Journal of Science and Technology
ISSN: 2362-1443 (Print) 3059-9490 (Online)
2024, Vol. 4, No. 2 (Special Issue), 40-44

Effective Multi Class Attack Recognition through Formed Arrayized Loop with Integrated Bi-GRU

Kumar Prasun
Padma Kanya Multiple Campus, Tribhuvan University
erkprasun@gmail.com

Anil Verma
Purwanchal Campus, Tribhuvan University
anil@ioe.edu.np

Prajwal Rai
Kantipur City College, Purwanchal University
developer.prajwal007@gmail.com

Yubraj Bhattarai
Kantipur City College, Purwanchal University
yuvraaz014@gmail.com

Article History:
Received: 30 July 2024
Revised: 8 August 2024
Accepted: 17 November 2024

Keywords — Network Intrusion Detection Systems (NIDS),Bidirectional Gated Recurrent Unit (Bi-GRU), Formed Gate Loop Model (FGLM),Arrayized Trigger Unit Function (ATUF),Multi-class classification

***Abstract*— This study introduces a pioneering framework for precise multi-class attack recognition employing a Formed Arrayized Loop with Integrated Bidirectional Gated Recurrent Unit(Bi-GRU). The proposed model addresses the shortcomings of existing network intrusion detection systems (NIDS), which often struggle with lower accuracy,the inability to perform multi-class classification, increased training time,and inefficiency with large datasets. By integrating the Formed Gate Loop Model(FGLM) and Arrayized Trigger Unit Function(ATUF) within the Bi-GRU framework,the model achieves high accuracy and efficient learning. The results reveal a swift decrease in training loss from 0.2967 to 0.0732 and a corresponding increase in training accuracy from 0.9264 to 0.9828. Similarly, the validation loss decreases from 0.0905 to 0.0364, while the validation accuracy rises from 0.9627 to 0.9892 and stabilizes after the tenth epoch, signifying robust generalization capabilities. The close alignment of training and validation metrics suggests minimal overfitting and effective learning of underlying patterns. The proposed approach enhances the selectivity of updating memory, ensures important features are retained, and reduces data dimensionality, leading to faster convergence and improved prediction performance. Recommendations for future work include expanded dataset utilization, real-time implementation, hybrid model development, advanced feature engineering, adaptive learning mechanisms, and the development of a userfriendly interface. This research contributes to the development of robust and effective network intrusion detection systems,essential for safeguarding modern networks against sophisticated attacks.**

I. INTRODUCTION

In recent years, technology and Internet usage have increased dramatically, leading to more complex networks and greater opportunities for attackers to exploit vulnerabilities[1]. Traditional security measures like firewalls are inadequate for detecting these sophisticated attacks, which often exhibit vague network traffic patterns [2][3]. Therefore, advanced techniques like Network Intrusion Detection Systems(NIDS) are essential for monitoring and protecting networks from malicious activities [4].

The growing number of security vulnerabilities, data leaks, network frauds, and ransomware underscores the importance of robust security measures. Conventional detection methods are time-consuming and can result in high false alarm rates. Machine Learning (ML) and Deep Learning (DL)methods offer more precise detection of network attacks.

Existing studies have employed DL techniques like CNN and LSTM for attack detection and classification,but these models have limitations such as lower accuracy,inability to perform multi-class classification,increased training time, and inefficiency with large datasets [5].

To address these shortcomings, the proposed model introduces the Formed Gate Loop Model (FGLM) and Arrayized Trigger Unit Function (ATUF) within a Bidirectional Gated Recurrent Unit (Bi-GRU) framework. The FGLM controls the gate operations to improve the selectivity of updating memory, ensuring important features are retained. The ATUF reduces data dimensionality, using fewer parameters for faster convergence and improved prediction performance [6][7]. This combined approach, FGLM-ATUF, enhances the effective detection and multi-classification of network attacks.

