Vol-08 Issue 03, March- 2024 Impact Factor: 7.936
ISSN: 2456-9348

iJETRM
International Journal of Engineering Technology Research & Management
www.ijetrm.com

ANOMALY BASED INTELLIGENT INTRUSION DETECTION SYSTEM OF SECURITY ATTACKS USING GRU AND LSTM CLASSIFIERS

J. Umadevi[1], Dr.S.Babu Renga Rajan[2],E.Suwetha[3]
[1]Assistant professor, PET Engineering College vallioor
[2]Professor& HOD, PET Engineering College vallioor
[3]PG student, PET Engineering college vallioor

Abstract
Anomaly-based intelligent intrusion detection systems leverage advanced algorithms and machine learning techniques to monitor network traffic, system behavior, and user activities in real-time. This proactive approach enhances the ability to detect and respond to emerging attack vectors that traditional signature-based systems may miss. This project proposes an anomaly-based intelligent intrusion detection systems of security attacks using GRU and LSTM classifiers. Initially input data set is gathered for data preprocessing. Data preprocessing is the concept of changing the raw data into a clean data set. The data-set is preprocessed in order to check missing values, noisy data, and other inconsistencies before executing it to the data exploration. This dataset is further moved to feature selection. The selected features are classified by using GRU and LSTM classifiers. The LSTM (Long -short-term memory) and GRU (Gated Recurrent Unit) have gates as an internal mechanism, which control what information to keep and what information to throw out. By doing this LSTM, GRU networks solve the exploding and vanishing gradient problem. Finally in model evaluation accuracy, recall, f1score, precision is predicted. This project is implemented in python language.

Keywords-
Cyber security, internet of things, intrusion detection system, security attacks, deep learning.

I. INTRODUCTION

The pervasive use of interconnected computer systems has become an irreplaceable aspect of organizational and daily life activities. Concurrently, it had led to concerns about the online privacy and security of the users. As per recent surveys, the reported cyber security attacks in 2021 were approximately 5.1 billion. The reports also indicate a surge in sophisticated and high-impact cyber [1]Vehicular Ad hoc Network (VANET) is an enabling technology to provide a variety of convenient services in intelligent transportation systems, and yet vulnerable to various intrusion attacks. Intrusion detection systems (IDSs) can mitigate the security threats by detecting abnormal network behaviours. Blockchain (BC) [2]emerges as a technology that can manage the data and build trust efficiently and transparently. It can also aid in transaction authorization and verification in the supply chain or payments without a third party

Problem statement -Anomaly-based intelligent intrusion detection systems play a critical role in safeguarding computer networks and systems from security attacks. These systems utilize advanced machine learning techniques, such as Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) classifiers, to analyze network traffic and identify abnormal patterns indicative of security breaches or malicious activities. The problem overview of developing such a system involves addressing the evolving landscape of cyber threats, including sophisticated attacks such as zero-day exploits and polymorphic malware, which traditional signature-based detection methods struggle to detect. the proposed intrusion detection system aims to enhance the detection accuracy and[3]We present a comparative study on the most popular machine learning methods applied to the challenging problem of customer churning prediction in the telecommunications industry. In the first phase of our experiments, all models were applied and evaluated using cross-validation on a popular, public domain dataset (CNN) is among the Deep learning models that are designed predominantly for image data. CNN is among the recent and highly accurate classification approaches in image processing. In the last few decades, the use of image processing in the healthcare industry has obligated researchers for achieving extreme precision in image analysis, detection, and classification.

Summary of our contribution -We have applied gated recurrent unit and long short term memory to perform feature selection and to reduce the dimensions of the data-set. After, pre-processing of data, we have applied some of the famous deep learning techniques.Then we have use the power of ensemble learning in order to algorithms and achieve better results.Then we have evaluate the algorithms on test set using confusion matrix and ROC curve, which have been mentioned in form of graphs and tables in order to compare which algorithm performs best for this particular data-set.

