A Hybrid Intrusion Detection Approach for Cyber Attacks

Amrita Bhatnagar [1], Arun Giri [2], Aditi Sharma[3*,4]

[1,2] Dept of Computer Science & Engg. Shobhit Institute of Engg. & Technology Meerut, India
[3] Dept of Computer Science & Engg. Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India
[4]IEEE, SIT, Pune, India

Emails: amritapsaxena@gmail.com; arun.giri@shobhituniversity.ac.in; aditi.sharma@ieee.org

Abstract

The field of cybersecurity constantly evolves as attackers develop new methods and technologies. Defending against cyberattacks involves a combination of robust security measures, regular updates, user education, and the use of advanced technologies, such as intrusion detection systems and artificial intelligence, to find out the threats in real-time. IDS are designed to identify and address any unauthorized actions or potential security threats within a computer network or system. A hybrid intrusion detection system (IDS) combines many detection techniques and strategies from different IDS types into a single, coherent solution. Combining the benefits of each approach should result in more comprehensive and effective intrusion detection. This paper outlines a proposed anomaly intrusion detection system (AIDS) framework that leverages a hybrid of deep learning strategies. It incorporates Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) models, which were developed using XGBoost, and their efficacy was assessed with the NSL-KDD dataset. The evaluation of the suggested model focused on its accuracy, detection capabilities, and the rate of false positives. The outcomes of this research are noteworthy within the cybersecurity field. In this paper, a framework of an Anomaly IDS is proposed. The purpose of an anomaly IDS, or AIDS, is to spot odd behavior on a network or system that might point to a security breach or malevolent attempt to hack it. Anomaly-based IDSs concentrate on finding departures from accepted typical behavior, in contrast to signature-based detection systems, which depend on a predefined database of known attack patterns.

Keywords: Intrusion; Deep learning; Machine Learning; RNN; LSTM; GRU; XGBoost

1. Introduction:

An IDS designed to detect and handle any unauthorized activity or potential security risk inside a network is a crucial component of cybersecurity architecture. The primary goal of an IDS is to monitor system or network activity, look for trends, and identify abnormalities that may indicate a security event or potential breach [1]. Among the primary duties of an IDS are to watch host or network activity continuously, look for trends, actions, and departures from the norm, and report any unusual activity to administrators or security staff, the system may act automatically or suggest manual involvement, depending on its capabilities. When suspicious activity is found, an intrusion detection system (IDS) notifies administrators or security systems. A security technology called an intrusion prevention system (IPS) continually analyzes network traffic to identify and stop malicious activities in real time. Network packets are analyzed and compared to a database containing known attack signatures, unusual behavior patterns, or pre-established rules in order for the system to function. The IPS works quickly to stop or lessen the threat if it finds suspicious or malicious activities.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

