and implemented a methodology for intrusion detection in fog computing [13]. They sought to classify incoming packets in binary. While isolation forest is utilised to increase accuracy even further, autoencoders (AEs) are employed to classify attack and normal data. The NSLKDD dataset is used to validate this research project [12]. In their study, Diro et al. (2021) [18] investigated the use of cutting-edge technologies and facilitators for intrusion detection in IoT/fog networks, including fog computing architecture, blockchain, and DL algorithms [7]. They talked about how Deep Learning (DL) techniques, which offer quick processing and compact data representations, have been proven to be promising for IoT security [10]. As a result, the spread of fog nodes combined with DL approaches may offer systems that are more durable, lightweight, autonomous, and efficient [17].

Using fog computing, Kumar et al. (2021) [5] introduced a unique distributed ensemble design-based IDS that integrates Gaussian naive Bayes, XGBoost, and k-nearest neighbours as first-level individual learners. A meta classifier was employed in conjunction with an ensemble stacking technique [15]. An adaptive IDS was created using Random Forest to safeguard IoT networks. The UNSW-NB15 and the real IoT-based dataset, DS2OS, were utilised in that study to confirm the efficacy of their suggested approach[14]. Reddy et al. (2021) [6] introduced an intrusion detection system that uses the Exact Greedy Boosting ensemble approach for device implementation in the fog node, as well as a security mechanism that ensures the truthful operation of IoT networks [19]. Their suggested approach classified and identified the sort of attack based on deviations from typical behaviour, allowing for the monitoring of traffic flow in the unique IoT Intrusion Dataset 2020 (IoTID20) [20] network traffic.

3. Methodology

Implementing IDS using deep learning could be a better solution to the previously mentioned problem. DL models are capable of producing new features by themselves. After receiving sufficient training, a deep learning model can execute thousands of repetitive tasks faster and more accurately. The DL technique, which is based on the model of prior suspicious network activity, aids in the detection of new attack types. As a result, fewer false alarms will occur and security staff will be better able to differentiate between malicious and benign network activities. Figure 1 displays the thesis framework schematic.

Image acquisition

Four different types of assaults are present in the NSL-KDD data set: DoS (Denial of Service), Probe, R2L (Remote to Local), U2R (User to Root (U2R), and regular connections.

Table 1. Attacks classification

Attackcategory	Subclasses
DoS	Pod, processtable, Neptune, back, land, Apache2, smurf, teardrop, udpstorm, and pod
Probe	Saint, Satan, mscan, nmap, portsweep, and Ipsweep

R2L	Guess passwd, ftp write, imap, multihop, named, phf, sendmail, attack, guess, spy, warezclient, warezmaster, work, xlock, xsnoop
U2R	buffer overflow, loadmodule, httptunnel, perl, ps, rootkit, sqlattack, and xterm

A summary of the various subclasses of every attack in the data set is provided in Table 1.

In contrast to the previous three assaults, which aim to stealthily enter the system without being noticed, the denial-of-service (DoS) attack aims to completely interrupt traffic flow by shutting down the system. Table 2 displays the distribution of connection records for the NSL-KDD training and testing datasets. Each record in the data set has 43 features: 41 features are related to the traffic input itself, 42 features indicate whether the record is an attack record or a regular record, and 43 features are related to the score, or the intensity of the traffic input.

Table 2. Attack distribution in NSL-KDD dataset

Attack category	Training dataset	Testing dataset
Normal	67343	9711
DoS	45927	7456
Probe	11656	2421
R2L	995	2756
U2R	52	200
Total	125973	22544

Preprocessing

Normalisation, feature selection, and feature dimensionality reduction are the three main steps in the preparation of data. In order to increase the detection efficiency, this is utilised to guarantee the quality of the incoming data. For multi-class classification, the model is trained using network records of four assaults and normal classes. The model is put through another test to gauge its performance [8].