II. REVIEW OF LITERATURE

Network intrusion detection and prevention systems utilize [4]In recent years cyberattacks, especially those targeting systems that keep or process sensitive information, are becoming more sophisticated. Critical National Infrastructures are the main targets of cyber attacks since essential information or services depend on their systems and their protection becomes a significant issue that is concerning both organizations and nationsmachine learning for accuracy that exceeds the limits of existing rule-based methods.

As machine learning models evolve, they require higher processing power, and accordingly, hardware accelerators with higher computational power are being released.[5]n order to proactively mitigate cyber-security risks, security analysts have to continuously monitor sources of threat information. However, the sheer amount of textual information that needs to be processed is overwhelming, and it requires a great deal of mundane labor to separate the threats from the noise. When a network intrusion occurs, it is important to detect it without delay and block it to prevent further damage. Nevertheless, a current machine-learning-based IDS/IPS determines whether an intrusion has occurred within each session only after the session has terminated, and traffic is differentiated with a 5-tuple, which are key to identifying one session. In traffic divided into sessions, the statistical values of the traffic transmitted and received from the beginning of the session until the end. Become the features of the session.

The machine learning model is trained using such features, and maliciousness is determined on a per-session basis. It means a network intrusion is detected after session termination, [6]The network architecture is always vulnerable to various types of security breaches, attempted break-ins, penetration attacks and other similar intrusions by unauthorized and malicious users. The network being a repository aims at sharing resources between authorized users, also attracts unwanted users who are interested in exploiting them. In addition, formulations of global protection policies are rare and difficult to implement. The security breach or intrusion is a critical issue for any organization.

As hardware technology continues to advance,[7]a hybrid and layered Intrusion Detection System (IDS) is proposed that uses a combination of different machine learning and feature selection techniques to provide high performance intrusion detection in different attack types. In the developed system, firstly data preprocessing is performed on the NSL-KDD dataset, then by using different feature selection algorithms. Ultimately, to detect an intrusion immediately, the problem of how to determine when accurate detection is possible must be solved

III. PROPOSED SYSTEM

This consist of various phases of the proposed model
it consist of five phases, namely,

1. Data preprocessing (data cleaning, data integration, data transformation, data reduction, data discretization)
2. Cleaning and filtering (handling null and missing values)and
3. Data exploration (exploratory data analysis EDA
4. Feature selection
5. Cross validation(using GRU and LSTM classifiers) Finally ,accuracy, recall, and precision are predicted in model evaluation of predictive models on test set (using confusion matrix and ROC curve)

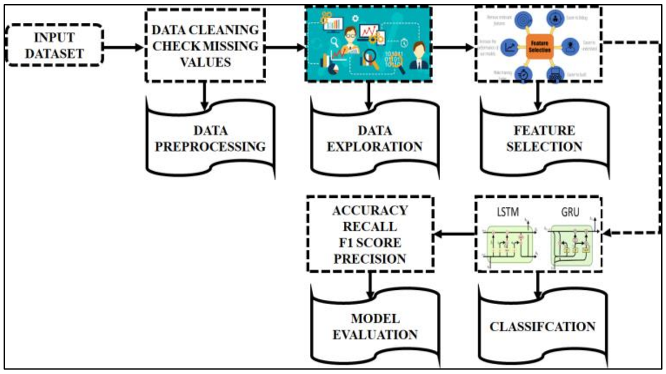


Fig 3.1Framework proposed system

Data pre-processing is one of the important techniques of data mining which helps to clean and filter the data. Thus, removing the inconsistencies and converting raw data into a meaningful information which can be managed efficiently. It is important to remove null values or missing values in the data-set and to check the data-set for imbalanced class distributions, which has been one of the emerging problems of data mining. The problem of imbalanced data-set can be solved through data preprocessing.

Data Preprocessing :

The input dataset is initially acquired for data preparation. The concept of data preprocessing is the transformation of raw data into a clean data set. Before performing the data exploration, the dataset is preprocessed to check for missing values, noisy data, and other irregularities.The primary purpose of feature selection is to improve predictive model performance while lowering modelling computational costs.