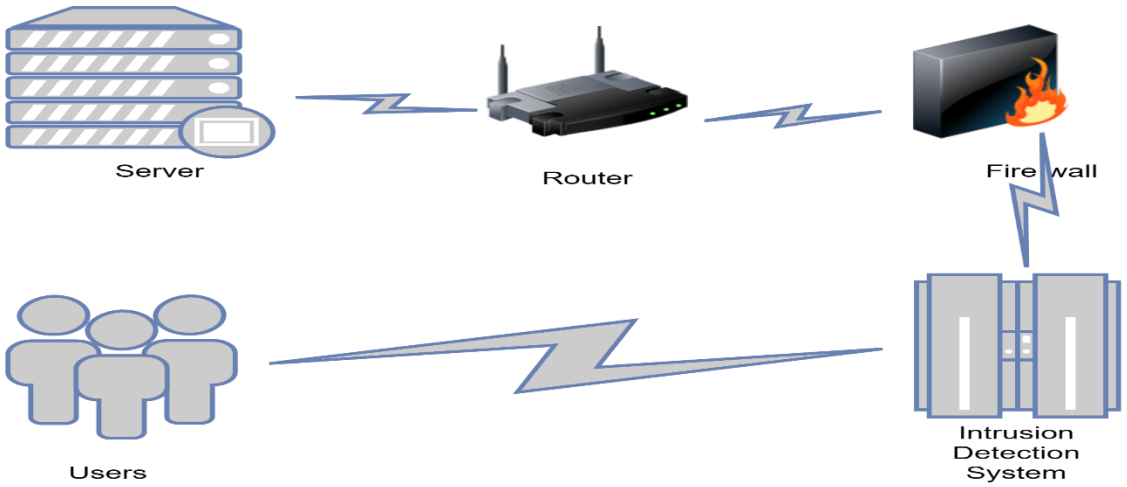

Figure 1: Intrusion Detection System

1.1 Types of IDS

An IDS can be classified into two categories HIDS and NIDS. An endpoint device, workstation, or server's internal operation can be monitored and analyzed by a Host Intrusion Detection System (HIDS), a security tool, for signs of unusual behavior or policy violations. HIDS is focused on the specific host or endpoint, as opposed to network-based intrusion detection systems (NIDS), which scan network data for indications of malicious activity or intrusion. An IDS monitors network or system traffic and activities and analyzes them for indications of hostile behavior or intrusion. An intrusion prevention system (IPS) goes above and beyond by putting countermeasures in place before attacks are detected. It monitors network traffic and, if it detects a threat, can quickly block or reroute hazardous data to prevent further damage [2]. IDSs fall into three basic categories: hybrid-inspired IDS (H-IDS), anomaly-based IDS (A-IDS), and signature-based IDS (S-IDS). S-IDS uses signatures, or patterns, found in the IDS database to identify attacks. A-IDS, on the other hand, scans the network to find and determine whether patterns (behaviors) represent intrusions or threats. A-IDS and S-IDS are combined to form H-IDS.[3]. In this paper, a framework of an Anomaly IDS is proposed. The purpose of an anomaly IDS, or AIDS, is to spot odd behavior on a network or system that might point to a security breach or malevolent attempt to hack it. Anomaly-based IDSs concentrate on finding departures from accepted typical behaviors, in contrast to signature-based detection systems, which depend on a predefined database of known attack patterns.

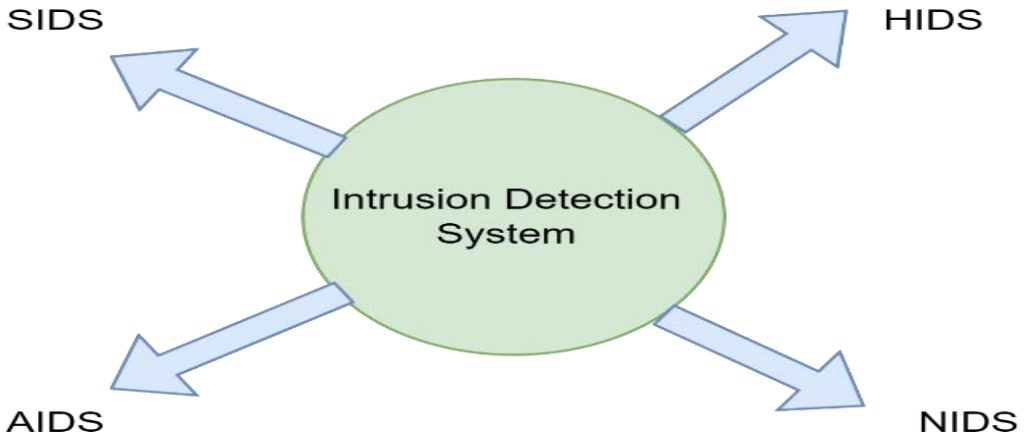

Figure 2: Types of IDS

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

2. Related Work

An in-depth examination of various machine learning methodologies has been endorsed to uncover the root causes of network security issues and glitches [4]. The classification of learning types depends on the nature of parameter adjustments. Typically, learning processes fall into the categories of supervised or unsupervised. Both ML and DL techniques fall under these classifications, encompassing supervised and unsupervised algorithms. In supervised algorithms, valuable insights are derived from labeled data, whereas unsupervised algorithms leverage unlabeled data for extracting meaningful features and information. This introduction provides an overview of commonly employed ML algorithms in IDS along with metrics and benchmark datasets [5]. ML and DL techniques can improve intrusion detection accuracy, reduce false alarm rates, and detect unknown attacks in networks [6]. The Authors used ML techniques like Decision Tree, Random Forest, SVM for Intrusion detection [7]. In this study, the author utilized different ML approaches such as Decision Trees, Random Forest, and Support Vector Machines (SVM) for constructing an effective IDS. Through experimentation, it was determined that the Random Forest algorithm outperformed the others when applied to the chosen features for IDS [8]. DL algorithms like DNN, RNN, and CNN are also very suitable for IDS [9]. The author applied DL techniques to detect attacks, employing LSTM. In the study, a novel IDS utilizing the LSTM Recurrent Neural Network (RNN) framework was developed, demonstrating greater accuracy compared to traditional RNN models [10]. In this paper, the LSTM DL method is used for network intrusion detection to get high accuracy and low false positive rates, making it a promising solution for network security [11]. The introduced ID model exhibited superior performance, evidenced by its high accuracy, elevated detection rates, and minimal false alarm rates. Within this setup, dimensionality reduction and feature selection were accomplished through the utilization of Principal Component Analysis (PCA) and Mutual Information (MI) methodologies [12]. This paper introduces a solution to enhance detection accuracy in traffic anomaly detection by proposing a DL model named DLNID, which merges an attention mechanism with a bidirectional LSTM (Bi-LSTM) network [13]. This study presents an enhancement in the efficiency of IDS for identifying irregular network traffic by creating an IDS that integrates a RNN utilizing gated recurrent units (GRUs) with an enhanced version of LSTM units, termed Cu-LSTMGRU, through a specialized computing unit [14]. The RNN-IDS model exhibits a robust capability for detecting intrusions and achieves high precision in both binary and multiclass categorization tasks. When compared to older classification algorithms like J48, naive Bayes, and random forest, this model demonstrates superior performance in terms of both accuracy and detection rates while maintaining a low rate of false positives, particularly in the context of multiclass classification tasks using the NSL-KDD dataset [15]. In this research paper, the authors introduce an innovative and scalable approach using wide and deep transfer learning (TL), employing a stacked Gated Recurrent Unit (GRU) model. This model is designed to effectively address challenges related to multi-dimensional point data and handle both multi-variate time series regression and classification problems within the domain of network intrusion detection [16]. The hybrid algorithm of CNN and LSTM achieves high accuracy in detecting network intrusions, making it promising for live network infrastructure [17].