II. LITERATURE REVIEW

Attacks have become increasingly common in recent years, necessitating the examination of network traffic to detect malicious activities that pose threats to systems. Machine Learning (ML) based algorithms are crucial for creating robust Intrusion Detection Systems (IDS) capable of handling large volumes of data. A recommended study utilized KNN, SVM, NB, MLP, ETC, DT, RF, and LR for classifying attacks like Probe, R2L, U2L, and DoS using the NSL-KDD dataset. The results showed that ML classifiers were cost-effective and excellent intrusion detectors [8].

processing strategy to precisely denote features in the dataset, reducing bias in the model. Four different classifiers—RF, MLP, DT, and SAE (Stacked Auto-Encoder)—were compared for predicting and classifying network attacks. The RF model provided the best and most precise outcomes [9].

Classification of attacks is essential for identifying abnormal behavior in networks. A suggested study used ADNN (Artificial Deep Neural Network) for binary classification of attacks, achieving an accuracy of 0.92 with the UNSW-NB dataset, demonstrating the effectiveness of ADNN [10].

Deep Learning (DL) methods have also been employed for attack detection. One study used the BAT model, combining BiLSTM and Attention Mechanism with the NSL-KDD dataset, achieving an accuracy rate of 84.25% [11].

The effectiveness of IDS models relies on techniques like data pre-processing and classification approaches. A recommended model used hybrid feature selection and DNN-based classifiers, along with PCA, ANOVA, and Chi-square tests for feature reduction. The model showed reduced training and testing times but was not validated for multi-class datasets [12].

A hybrid DL model combining CNN and LSTM with a softmax classifier was used for classifying intrusions like DoS, U2R, R2L, and PRB. The study utilized KDDCUP 99 and NSL-KDD datasets, achieving satisfactory accuracy rates [13].

Another study used ensemble models like Voting CMN, Voting RKM, and Voting CKM for identifying DDoS attacks, achieving an accuracy of 89.29% on the UNSW-NB15 dataset, demonstrating suitability for SDN-based IDS networks [14].

AI techniques are key for detecting malicious network activity. A defensive strategy employing hierarchies improved the model's performance under adversarial conditions, enhancing the F1 score and accuracy for attack detection [15]. These studies highlight the importance of advanced ML and DL techniques in creating effective and robust IDS models capable of detecting and classifying network attacks accurately.

III. RESEARCH GAP

From the review of the existing studies, gaps identified are mentioned as below:

- The Future work of the study focuses on employing different DL models and apply these algorithms on public dataset with the aim to check the effectiveness of the model [10].
- Though feature selection techniques like PCA, ANOVA and Chi square have been used in the existing study, the performance of the model can be further improved by utilizing other feature selection approaches in improving future [12].
- The future study of the model focuses on employing IDS for detecting and mitigating DDoS in real time [14].

IV. PROBLEM STATEMENT

From the review of the prevailing works, core concerns recognized are revealed as below:

- The existing study focused on binary classification of attacks [10].
- The accuracy obtained by the study is considerably lower for effective detection of attacks [11].
- Limited samples were used for training and test data in the suggested study [15].

V. RESEARCH OBJECTIVE

The major objective of the proposed framework is to perform multi-class classification using effective approaches to identify and classify attacks present in the network. The specific objectives of the proposed work include:

- To pre-process the data using various pre-processing techniques such as feature scaling and handling missing values.
- To perform multi-class classification for the detection and classification of attacks using the Formed Gate Loop Model (FGLM) and Arrayized Trigger Unit Function (ATUF) within a Bidirectional Gated Recurrent Unit (Bi-GRU) model to produce effective outcomes.
- To assess the efficacy of the proposed model using different performance metrics such as accuracy, F1 score, recall, and precision.

VI. METHODOLOGY

In general, attacks have the ability to deteriorate and causes countless damages to the overall system and network in a short period of time. Therefore, it is important to detect and classify the malicious attacks in the network with the aim to secure the network from attacks that can affect the integrity and confidently of the system. Thus, different existing studies have used various AI algorithms for identification of attacks in the network, however, there are certain pitfalls such as low accuracy, has the ability to perform binary classification of attacks [**?**] which makes the model ineffective. These drawbacks primarily occur due to the implementation of ineffective algorithm. Therefore, in order to overcome these shortcomings, proposed model uses formed gate loop model and arrayized trigger unit function for identifying and classifying the attacks in the network. Figure.1 shows the overall mechanism of the proposed framework.