Cleaning and Filtering:

Cleaning & Filtering: This phase consists of data cleaning and filtering by removing missing values, non-relevant parameters, etc. Data cleaning is the key to reduce dimensions of the data-set It refers to the first step in data analysis in which data analysts define dataset characterizations using data visualisation and statistical tools. These datasets are then passed to the feature selection stage.

Data exploration

Data exploration also known as data exploratory data analysis, refers to the initial phase of the data analysis process where the main objective[8] Intrusion detection system (IDS) plays a significant role in preventing network attacks and plays a vital role in the field of national security is to gain a better understanding of the data-set data exploration helps identify patterns, trends, and distributions with in the data. This involves examining the central tendency and dispersion of numerical variables, and visualizing the data through various charts, graphs and statistical summaries.

Feature Selection

Feature Selection, also known as variable selection or attribute selection is the process of identifying and selecting a subset of relevant features from a large set of available feature in a data set[9]IT services, thereby freeing them from complex underlying hardware, software, and protocol stacks. Although “open for all service” is the essence of cloud computing, it does not necessarily comprise useless information. Tenants can use cloud services for efficient computing improve the performance and efficiency of deep learning models

Cross Validation

To overcome these problems, researchers proposed new anomaly detection techniques based on machine learning [1]. By using a comprehensive dataset with multiple attack types, a well-trained model can be created to improve anomaly detec- tion performance To overcome these problems, researchers proposed new anomaly detection techniques based on machine learning [1]. By using a comprehensive dataset with multiple attack types, a well-trained model can be created to improve anomaly detec- tion performance However, a vast quantity of training data is required for the operation, which can become challenging in a heterogeneous and dynamic environment.In particular, with the increasing number of potential attacks, collecting a big amount of data that describes each possible attack category is not always feasible However, a vast quantity of training data is required for the operation, which can become challenging in a heterogeneous and dynamic environment.In particular, with the increasing number of potential attacks, collecting a big amount of data that describes each possible attack category is not always feasible

Recently, machine learning techniques are gaining much interest in security applications as they exhibit fast processing[10] capabilities with real-time predictions. One of the significant challenges in the implementation of these techniques is the available training data for each new potential attack categoryModel evaluation Finally,accuracy, recall, f1score and precision are predicted in model evaluation For model evaluation confusion matrix and ROC curve are taken into consideration..

IV. METHODOLOGY

Anomaly-based intelligent intrusion detection systems involves.[11]To ensure information security of the train-ground communication system, an intrusion detection method based on machine learning and state observer is proposed to detect and recognize various attacks in this paper[12]Electrical networks of transmission system operators are mostly built up as isolated networks without access to the Internet. With the increasing popularity of smart grids, securing the communication network has become more important to avoid cyber-attacks that could result in possible power outages.an intrusion detection model SAAE-DNN, based on stacked autoencoder (SAE), attention mechanism and deep neural network (DNN), is proposed.

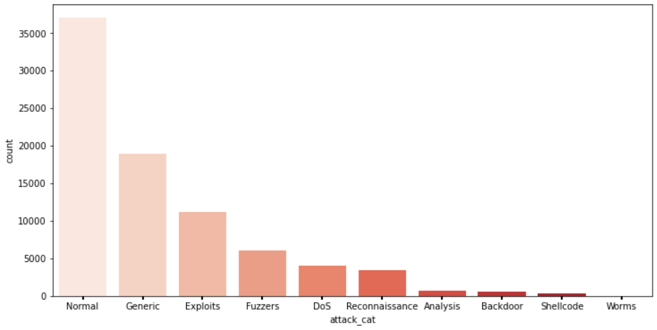


Fig 4.1 Attack categories

It represents that levels of IoT networks attacks. This figure consider a count and attack categories. intrusion detection systems focuses on assessing the interaction and interoperability between different components or modules of the system.

.