The author proposed a sequential LSTM neural network autoencoder framework that effectively detects computer network intrusions, providing dynamic, robust, and scalable performance [18]. The integration of Multiscale Convolutional Neural Network (MSCNN) with Long Short-Term Memory (LSTM) in the MSCNN-LSTM model leads to enhanced accuracy in intrusion detection, as well as reductions in false alarm and false negative rates when contrasted with traditional neural networks [19]. In this paper, the hybrid ELSTM-RNN approach improves the security of intrusion detection in communication networks. It overcomes the challenges associated with gradient clipping and outperforms methods like LPBoost and DNNs in terms of accuracy, precision, recall, and reducing error rates [20].

3. Recurrent Neural Network

Recurrent neural networks (RNNs) are different from typical neural networks in that they create a sequential dependence by using the outcome of the previous step as the input for the current phase. Conventional neural networks, on the other hand, handle inputs and outputs as separate entities. However, when it is necessary to guess the following word in a sentence, the preceding words are necessary, hence it is necessary to retain the preceding words. Thus, RNN was created, and it used a Hidden Layer to tackle this problem. The "vanishing gradient" issue affects RNNs, making it difficult to identify long-range dependencies in sequences. More sophisticated RNN architectures have been created to overcome this problem, such as LSTM & GRU. Because of their more complex memory cell structure, long sequence transistors (LSTMs) can store and recall information over longer periods. Input, forget, and output gates are among them to regulate the information flow. GRUs share a gating mechanism with LSTMs, albeit in a less complex design. They are more computationally efficient than LSTMs because they integrate the input and forget gates into a single gate.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

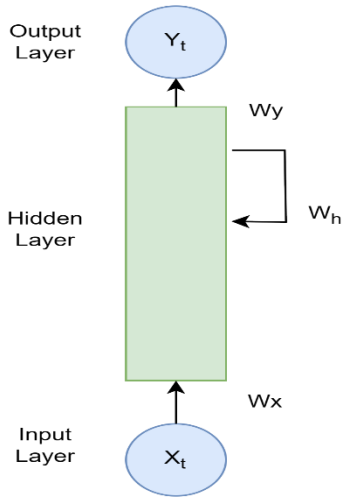

Figure 3: RECURRENT NEURAL NETWORK

3.1 RNN Architecture

By progressively scanning the data from left to right and updating the hidden state at each time step, the RNN accepts an input vector (X) and outputs a vector (L). All time steps have the same set of parameters. This indicates that the network as a whole uses the same set of parameters, denoted by U, V, and W. V stands for the weight connected to the connection between hidden layers, W for the connection from hidden layer h to output layer L, and U for the weight parameter controlling the connection from input layer X to the hidden layer h. By keeping the knowledge from the previous input in its current hidden state, this parameter sharing enables the RNN to handle sequential data more quickly and accurately while capturing temporal relationships.

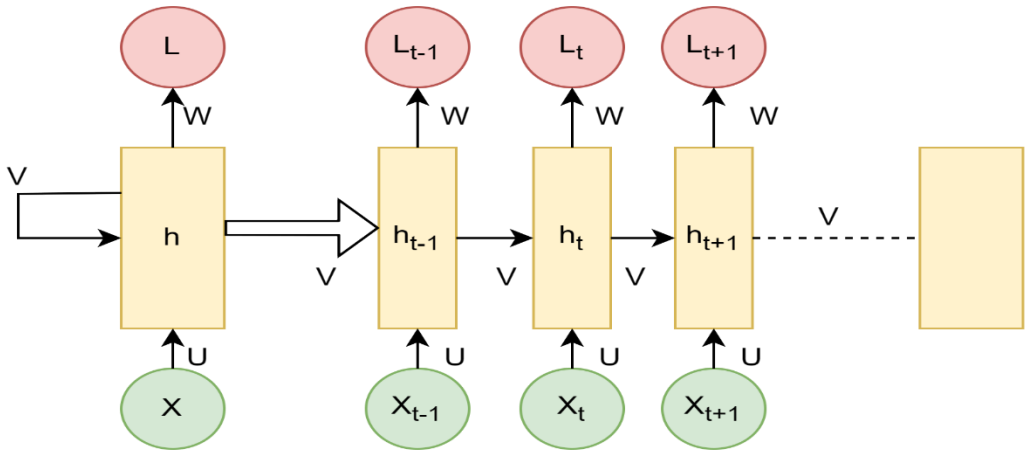

Figure 4: RNN Architecture

For every time step, there is one fixed activation function unit in the recurrent neural network. Every unit possesses an internal state known as the unit's hidden state. At a particular time step, this hidden state represents the prior information that the network now possesses. This concealed state is updated at each time step to reflect any modifications to the network's historical knowledge. This recurrence relation is used to update the concealed state.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