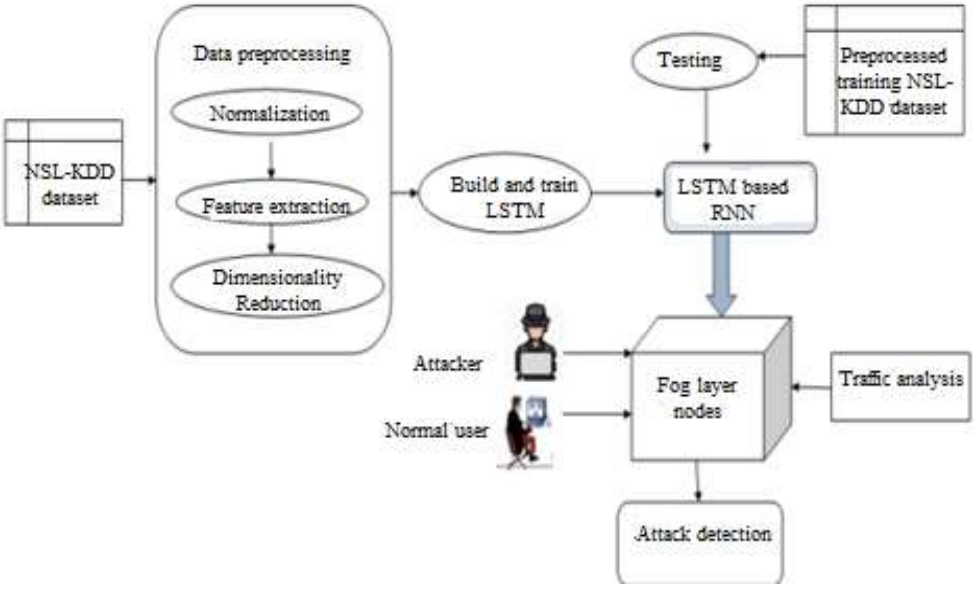

Figure 1. proposed architecture

Below is a quick explanation of the steps in this suggested model.

1. Preprocessing the NSL-KDD dataset for training and testing

- Normalization of data.
- Selecting the optimal features by reducing the dimensional of unnecessary features.

2. Implementation of LSTM based RNN deep learning models.
3. Train the LSTM based RNN classifier with preprocessed NSL-KDD training set.
4. Test the LSTM based RNN classifier with preprocessed NSL-KDD testing set.
5. Measure the performance and Comparison of results.

- **Normalization**

  By scaling the input features to a common scale, normalisation is a crucial step in data mining that can help to improve the performance of machine learning algorithms. This may lessen the effect of outliers and increase the model's accuracy. An attribute's values can be scaled via normalisation to fall inside a more narrow range, like -1.0 to 1.0 or 0.0 to 1.0. In general, classification algorithms benefit from it. When working with attributes that are on multiple scales, normalisation is usually necessary to avoid diluting the impact of an equally essential attribute (on a lower scale) due to other attributes having values on a bigger scalePut another way, when there are several characteristics yet the values of those attributes are on different scales, this could result in subpar data models when data mining is done. In order to put all the qualities on the same scale, they are normalised. [9].

- **Dimensionality Reduction based Modified Principal Component Analysis**

The MPCA reduces band rectification and directs end member selection by extracting the essential elements from the picture and increasing the amount of over-resulted entities.

Classification: LSTM based RNN

RNNs can retain inputs for extended periods of time because to LSTMs. This is due to the fact that LSTMs, like computer memory, store input data images in a memory. Information can be read, written to, and deleted from the LSTM-RNN's memory. This memory can be thought of as a gated cell, where the gate denotes that the cell chooses, according to the value it places on the information, whether to keep it or not, or to open the gates. Weights are used to assign importance, and the algorithm also learns these. Three gates make up an LSTM-RNN: an input, a forget, and an output gate. These gates control whether to allow data to enter the system (input gate), discard data that isn't needed (forget gate), or allow data to affect the output at the current time step (output gate) [11].