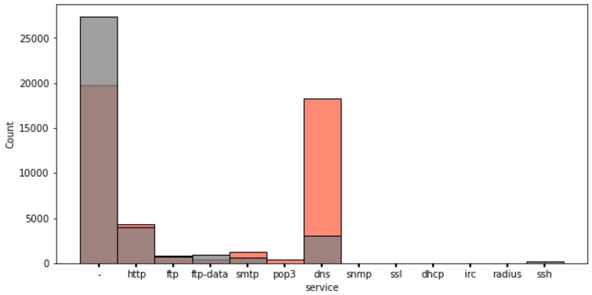
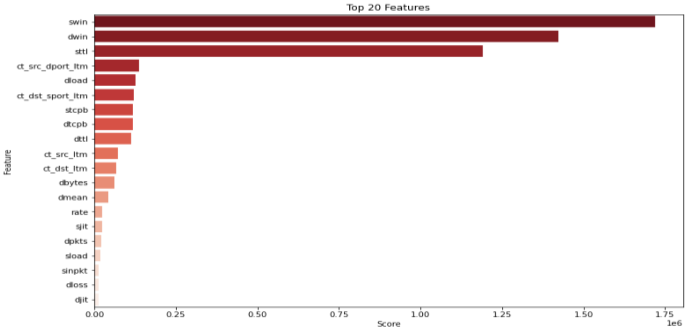


Fig. 4.2 service

This figure represent the service. A service bar chart in the context of intrusion detection could be a graphical representation illustrating the distribution or status of different services within a network or system.[13]Recent traffic classification works suggested using statistical flow features to classify network traffic accurately using machine learning techniques. The selected classification features must be stable and can work across different spatial and temporal heterogeneity.



..

Figure: 4.3 Top Features

This figure demonstrates that each bar on the chart represents a specificfeature used in the intrusion detection system.These[14] Various management tasks and network operations such as security, intrusion detection, Quality-of-Service provisioning, performance monitoring, resource provisioning, and traffic engineering require traffic classification.[15]A possible solution to this issue is the use of the integrated fiber-wireless access network. In addition, dynamic and efficient network configurations can be achieved through software-defined networking (SDN), an innovative and programmable networking architecture enabling machine learning (ML) to automate networks features could includeaspectssuch as network traffic patterns, user behavior, system logs, anomaly scores, or any other characteristics relevant to intrusion detection.

Performance indicators – Recall It is the ratio of real churners (True Positive), and is calculated under the following:

$$Recall = \frac{T_p}{T_p + F_n}$$

Precision - It is the ratio correct predicted churners, and is calculated under the following:

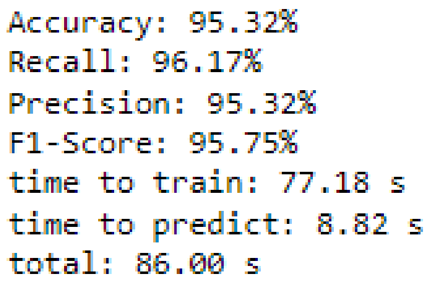
$$Precision = \frac{T_p}{T_p + F_p}$$

Accuracy - It is ration of number of all correct predictions, and is calculated under the following:

$$Accuracy = \frac{(T_p + T_n)}{(T_p + F_p + T_n + F_n)}$$

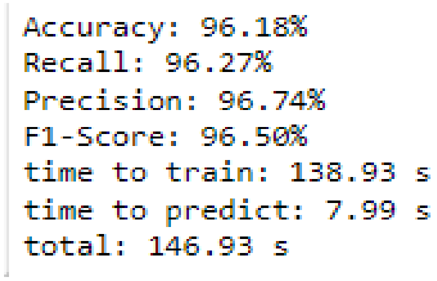
V. DISCUSSION

Final data preprocessed datasets implemented on chosen standard deep learning algorithm of Gated recurrent unit and Long short term memory classifiers.Furthermore, accuracy performance of above model improved with help of GRU and LSTM classifiers The acquired, evaluated results are represented in Table (5.1) and Table (5.2) These results are graphically represented confusion matrix shown in figure 5.1 (a),(b)respectively.It shows that confusion matrix for LSTM. In this image we find accuracy, recall, precision, F1-score.