The formula for calculating the current state**:**

$$h_t = f(h_t - 1, X_t) \quad (1)$$

where
Current state = h_t
Next state = h_{t+1}
Previous State = h_{t-1}
The formula for applying the Activation function(tanh)

$$h_t = tanh(W_{hh}\, h_t - 1 + W_{xh} h X_t) \quad (2)$$

where,

- W_{hh} - weight at recurrent neuron
- W_{xh} - weight at input neuron

The formula for calculating output:

$$L_t = W_{hL} h_t \quad (3)$$

- L_t - output
- W_{hL} - weight at output layer

4. DATASET

This work has made use of the NSL-KDD dataset. The NSL-KDD dataset is a more refined and condensed version of the KDD'99 dataset, which was used as a benchmark for assessing intrusion detection systems. The KDD'99 dataset has a lot of redundant records in both the training and test sets, which is its biggest drawback. This makes learning classifiers biased toward the more frequently occurring records during training and increases classification accuracy whenever these same records appear in the test set. The NSL-KDD dataset addresses the issues present in the KDD-CUP dataset by rectifying problems, eliminating duplicate records from both the training & test sets, and enhancing the representation of minority samples in the test set. This improvement enables a more effective differentiation between various models in intrusion detection. By eliminating redundant data, the NSL-KDD gets over the restrictions above and offers a better classifier evaluation. There are 125,973 records in the training set KDDTrain+ and 22,544 records in the testing set KDDTest+.Each record in the NSL-KDD dataset has 41 features, divided into three groups.

5. PROPOSED FRAMEWORK

In the suggested system we have used a hybrid model consisting of a combination of LSTM and GRU for classification. For feature extraction, we used the XGboost algorithm which gives very good results. After the collection of data (NSL -KDD) some preprocessing techniques are also applied to the data. We applied data cleaning, Data Normalization, and one hot encoding technique to improve the data then we applied a feature extraction technique and then a classification technique to find out the attack. This framework can be used for multi-classification and binary classification. Four types of classes can be find out DoS, Probe, U2R, R2L. We used the ReLU activation function for the input layer, sigmoid for the hidden layer, and softmax for the output layer. We have used TensorFlow, an open-source Python neural network library, and Keras to implement our model on Google Colab. The evaluation of the suggested method's efficacy involved the creation of a confusion matrix. In this matrix, each row signifies a case within a predicted class, and each column signifies a case within the actual class.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