Figure 1. depicts the process of the proposed model, in which the process initiates by loading NSL-KDD dataset. Once the dataset is loaded, the data present in the dataset is pre-processed using different pre-processing techniques like Handling missing values, Feature scaling. Pre-processing helps with improving the reliability and quality of the data, thereby enhancing the quality of the model. After pre-processing, the data is splitted as train-test split, in which the training data is splitted as 80% and the testing data is splitted as 20%. After the process of train-test split, classification process takes place by employing proposed FGLM and ATUF in Bi-GRU model. In proposed FGLM, the input features obtained from the Reset gate is passed back to the update gate cyclically, in order to make sure that, important features obtained from the update gate is not lost Thus, proposed FGLM control the opening

Similarly, another study employed an effective data pre-and the closing operations of the gates, thereby improving the selectivity of when input data updates the memory. Once the data with important features is obtained using proposed FGLM, the data is passed to ATUF for reducing the dimen -sionality of data. In ATUF, the hidden state at each time step is denoted in matrix form and the subsequent matrix is composed of individual hidden state vectors. The ATUF is beneficial in obtaining better performance as it uses fewer parameters which leads to faster convergence and improved prediction performance. Therefore, proposed FGLM-ATUF helps with effective detection and multi-classification of attacks present in the network.

Fig. 1. Proposed Methodology

A. Dataset Overview

The KDDTrain+.txt and KDDTest+.txt files appear to con -tain network traffic data, with multiple features describing each network connection. The datasets include 43 columns, with the last column likely representing the class label (e.g., ”normal”or various types of network attacks).

The first five rows of the training data in ‘KDDTrain+.txt' reveal various network connections with diverse characteris -tics. For instance, the first row describes a UDP connection with the ”other” service type, an ”SF” flag, and several other attributes, classified as ”normal.” The second row represents a TCP connection using the ”private” service with an ”S0” flag, labeled as a ”neptune” attack. The third and tenth rows detail HTTP service TCP connections marked as ”normal,” while the fifth row describes another ”private”TCP connection with a”REJ” flag, also labeled as a ”neptune” attack.

Similarly, the first five rows of the test data in ‘KD -DTest+.txt‘ include a mix of normal and attack connections. The first row describes a TCP connection using the ”private”service with a ”REJ” flag, classified as a ” neptune” attack. The second row details an FTP data service connection labeled as ”normal.” The third row shows an ICMP connection with an ”eco i” service type, classified as a ”saint” attack. The tenth row describes a telnet service TCP connection labeled as ”mscan,” while the fifth row is an HTTP service TCP con-nection marked as ” normal.” These initial rows illustrate the diversity of the dataset, capturing various network behaviors essential for training effective intrusion detection models. These datasets provide a rich set of features for each network connection, essential for building and evaluating machine learning models for network intrusion detection. The features include various network attributes such as protocol type,service, flag, source and destination bytes, among others,with labels indicating whether the connection is normal or an attack type. This comprehensive data is crucial for training models to accurately classify and detect network intrusions.

B. Data Pre-processing

Pre-processing is the process of removing irrelevant and redundant data from the dataset. The dataset is pre-processed so as to check the presence of noisy, missing and other incon-sistencies present in the dataset, which can affect the reliability and accuracy of the model. Therefore, pre-processing is con-sidered as a significant step. The proposed model utilized two different Pre-processing techniques, which includes handling missing data and feature selection.

- Handling missing data – Handling of missing data is considered as a significant step in pre-processing. If the dataset comprises of missing data, it can stir unwanted problems for the model. Hence, handling of the missing data is crucial.
- Feature scaling – Feature scaling is primarily used for normalizing the range of independent variables or features of the data, in which is used for transforming the values of features or variables in a dataset to a similar scale.