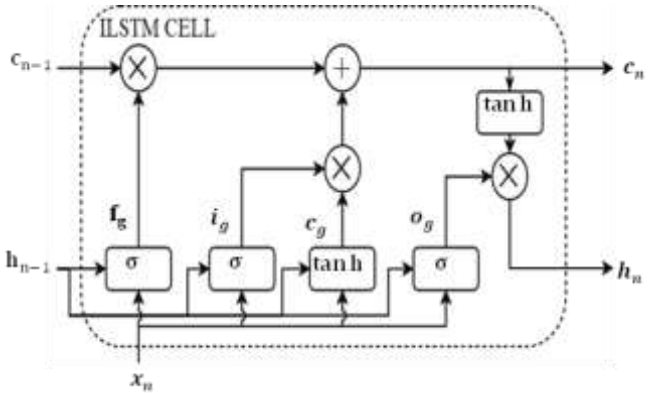

Figure 2. LSTM based Recurrent Neural Network (LSTM-RNN)

Fig.2 demonstrates the architecture of the LSTM recurrent neural network. The architectures of a networks are mostly designed to extract information from 2D structure of an input image. The LSTM-RNN layer is made up of cell states that have been propagated over time. Cell states are modified at each time step based on the gate output, which is determined based on the current input and previous

hidden states. The following are the formulations:

$$f_g = \sigma\left(W_f\left[h_{g-1}, x_n\right] + b_f\right) \quad (5)$$

$$i_g = \sigma\left(W_i\left[h_{g-1}, x_n\right] + b_i\right) \quad (6)$$

$$K_g = \tanh\left(W_g[g, x_n] + b_g\right) \quad (7)$$

$$c_g = c_{g-1} * f_g + i_g * G_g \quad (8)$$

Where K_g denotes the nominee of cell states. W_f, W_i, and W_g are weight matrices. b_f, b_i, and b_g are biases, and c_g and h_g are the cell states and the performance of the LSTM-RNN block, respectively.

4. Results and discussion

The real-time classification experiment was showcased for the purpose of detecting DoS attacks. One Windows 7 Virtual Machine (VM) was utilised to implement the suggested LSTM-based RNN. Every traffic was observed by means of this technology. The regular connections were designated as 0, and the DoS, Probe, R2L, and U2R attacks were labelled 1, 2, 3, and 4, accordingly. Each batch size was set to 64 and the number of epochs to 50. In our model, the accuracy of the training and testing sets grows with increasing epoch. The loss of the training and testing sets decreases as the epoch increases. Accuracy rises and loss falls with the number of training rounds, but ultimately it seems to be flat. Every ten epochs, from 10 to 50, we tested in order to determine a better epoch value.

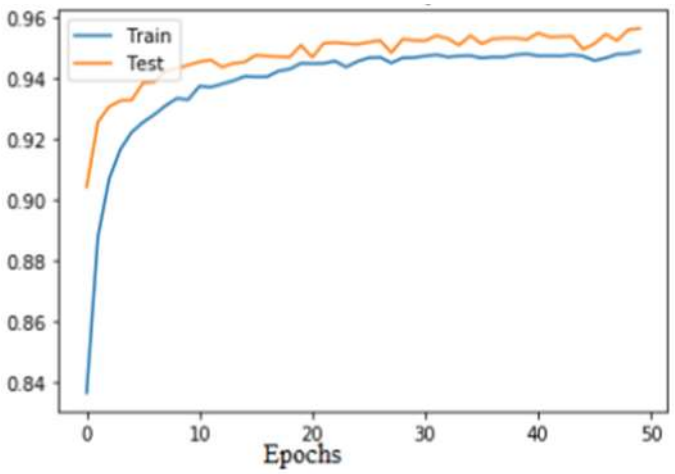

Figure 3. Accuracy of proposed model

Table 3 displays the accuracy, precision, recall, F-Score, false alarm rate, and misclassification rate for each class as well as the proposed model's performance on the test dataset. For the DoS assault, the accuracy and false alarm rate are 0.7% and 99.2%, respectively. The R2L, U2R, and Probe attacks have accuracy rates of 96.5%, 97%, and 98.5%, in that order. The R2L, U2R, and Probe attacks have false alarm rates of 1.2%, 1.0%, and 0.95%, respectively.