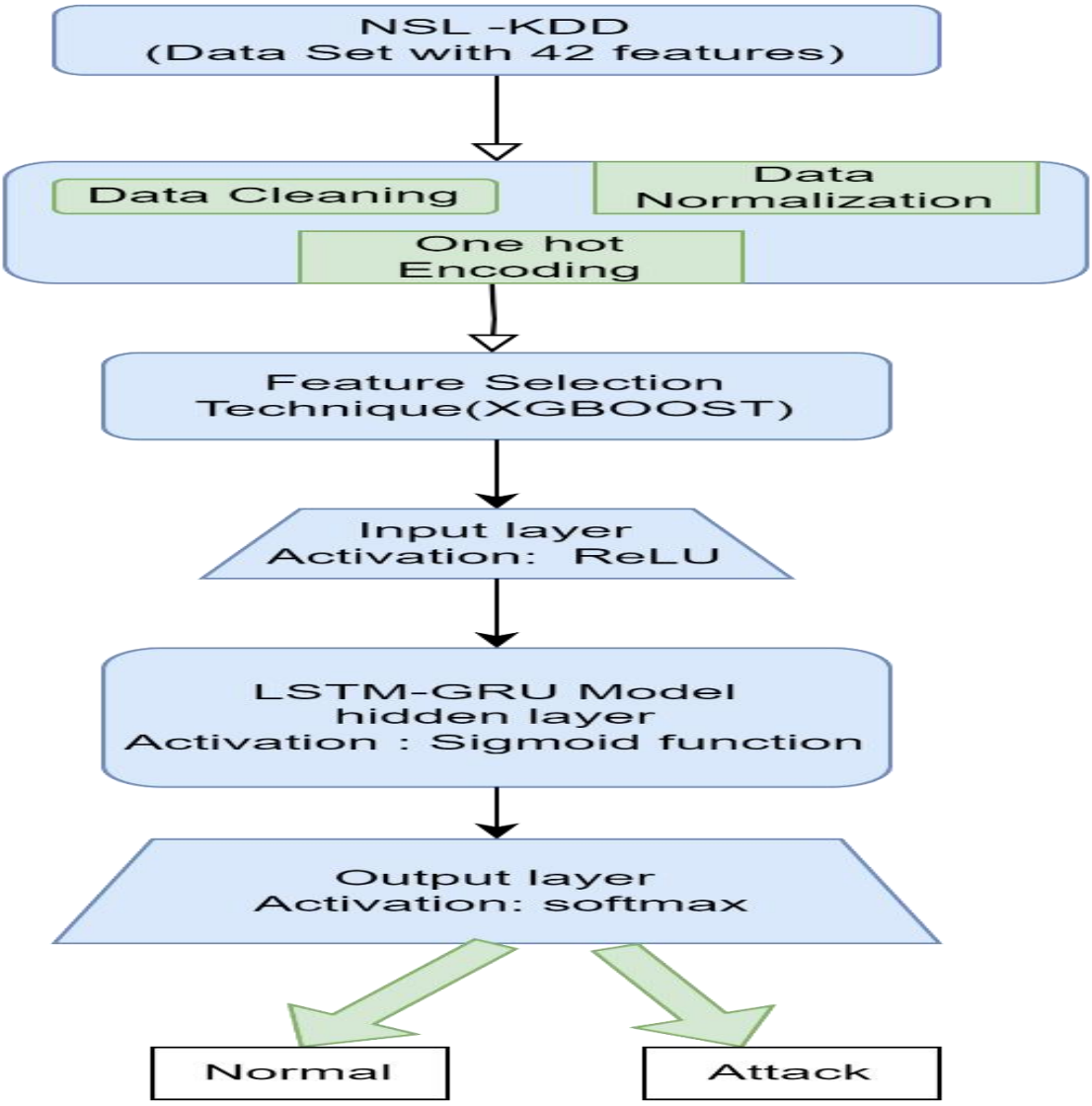

Figure 5: Proposed Framework

ALGORITHM

Input

1. Dataset input for training and testing

Data Preprocessing

2. Data cleaning: remove duplicate and irrelevant data
3. Data Normalization: using min-max scaling tech.
4. One hot encoding: Convert input data to binary

Feature Selection

1. Selection of 22 features from the dataset using XGboost

Data Training

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

1. Backward Propagation: update weights
2. Forward Propagation: find out output

Model Building

1. Two layers for hybrid model (LSTM, GRU)
2. First layer of LSTM with 128 hidden layer
3. Second layer of GRU with 64 hidden layer (output of LSTM given to GRU layer)

Evaluation

1. Calculations and assessments were done for accuracy, detection rate, and false alarms to determine the efficacy of the model.

Output

1. Detect Attacks

LSTM-GRU hybrid model approach

In the proposed model, we have used an LSTM-GRU hybrid architecture, in which we have 6 layers,3 layers for LSTM and 3 layers for GRU

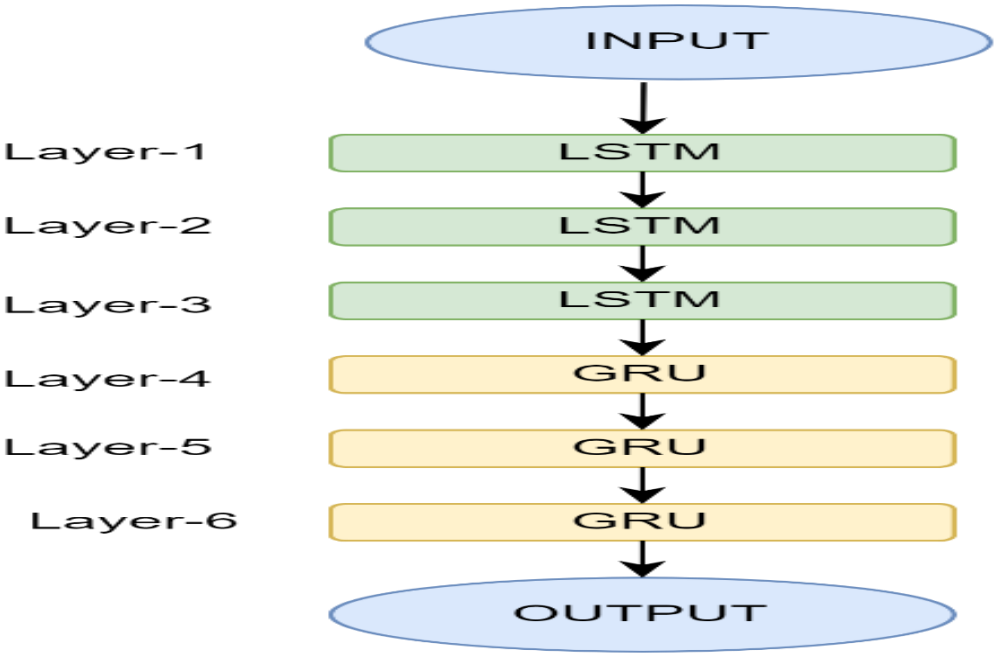

Figure 6: Layers in Model

6. FEATURE NORMALIZATION

A preprocessing method called feature normalization is used in machine learning to scale and standardize a dataset's input features. The goal is to ensure that all features are equally valuable to the learning process, to prevent some features from being preferred over others, and to increase the consistency of the algorithm. In this article, we will use the min-max scaling technique.