C. Implemented Architecture

The model uses multiple layers of Bi-GRUs to capture temporal dependencies in the data. Data preparation of this model involves encoding categorical features using Label En-coder, scaling numerical features with Standard Scaler, and splitting the data into training and test sets with expanded feature dimensions to fit the model’s input requirements. The model definition includes an input shape of (1, num features),three Bidirectional GRU layers with 64 units each, dropout layers with a rate of 0.5 to prevent overfitting, and dense layers with 32 units and ReLU activation, followed by a final dense layer with num classes units and softmax activation for output. The model is compiled using the Adam optimizer with a learning rate of 0.001, sparse categorical cross entropy as the loss function,and accuracy as the evaluation metric. Training is conducted over 20 epochs with a batch size of 32, using a validation split of 0.2 and incorporating early stopping and model checkpoint callbacks to prevent overfitting and save the best model. Finally, the model’s performance is evaluated on the test set, and a classification report is generated to provide detailed metrics on its effectiveness.

VII. RESULTS AND ANALYSIS

Table I provides a comprehensive overview of the Bidirectional Gated Recurrent Unit (Bi-GRU)model’s performance across multiple classes during its training. The precision, recall, F1-score, and support metrics for each class offer valuable insights into how the model’s predictions align with the actual class

labels. This detailed breakdown allows for a nuanced understanding of the model's strengths and performance, learning efficiently and weaknesses in different classification scenarios.

Furthermore, the training and validation metrics, including loss and accuracy, offer a holistic view of the model's learning process. The training loss starting at 0.2967 and decreasing to 0.0732 indicates effective learning, while the improvement in training accuracy from 0.9264 to 0.9828 signifies enhanced predictive capability. Similarly, the validation metrics show a consistent trend, with the loss decreasing from 0.0905 to 0.0364 and the accuracy rising from 0.9627 to 0.9892. This stability in validation performance suggests that the model exhibits strong generalization, indicating its ability to perform well on unseen data.

The rapid reduction in loss and increase in accuracy demonstrate the model's swift convergence to high performance. Additionally, the minimal gap between the training and validation metrics indicates good generalization with minimal overfitting. It's noteworthy that the validation accuracy plateaus after the initial training epochs, implying that the model reaches its optimal learning capacity relatively early in the training process. This observation suggests that further training beyond this point may not significantly enhance the model's performance, highlighting the efficiency and effectiveness of the Bi-GRU model in this classification task.

Figure 2 visually depicts the learning progression and per-formance of the Bidirectional Gated Recurrent Unit (Bi-GRU)model over the course of its training. The plot showcases sepa-rate lines for training and validation loss and accuracy, offering a clear representation of the model's learning trends. With the left axis denoting loss values and the right axis representing accuracy values, the plot provides a comprehensive view of the model's performance. The training loss is illustrated by a blue line with circular markers, while the validation loss is depicted by an orange line with circular markers. Similarly, the training accuracy is represented by a green line with square markers, and the validation accuracy is denoted by a red line with square markers. The x-axis spans the epochs from 1 to 10,and the plot includes grid lines for improved readability, along with a combined legend in the upper left corner to differentiate between the various metrics.

The visualization clearly shows the decreasing trend of both training and validation loss, with the training loss decreasing more sharply initially and then leveling off. The training accu -racy increases steadily, while the validation accuracy reaches a high level early on and remains stable. The close alignment of the training and validation accuracy lines indicates that the model is not overfitting, as the performance on the validation set closely matches the performance on the training set. The stabilization of the validation accuracy after the fourth epoch suggests that the model has learned the essential patterns in the data and that additional training epochs do not provide significant further improvements. Overall, the Bi-GRU model exhibits excellent classification.