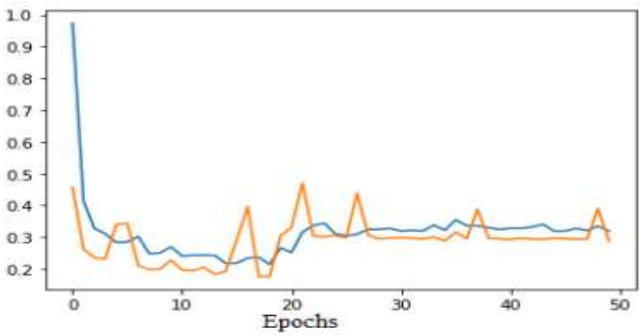

Figure 4. Loss of proposed model

Table 3. Performance metrics of HD detection

Models	Accuracy (%)	False alarm rate	Misclassification rate	F1-Score	Precision (%)	Recall (%)
Normal	97.5	2.0	2.5	0.97	97	89.85
DoS	99.2	0.7	0.8	0.985	97.50	90.25
Probe	96.5	0.95	3.5	0.97	98.15	81.05
R2L	97	1.2	3	0.985	97.50	90.25
U2R	98.5	1.0	1.5	0.97	98.15	81.05

Our LSTM-based RNN model's accuracy was evaluated against both the most recent deep learning model algorithms and traditional machine learning models. The experiment showed that on the NSL-KDD dataset, our suggested hybrid deep learning model, an RNN based on LSTM, performs classification with excellent accuracy.

Table 4. Performance evaluation of ICNN-FCID with different activation functions

Models	Accuracy (%)	Precision (%)	Recall (%)	F1-Score
ReLU	97.5	97	99.85	0.97
Sigmoid	89.2	87.50	90.25	0.885
Tanh	90.5	88.15	81.05	0.87

Table 4 displays the confusion matrix for the LSTM based RNN model with ReLU activation function for the NSL-KDD testing dataset. With the ReLU activation function, the LSTM-based RNN model has shown better classification results and high accuracy.

Table 5. Performance metrics with conventional models

Models	Accuracy (%)	Time complexity
FFDNN [8]	90	5 min
GRU, LSTM, Bi-LSTM CNN, CNNLSTM, and DNN [9]	90.7	2 min
k-nearest neighbors, XGBoost, and Gaussian naive Bayes [10]	92	2 min
Exact Greedy Boosting ensemble method [12]	93	1,9 min
LSTM based RNN	99.2	5s

We conducted an experiment to show that utilising LSTM based RNN for a Network Intrusion Detection System (NIDS) is feasible and may effectively leverage deep learning capabilities for network intrusion detection.

5. Conclusion and future scope

This study proposes a hybrid classification model for multiclass attack classification in fog computing environments by integrating an LSTM-based RNN with training and implementation. We employed normalisation and feature extraction from the dataset to increase the model's accuracy. The KDD

Train+ dataset was used to train our hybrid model, while the KDD Test+ dataset was used to test it. Our model performs better than other current deep learning algorithms and conventional machine learning techniques, with an accuracy of 99.2%. We have shown that our model is effective in classifying DoS, Probe, R2L, and U2R attacks in fog computing settings. Our test, which we ran to identify DoS assaults using virtualization technology, produced the desired outcomes. As a result, the suggested RNN classification model based on LSTM can operate effectively in real time settings.

Reference

[1] Hady, Anar A., Ali Ghubaish, Tara Salman, Devrim Unal, and Raj Jain. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." *IEEE Access* 8 (2020): 106576-106584.

[2] Balyan, Amit Kumar, Sachin Ahuja, Sanjeev Kumar Sharma, and Umesh Kumar Lilhore. "Machine learning-based intrusion detection system for healthcare data." In *2022 IEEE VLSI Device Circuit and System (VLSI DCS)*, pp. 290-294. IEEE, 2022.

[3] Pande, Sagar, Aditya Khamparia, and Deepak Gupta. "An intrusion detection system for health-care system using machine and deep learning." *World Journal of Engineering* 19, no. 2 (2022): 166-174.