$$X \text{ normalization} = X - \min(X)/\max(X)-\min(X)$$

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

7.XGBOOST FEATURE SELECTION

XGBoost, or Extreme Gradient Boosting, stands out as a widely embraced ML algorithm employed for tasks like regression and classification in supervised learning. While XGBoost is not a feature extraction technique, it does provide some mechanisms that are comparable to feature extraction in that they assess feature significance. XGBoost provides a built-in feature importance score mechanism based on the contribution of each feature to the model's performance. In machine learning, feature selection is an essential phase, particularly when working with high-dimensional data. Three categories of feature significance scores are computed by XGBoost. Gain: The average reduction in loss experienced while utilizing a splitting function. Cover: The quantity of times a feature is applied, weighted by training data points, to divide data among trees. Weight: The total count of data splits across all trees using a feature.

8. PERFORMANCE EVALUATION

Calculations and assessments were performed to determine the accuracy, detection rate, and false alarms of the model in order to determine its efficacy. The data categories in the confusion matrix are shown in Table 1. When attack information is correctly identified as an attack, it is referred to as True Positive (TP). False Positives (FP) happen when legitimate material is mistakenly identified as malicious. Genuine Negatives (TN) signify accurately classifying normal data as normal. False Negatives (FN) happen when real attack data is mistakenly classified as normal.

9.EXPERIMENTAL RESULT & DISCUSSION

Table 1: Data categories

Actual Predicted	Malicious	Normal
Malicious	TP	FN
Normal	FP	TN

Table 2: Confusion Matrix for KDDTrain^{+}

Actual Predicted	Malicious	Normal
Malicious	14500	735
Normal	109	7200

Table 3: Confusion Matrix for KDDTest^{+}

Actual Predicted	Malicious	Normal
Malicious	8150	934
Normal	66	2700

Table 4: Confusion Matrix for KDDTest^{-21}

Actual Predicted	Malicious	Normal
Malicious	102,900	12,335
Normal	1238	9500

Table 5: Proposed System Performance for each dataset

Dataset	Accuracy	False Alarm	Detection Rate
KDDTrain^{+}	97	0.40	96
KDDTrain^{+}	92	0.58	91
KDDTest^{-21}	90	0.130	89

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

Table 6: Comparison with Old Model

Model	Accuracy
RNN (basic)	81.29%
RNN(GRU)	85.65%
RNN(LSTM)	88.4%
RNN(LSTM-GRU)	90%