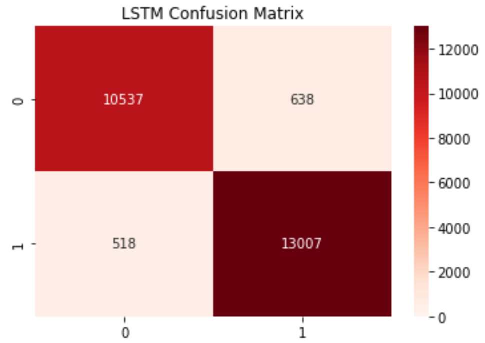
```
Accuracy: 95.32%
Recall: 96.17%
Precision: 95.32%
F1-Score: 95.75%
time to train: 77.18 s
time to predict: 8.82 s
total: 86.00 s
```

Table 5.1 Confusion matrix for LSTM

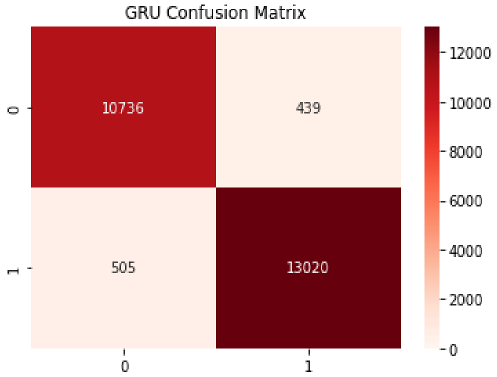


```
Accuracy: 96.18%
Recall: 96.27%
Precision: 96.74%
F1-Score: 96.50%
time to train: 138.93 s
time to predict: 7.99 s
total: 146.93 s
```

Table 5.2 Confusion matrix for GRU



(a)



(b)

Fig 5.3 (a), (b) Graphical representation of Confusion matrix of GRU and LSTM

In overall analysis of confusion matrix of Gated recurrent unit and Long short term memory with are resulted 95.32%, 96.18% respectively. showed that the uses of Gated recurrent unit and Long short term algorithm achieve highest accuracy. Especially, highest F1- measure were observed compared to others.

VI.CONCLUSION AND FUTURE ENHANCEMENT

The proposed Intrusion Detection System has the advantage of being able to stop malicious users before they cause damage to the network, because it can determine whether an intrusion is occurring before the session terminates. In addition, using the packet feature to reduce unnecessary time and memory to statistically analyze and calculate packet data to generate the session feature is a great advantage. This is important considering that network intrusions are becoming more diverse while, at the same time, the number and quantity of sessions are increasing significantly. In this project an anomaly-based intelligent intrusion detection systems of security attacks using Gated recurrent unit and Long short term memory classifiers was developed. The input datasets was initially acquired for data preparation.The concept of data preprocessing is the transformation of raw data into a clean data set. Before running the data exploration, the datasets was preprocessing to check for missing values, noisy data, and other irregularities. It refers to the first step in data analysis in which data analysts define datasets characterizations using data visualization and statistical tools. These datasets are then passed to the feature selection stage. The primary purpose of feature selection is to improve predictive model performance while lowering modeling computational costs. Grated recurrent unit and Long short term memory classifiers were used to classify the selected characteristics.The fundamental mechanism of the Long-Short-Term Memory and Gated Recurrent Unit is gates, which control what information is kept and what information is discarded. Gated recurrent unit networks handle the exploding and disappearing gradient problem using Long short term memory. Finally, accuracy, recall, f1score, and precision are predicted in model evaluation.

REFERENCE

[1]Shu J, Zhou L, Zhang W, Du X and Guizani M, Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach, IEEE Transactions on Intelligent Transportation Systems, 2020, vol. 22, no. 7, pp.4519-4530.

[2]B. ShanmugaSundari, "Blockchain Technology for Secure Supply chain Management, International Journal of Research in Science, Engineering and Technology (IJIRSET), Volume 12, Issue 7, July 2023 e-ISSN: 2319-8753|p-ISSN: 2347-6710

[3] B. ShanmugaSundari, Machine Learning Approach on Customer Churn Analysis: A Comparative Study, International Journal for Science and Advance Research in Technology" ISSN[Online}: 2395-1052, Volume : 8, Issue : 6: https://ijsart.com/Home/IssueDetail?id=55341, **Publication Date:** 6/20/2022

[4] Ferrag, Mohamed Amine, LeandrosMaglaras, Ahmed Ahmim, MakhloufDerdour, and HelgeJanicke, Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks, 2020, no.3.