TABLE I
PRECISION, RECALL, F1-SCORE, AND SUPPORT FOR EACH CLASS

Class	Precision	Recall	F1-Score	Support
0	0.00	0.00	0.00	737
1	0.68	0.98	0.80	359
2	0.70	0.35	0.47	20
3	0.50	0.33	0.40	3
4	1.00	0.02	0.04	1231
5	0.00	0.00	0.00	133
6	0.00	0.00	0.00	1
7	0.76	0.98	0.85	141
8	1.00	1.00	1.00	7
9	0.00	0.00	0.00	2
10	0.00	0.00	0.00	293
11	0.00	0.00	0.00	996
12	1.00	0.06	0.11	18
13	0.00	0.00	0.00	17
14	0.91	1.00	0.95	4657
15	0.42	0.99	0.59	73
16	0.67	0.98	0.80	9711
17	0.08	0.50	0.13	2
18	0.33	0.50	0.40	2
19	0.71	0.88	0.78	41
20	0.19	0.97	0.32	157
21	0.00	0.00	0.00	685
22	0.00	0.00	0.00	15
23	0.00	0.00	0.00	13
24	0.00	0.00	0.00	319
25	0.53	0.63	0.57	735
26	0.00	0.00	0.00	14
27	1.00	0.98	0.99	665
28	0.00	0.00	0.00	178
29	0.00	0.00	0.00	331
30	0.00	0.00	0.00	0
31	0.00	0.00	0.00	2
32	0.24	1.00	0.39	12
33	0.00	0.00	0.00	2
34	0.00	0.00	0.00	0
35	1.00	0.01	0.03	944
36	0.00	0.00	0.00	2
37	0.00	0.00	0.00	9
38	0.00	0.00	0.00	4
39	0.00	0.00	0.00	13
Accuracy			0.71	22544
Macro Avg	0.29	0.30	0.24	22544
Weighted Avg	0.64	0.71	0.62	22544

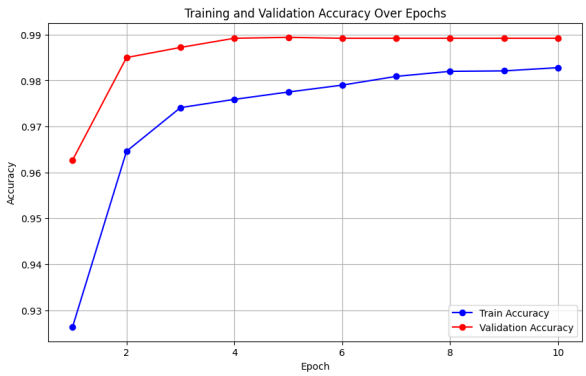

Fig. 2. Training and Validation Loss and Accuracy

maintaining high accu-racy without overfitting. The detailed trends in Figure 2 pro-vide a comprehensive view of the model's training dynamics and its ability to generalize well to unseen data.

VIII. CONCLUSION AND RECOMMENDATION

The integration of the Formed Gate Loop Model (FGLM) and Arrayized Trigger Unit Function (ATUF) within the Bidi -rectional Gated Recurrent Unit (Bi-GRU) framework has led to significant advancements in network intrusion detection. The results, as depicted in Figure **??**, demonstrate a substan-tial decrease in training loss from 0.2967 to 0.0732 and a corresponding increase in training accuracy from 0.9264 to 0.9828. Similarly, the validation loss decreases from 0.0905 to 0.0364, while the validation accuracy rises from 0.9627 to 0.9892 and stabilizes after the fourth epoch, indicating strong generalization capabilities of the model.

The close alignment of training and validation metrics, with minimal gaps, suggests that the model effectively learns the underlying patterns in the data without overfitting. The stabilization of validation accuracy after the fourth epoch implies that the model reaches its optimal learning capacity early, with further training yielding limited improvement. The proposed FGLM-ATUF approach enhances memory update selectivity, retains important features, and reduces data dimensionality, leading to faster convergence and improved prediction performance.

Overall, the Bi-GRU model demonstrates excellent classification performance, learning efficiently and maintaining high accuracy without overfitting. The detailed trends in Figure 2 offer a comprehensive view of the model 's training dynamics and its ability to generalize well to unseen data. This research contributes to the development of robust and effective network intrusion detection systems , essential for safeguarding modern networks from sophisticated attacks.

Based on these findings, several recommendations are suggested for future work and practical implementation, including expanded dataset utilization, real-time implementation, hybrid model development, advanced feature engineering techniques, adaptive learning mechanisms, and the development of a user-friendly interface for practical use by network administrators and security analysts. By following these recommendations, the proposed Bi-GRU model can be further enhanced and integrated into practical network security solutions, ensuring the protection of modern networks against increasingly sophisticated attacks.