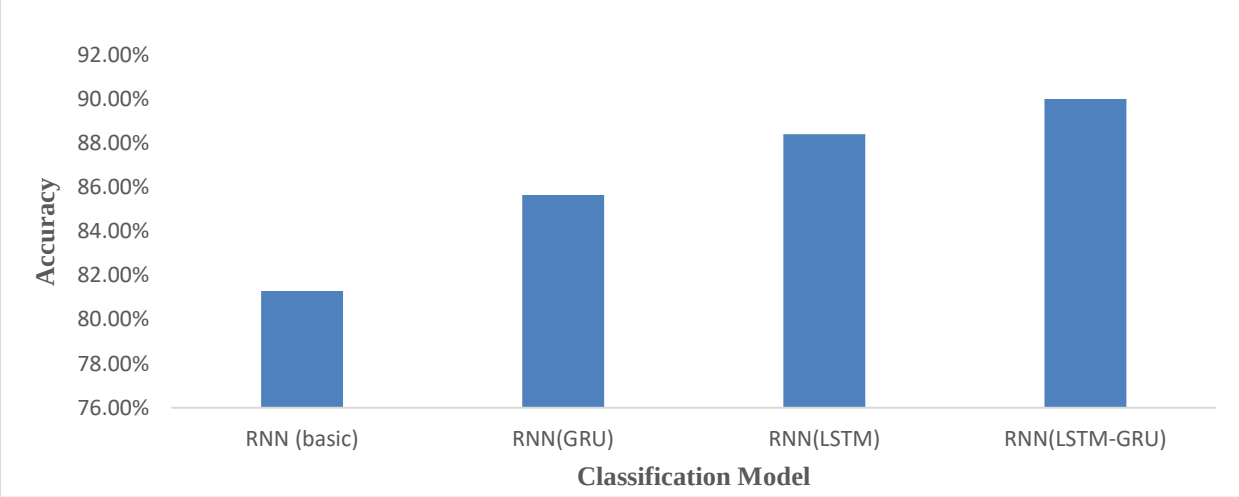

Figure 7: Comparison Chart

10. Conclusion

The development of an LSTM-based ID system as described indicates a promising direction in cybersecurity, leveraging the strengths of LSTM networks to address the limitations of traditional RNNs. For researchers and practitioners in the field, such advancements not only offer immediate improvements in detecting and mitigating intrusions but also open avenues for further research into making ID systems more effective, adaptable, and scalable. This study is carried out for efficient IDS using a hybrid architecture of DL techniques. This paper, suggests the hybrid architecture of the LSTM and GRU model including feature selection using XGboost and it shows better accuracy in comparison with the previous models. We achieved 90% accuracy using the proposed architecture. The results achieved are significant in the area of cyber security. The hybrid model performs more accurately than other models. In the future, this hybrid model can be used for IOT applications for intrusion detection. We can use hybrid model for heterogeneous networks using federated learning.

References

[1] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[2] N. Chakraborty, “INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM: A COMPARATIVE STUDY,” International Journal of Computing and Business Research.

[3] A. Choudhary, A. Tripathi, A. Sharma and R. Singh, "Evolution and comparative analysis of different Cloud Access Security Brokers in current era," 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP), Uttarakhand, India, 2022, pp. 36-43, doi: 10.1109/ICFIRTP56122.2022.10059416.

[4] S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, “A Survey on Anomaly Based Host Intrusion Detection System,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Apr. 2018. doi: 10.1088/1742-6596/1000/1/012049.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

[5] Ahmed Sleem. (2022). Intelligent and Secure Detection of Cyber-attacks in Industrial Internet of Things: A Federated Learning Framework. Journal of Journal of Intelligent Systems and Internet of Things, 7 (1), 51-61 (Doi : https://doi.org/10.54216/JISIoT.070105)

[6] Sharma, A., Goar, V., Kuri, M., Chowdhary, C.L. (2023). Supply Chain Management Using Blockchain Security Enhancement. In: Goar, V., Kuri, M., Kumar, R., Senjyu, T. (eds) Advances in Information Communication Technology and Computing. Lecture Notes in Networks and Systems, vol 628. Springer, Singapore. https://doi.org/10.1007/978-981-19-9888-1_15

[7] Li, Z., Rios, A., & Trajković, L. (2021). Machine Learning for Detecting Anomalies and Intrusions in Communication Networks. *IEEE Journal on Selected Areas in Communications*, 39, 2254-2264. https://doi.org/10.1109/JSAC.2021.3078497.

[8] V. Gupta, N. Kumar, A. Sharma and A. Abraham, "Sensor Routing Protocol with Optimized Delay and Overheads in Mobile based WSN", Journal of Information Assurance & Security, vol. 16, no. 4, 2021.

[9] J. Suji Priya, Dr. Aditi Sharma, Dr. S. Gopinath, H. Muthukrishnan, Emmanuel Babu Pukkunnen, Dr. P. Jenopaul, S. Gowdham Kumar. (2021). Block Chain (Binary Relevance Method) Using Machine Learning Technique. Annals of the Romanian Society for Cell Biology, 1537–1548.

[10] Ferrag, M., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.*, 50. https://doi.org/10.1016/j.jisa.2019.102419.

[11] Liu, H., & Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*. https://doi.org/10.3390/app9204396.

[12] Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. (2019). A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection. *IEEE Communications Surveys & Tutorials*,21,686-728. https://doi.org/10.1109/COMST.2018.2847722.

[13] A. K. Vashishtha, A. Chauhan and A. Sharma, "Key Spreading and Mutual Validation schemes for Privacy Protection in Fog Computing Environment using MNSOR Protocols", Journal of Information Assurance & Security, vol. 16, no. 4, pp. 148-155, 2021.

[14] Samanta, S., Sarkar, A., Sharma, A., Geman, O. (2022). Security and Challenges for Blockchain Integrated Fog-Enabled IoT Applications. In: Rout, R.R., Ghosh, S.K., Jana, P.K., Tripathy, A.K., Sahoo, J.P., Li, KC. (eds) Advances in Distributed Computing and Machine Learning. Lecture Notes in Networks and Systems, vol 427. Springer, Singapore. https://doi.org/10.1007/978-981-19-1018-0_2

[15] R. Bhadada and A. Sharma, "Montgomery implantation of ECC over RSA on FPGA for public key cryptography application," 2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking, Surat, India, 2014, pp. 1-5, doi: 10.1109/ET2ECN.2014.7044973.

[16] A. Sharma, M. Patel, A. Choudhary and G. Kumar, "Blockchain Based Security Enabled Smart Contract for Energy Management," 2023 16th International Conference on Security of Information and Networks (SIN), Jaipur, India, 2023, pp. 1-7, doi: 10.1109/SIN60469.2023.10474845.

[17] Srinath Venkatesan, "Design an Intrusion Detection System based on Feature Selection Using ML Algorithms "

[18] MSEA, vol. 72, no. 1, pp.702–710, Feb. 2023. DOI: https://doi.org/10.17762/msea.v72i1.2000

[19] Shone, N., Ngoc, T., Phai, V., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2, 41-50. https://doi.org/10.1109/TETCI.2017.2772792.