[5] Mendsaikhan O, Hasegawa H, Yamaguchi Y and Shimada H, Quantifying the significance and relevance of cyber-security text through textual similarity and cyber-security knowledge graph, IEEE Access, 2020, vol. 8, pp.177041-177052.

[6] Gurung S, Ghose M K and Subedi A, Deep learning approach on network intrusion detection system using NSL-KDD dataset. International Journal of Computer Network and Information Security, 2019, vol. 11, no.3, pp.8-14.

[7] Cavusoglu U, A new hybrid approach for intrusion detection using machine learning methods. Applied Intelligence, 2019, vol. 49, no.7, pp.2735-2761.

[8] Tang C, Luktarhan N and Zhao Y, SAAE-DNN: Deep learning method on intrusion detection. Symmetry, 2020, vol. 12, no. 10, pp.1695.

[9] Wang W, Du X, Shan D, Qin R and Wang N, Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine, IEEE Transactions on Cloud Computing, 2022, vol. 10, no. 3, pp. 1634-1646.

[10] Chkirbene Z, Erbad A, Hamila R, Gouissem A, Mohamed A, Guizani M and Hamdi M, A Weighted Machine Learning-Based Attacks Classification to Alleviating Class Imbalance, IEEE Systems Journal, 2021,vol. 15, no. 4, pp. 4780-4791.

[11] Gao B, B. Bu, Zhang W and Li X, An Intrusion Detection Method Based on Machine Learning and State Observer for Train-Ground Communication Systems, IEEE Transactions on Intelligent Transportation Systems, 2022, vol. 23, no. 7, pp. 6608-6620.

[12] Hong J and Liu C, Intelligent Electronic Devices With Collaborative Intrusion Detection Systems, IEEE Transactions on Smart Grid, 2019, vol. 10, no. 1, pp. 271-281.

[13] B. Mohammed et al., "Edge Computing Intelligence Using Robust Feature Selection for Network Traffic Classification in Internet-of-Things," in IEEE Access, vol. 8, pp. 224059-224070, 2020.

[14] Umair, M.B., Iqbal, Z., Bilal, M., Almohamad, T.A., Nebhen, J. and Mehmood, R.M..An Efficient Internet Traffic Classification System Using Deep Learning for IoT.ArXiv preprint arXiv: 2107.12193.2021.

[15] Ganesan, E., Hwang, I., Liem, A.T. and Ab-Rahman, M.S., June. SDN-enabled FiWi-IoT smart environment network traffic classification using supervised ML models.In Photonics (Vol. 8, No. 6, p. 201). Multidisciplinary Digital Publishing Institute, 2021.

[16] Raikar, M.M., Meena, S.M., Mulla, M.M., Shetti, N.S. and Karanandi, M., Data traffic classification in software defined networks (SDN) using supervised-learning. Procedia Computer Science, 171, pp.2750-2759, 2020.

[17] A. Sivanathan et al., "Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics," in IEEE Transactions on Mobile Computing, vol. 18, no. 8, pp. 1745-1759, 1 Aug. 2019.

[18] A. M. Sadeghzadeh, S. Shiravi and R. Jalili, "Adversarial Network Traffic: Towards Evaluating the Robustness of Deep-Learning-Based Network Traffic Classification," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1962-1976, June 2021.

[19] A. Hameed, J. Violos and A. Leivadeas, "A Deep Learning Approach for IoT Traffic Multi-Classification in a Smart-City Scenario," in IEEE Access, vol. 10, pp. 21193-21210, 2022.

[20] Z. Bu, B. Zhou, P. Cheng, K. Zhang and Z. -H. Ling, "Encrypted Network Traffic Classification Using Deep and Parallel Network-in-Network Models," in IEEE Access, vol. 8, pp. 132950-132959, 2020.