[4] Yashir Ahamed, M., Lalthlamuanpuii, R., Chetia, B., Lallawmawmi, & Lalngaizuali. (2023). Usage of Medical Library Resources: A Study in the Regional Institute of Medical Sciences, Imphal. Indian Journal of Information Sources and Services, 13(2), 1–6.

[5] Thamilarasu, Geethapriya, Adedayo Odesile, and Andrew Hoang. "An intrusion detection system for internet of medical things." *IEEE Access* 8 (2020): 181560-181576.

[6] Öztürk, Tolgahan, Zeynep Turgut, Gökçe Akgün, and Cemal Köse. "Machine learning-based intrusion detection for SCADA systems in healthcare." *Network Modeling Analysis in Health Informatics and Bioinformatics* 11, no. 1 (2022): 47.

[7] Mehak, S., Himanshi., & Sanju, S. (2024). Privacy-enhancing Blockchain Solutions for the Healthcare Sector: Efficient Message Sharing and Robust Big Data Protection. Journal of Internet Services and Information Security, 14(2), 85-97.

[8] Saif, Sohail, Priya Das, Suparna Biswas, Manju Khari, and Vimal Shanmuganathan. "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare." *Microprocessors and Microsystems* (2022): 104622.

[9] Ashraf, Eman, Nihal FF Areed, Hanaa Salem, Ehab H. Abdelhay, and Ahmed Farouk. "Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications." In *Healthcare*, vol. 10, no. 6, p. 1110. MDPI, 2022.

[10] Malathi, K., Shruthi, S.N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P.M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 60-72. https://doi.org/10.58346/JOWUA.2024.I2.005

[11] Jain, Anshul, Tanya Singh, and Satyendra Kumar Sharma. "Security as a solution: an intrusion detection system using a neural network for IoT enabled healthcare ecosystem." *Interdisciplinary Journal of Information, Knowledge, and Management* 16 (2021): 331-369.

[12] Marangunic, C., Cid, F., Rivera, A., & Uribe, J. (2022). Machine Learning Dependent Arithmetic Module Realization for High-Speed Computing. Journal of VLSI Circuits and Systems, 4(1), 42-51.

[13] Subasi, Abdulhamit, Shahad Algebsani, Wafa Alghamdi, Emir Kremic, Jawaher Almaasrani, and Najwan Abdulaziz. "Intrusion detection in smart healthcare using bagging ensemble classifier." In *International Conference on Medical and Biological Engineering*, pp. 164-171. Cham: Springer International Publishing, 2021.

[14] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. Archives for Technical Sciences, 2(29), 11-22.

[15] Kavitha R., et.al The location-identity split no longer considered harmful, Eurasian Journal of Analytical Chemistry,

V-13, I-3, PP:996-1002, 2018.

[16] Savanović, Nikola, Ana Toskovic, Aleksandar Petrovic, Miodrag Zivkovic, Robertas Damaševičius, Luka Jovanovic, Nebojsa Bacanin, and Bosko Nikolic. "Intrusion detection in healthcare 4.0 internet of things systems via metaheuristics optimized machine learning." *Sustainability* 15, no. 16 (2023): 12563.

[17] Sundararajan, T. V. P., and A. Shanmugam. "A novel intrusion detection system for wireless body area network in health care monitoring." *Journal of Computer Science* 6, no. 11 (2010): 1355.

[18] Akram, Faiza, Dongsheng Liu, Peibiao Zhao, Natalia Kryvinska, Sidra Abbas, and Muhammad Rizwan. "Trustworthy intrusion detection in e-healthcare systems." *Frontiers in public health* 9 (2021): 788347.

[19] Kutlu, Y., & Camgözlü, Y. (2021). Detection of coronavirus disease (COVID-19) from X-ray images using deep convolutional neural networks. Natural and Engineering Sciences, 6(1), 60-74.

[20] Lee, Jae Dong, Hyo Soung Cha, Shailendra Rathore, and Jong Hyuk Park. "M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT." Computers, Materials & Continua 67, no. 2 (2021).