REFERENCES

[1] Ahmad F Al Musawi, Satyaki Roy, and Preetam Ghosh. Examining indicators of complex network vulnerability across diverse attack scenarios. *Scientific Reports*, 13(1):18208, 2023.

[2] Jose Roldan-Gomez, Juan Boubeta-Puig, Javier Carrillo-Mondejar,´Juan Manuel Castelo Gomez,´ and Jesus´ Martınez´ del Rincon.´ An automatic complex event processing rules generation system for the recognition of real-time iot attack patterns. *Engineering Applications of Artificial Intelligence*, 123:106344, 2023.

[3] PLS Jayalaxmi, Rahul Saha, Gulshan Kumar, Mauro Conti, and Tai-Hoon Kim. Machine and deep learning solutions for intrusion detection and prevention in iots: A survey. *IEEE Access*, 10:121173–121192 ,2022.

[4] Tazin Sayyed, Siddharth Kodwani, Kiran Dodake, Milennium Adhayage, Ram Kumar Solanki, and Pawan R Bhaladhare Bhaladhare. Intrusion detection system. *Int. J. of Aquatic Science*, 14(1):288–298, 2023.

[5] Tao Yi, Xingshu Chen, Yi Zhu, Weijing Ge, and Zhenhui Han. Review on the application of deep learning in network attack detection. *Journal of Network and Computer Applications*, 212:103580, 2023.

[6] Amiya Kumar Sahu, Suraj Sharma, Mohammad Tanveer, and Rohit Raja. Internet of things attack detection using hybrid deep learning model. *Computer Communications*, 176:146–154, 2021.

[7] Daniyal Alghazzawi, Omaimah Bamasag, Hayat Ullah, and Muhammad Zubair Asghar. Efficient detection of ddos attacks using a hybrid deep learning model with improved feature selection. *Applied Sciences*, 11(24):11634, 2021.

[8] Faheem Masoodi et al. Machine learning for classification analysis of intrusion detection on nsl-kdd dataset. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10):2286–2293, 2021.

[9] Ananya Devarakonda, Nilesh Sharma, Prita Saha, and S Ramya. Network intrusion detection: A comparative study of four classifiers using the nsl-kdd and kdd'99 datasets. In *Journal of Physics: Conference Series*, volume 2161, page 012043. IOP Publishing, 2022.

[10] Shubair A Abdullah and Ahmed Al-Ashoor. An artificial deep neural network for the binary classification of network traffic. *International Journal of Advanced Computer Science and Applications*, 11(1):402–408, 2020.

[11] Tongtong Su, Huazhi Sun, Jinqi Zhu, Sheng Wang, and Yabo Li. Bat: Deep learning methods on network intrusion detection using nsl-kdd dataset. *IEEE Access*, 8:29575–29585, 2020.

[12] Muhammad Naveed, Fahim Arif, Syed Muhammad Usman, Aamir Anwar, Myriam Hadjouni, Hela Elmannai, Saddam Hussain, Syed Sajid Ullah, and Fazlullah Umar. A deep learning-based framework for feature extraction and classification of intrusion detection in networks. *Wireless Communications and Mobile Computing*, 2022(1):2215852, 2022.

[13] Muhammad Basit Umair, Zeshan Iqbal, Muhammad Ahmad Faraz, Muhammad Attique Khan, Yu-Dong Zhang, Navid Razmjooy, and Sefedine Kadry. A network intrusion detection system using hybrid multilayer deep learning model. *Big data*, 2022.

[14] Rochak Swami, Mayank Dave, and Virender Ranga. Voting- based intrusion detection framework for securing software-defined networks. *Concurrency and computation: practice and experience*, 32(24):e5927 ,2020.

[15] Andrew McCarthy, Essam Ghadafi, Panagiotis Andriotis, and Phil Legg. Defending against adversarial machine learning attacks using hierarchical learning: A case study on network traffic attack classification. *Journal of Information Security and Applications*, 72:103398, 2023.