[20] A. A. Alzubaidi, A. A. Alshahrani, and A. M. Alzahrani, "A Hybrid Deep Learning Model for Intrusion Detection System," Journal of Information Security and Applications, vol. 57, pp. 102-110, 2021. doi: 10.1016/j.jisa.2021.102110.

[21] G. Sonowal, A. Sharma and L. Kharb, "Spear-phishing emails verification method based on verifiable secret sharing scheme", Journal of Information Assurance & Security, vol. 16, no. 3, pp. 117-124, 2021.

[22] Mariam Ibrahim, Ruba Elhafiz, Modeling an intrusion detection using recurrent neural networks, Journal of Engineering Research, Volume 11, Issue1,2023,100013, ISSN 2307- 1877 https://doi.org/10.1016/j.jer.2023.100013.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024

[23] Samanta, Saikat, Sarkar, Achyuth, Gupta, Charu and Sharma, Aditi. "Machine learning integrated blockchain model for Industry 4.0 smart applications". Knowledge Engineering for Modern Information Systems: Methods, Models and Tools, edited by Anand Sharma, Sandeep Kautish, Prateek Agrawal, Vishu Madaan, Charu Gupta and Saurav Nanda, Berlin, Boston: De Gruyter, 2022, pp. 13-25. https://doi.org/10.1515/9783110713633-002

[24] Boukhalfa, A., Abdellaoui, A., Hmina, N., & Chaoui, H. (2019). LSTM deep learning method for network intrusion detection system. *International Journal of Electrical and Computer Engineering (IJECE)*. https://doi.org/10.36478/jeasci.2020.227.232.

[25] Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(1), 65. https://doi.org/10.1186/s40537-021-00448-4

[26] Kumar, N., Sharma, A. (2019). A Spoofing Security Approach for Facial Biometric Data Authentication in Unconstraint Environment. In: Pati, B., Panigrahi, C., Misra, S., Pujari, A., Bakshi, S. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 713. Springer, Singapore. https://doi.org/10.1007/978-981-13-1708-8_40

[27] Fu, Yanfang & Du, Yishuai & Cao, Zijian & Li, Qiang & Xiang, Wei. (2022). A Deep Learning Model for
a. Network Intrusion Detection with Imbalanced Data. Electronics. 11. 898. 10.3390/electronics11060898.

[28] Aldallal A. Toward Efficient Intrusion Detection System Using Hybrid Deep Learning Approach. *Symmetry*. 2022; 14(9):1916. https://doi.org/10.3390/sym14091916

[29] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for 5, Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol-5.pp. 21954-21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[30] Nongmeikapam Brajabidhu Singh, Moirangthem Marjit Singh, Arindam Sarkar, Jyotsna Kumar Mandal, A novel wide & deep transfer learning stacked GRU framework for network intrusion detection, Journal of Information Security and Applications, Volume 61,2021,102899, ISSN22141226 https://doi.org/10.1016/j.jisa.2021.102899

[31] Ahsan, M., & Nygard, K. (2020). Convolutional Neural Networks with LSTM for Intrusion Detection. , 69-79. https://doi.org/10.29007/j35r.

[32] Sharma, A., Sharma, C., Sharma, R., Panchal, K.D. (2023). Crime Analysis and Prediction in 7 States of India Using Statistical Software RStudio. In: Goar, V., Kuri, M., Kumar, R., Senjyu, T. (eds) Advances in Information Communication Technology and Computing. Lecture Notes in Networks and Systems, vol 628. Springer, Singapore. https://doi.org/10.1007/978-981-19-9888-1_8

[33] Mirza, A., & Cosan, S. (2018). Computer network intrusion detection using sequential LSTM Neural Networks autoencoders. *2018 26th Signal Processing and Communications Applications Conference (SIU)*, 1-4. https://doi.org/10.1109/SIU.2018.8404689.

[34] J. K. Samriya, C. Chakraborty, A. Sharma, M. Kumar and S. K. R, "Adversarial ML-Based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2023.3341696.

[35] Zhang, J., Ling, Y., Fu, X., Yang, X., Xiong, G., & Zhang, R. (2020). Model of the intrusion detection system based on the integration of spatial-temporal features. Comput. Secur., 89. https://doi.org/10.1016/j.cose.2019.101681.

[36] Donkol, A., Hafez, A., Hussein, A., & Mabrook, M. (2023). 11, 9469- Optimization of Intrusion Detection
a. Using Likely Point PSO and, Enhanced LSTM-RNN Hybrid Technique in Communication Networks. IEEE Access 11, 9469-9482 https://doi.org/10.1109/ACCESS.2023.3240109.

Doi : https://doi.org/10.54216/JCIM.130201
Received: July 21, 2023 Revised: November 16, 2023 Accepted: February 02, 2024