VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model

Ghayth ALMahadin, Yassine Aoudni, Mohammad Shabaz, Anurag Vijay Agrawal, Ghazaala Yasmin, *Member, IEEE*, Esraa Saleh Alomari, Hamza Mohammed Ridha Al-Khafaji, *Senior Member, IEEE*, Debabrata Dansana, and Renato Racelis Maaliw, III, *Senior Member, IEEE*

***Abstract*—The rise of Vehicular Ad-hoc Networks (VANETs) has led to the growing significance in intelligent transportation systems. This research suggests a deep learning model for anomaly detection based on GRU over VANET network traffic to address this challenge. Consumer electronics technologies can be successfully introduced to the market in one of two ways: either there is a clear benefit for the customer from using this technology, or it is required by a regulatory order that prevents the use of alternatives. It is possible to detect unknown assaults and DoS floods using traffic anomalies. Users can keep track of the security features of multimedia services by using Traffic Anomaly Detection, which provides an overview of traffic anomaly detection analysis. Anomaly detection methods fall into three categories: unsupervised, semi-supervised, and supervised. The right anomaly detection technique basically depends on the labels that are present in the dataset. To further improve the accuracy of proposed model, a new semi-supervised technique for detecting VANET network activity anomalies called SEMI-GRU has been proposed. The results demonstrate that proposed GRU-based deep learning model outperforms existing methods in detecting network anomalies with low false positive rates.**

***Index Terms*—Anomaly detection, intrusion detection system, deep learning, GRU, network traffic, classification.**

Manuscript received 26 May 2023; revised 14 July 2023, 10 August 2023, and 11 October 2023; accepted 16 October 2023. Date of publication 20 October 2023; date of current version 26 April 2024. *(Corresponding author: Mohammad Shabaz.)*

Ghayth ALMahadin is with the Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Amman 19328, Jordan (e-mail: g.mahadin@ammanu.edu.jo).

Yassine Aoudni is with the Computer and Embedded Systems Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3038, Tunisia (e-mail: yassine.aoudni@enis.tn).

Mohammad Shabaz is with the Department of Computer Science and Engineering, Model Institute of Engineering and Technology Jammu, Jammu 180001, India (e-mail: bhatsab4@gmail.com).

Anurag Vijay Agrawal is with the Electronics and ICT Academy, Department of Electronics and Communication Engineering, Indian Institute of Technology Roorkee, Roorkee 247667, India (e-mail: aagrawal3@ec.iitr.ac.in).

Ghazaala Yasmin is with the School of Computer Science Engineering and Technology, Bennett University, Greater Noida 201310, India (e-mail: ghazaala.yasmin@gmail.com).

Esraa Saleh Alomari is with the College of Education for Pure Sciences, Wasit University, Al-Kut 52001, Iraq (e-mail: ealomari@uowasit.edu.iq).

Hamza Mohammed Ridha Al-Khafaji is with the Biomedical Engineering Department, College of Engineering and Technologies, Al-Mustaqbal University, Hillah 51001, Iraq (e-mail: hamza.alkhafaji@uomus.edu.iq).

Debabrata Dansana is with the Department of Computer Science, Rajendra University, Balangir 767001, India (e-mail: debabratadansana07@gmail.com).

Renato Racelis Maaliw, III is with the College of Engineering, Southern Luzon State University, Lucban 4328, Philippines (e-mail: rmaaliw@slsu.edu.ph).

Digital Object Identifier 10.1109/TCE.2023.3326384

I. Introduction

With the growing integration of networked systems in cyber-physical transportation systems, cyber threats are becoming more sophisticated and frequent. Cyber risks are evolving and multiplying as networked technologies are being increasingly integrated into cyber-physical transportation networks. Through anomaly detection over network traffic, which entails spotting out-of-the-ordinary patterns or behaviours that depart from typical VANET network activity, it is possible to spot potential threats. Anomaly detection can be done using various techniques, including statistical analysis. Statistical methods are often used to detect anomalies in network traffic [1]. Research on network anomaly detection has been focused on business situations. The attack surface for consumer networks has been growing quickly as there are more Internet of Things (IoT) devices in the digital world. For attacks like Distributed Denial of Services (DDoS), the majority of the hacked machines are turned into zombies. Contrary to the majority of business networks, consumer networks lack the management switches and firewalls needed to quickly monitor and stop unwanted network traffic. Numerous attacks that do not affect consumer networks are directed at commercial networks. Hackers frequently employ well-known cyber-attacks such as viruses, drive-by downloads, phishing, and password attacks. DDoS (or denial of service). A DDoS attack usually uses many computers or numerous hosts that have been infected with virus.

Consumers will ultimately pay for service cost increases through increased retail service prices in the market. For merchants who offer high levels of customer service and awareness, their pricing advantage is apparent. Consumers may always be served by providers at a hefty cost. In a consumer network, there are no monitored devices or networks that are handled. Aware of privacy issues, no There are not any customers network information acquired or released. These techniques involve calculating statistical measures such as mean, variance, and standard deviation to identify patterns that deviate from normal behaviour. Statistical methods work well for detecting simple anomalies, but they may not be effective for complex VANET network traffic patterns [2]. Machine learning algorithms can be used for anomaly detection over network traffic. These algorithms use statistical models to identify patterns in VANET network traffic data and can

learn from historical data to improve accuracy. Networked systems are becoming more and more integrated with cyber-physical transportation systems. In addition, machine learning algorithms can be supervised or unsupervised, which is more effective for anomaly detection as it can identify unknown patterns in the data. However, deep learning approaches require significant computational resources and may not be suitable for all environments [3].

Anomaly detection over Cyber-Physical Transportation Systems (CPTS) faces several challenges, including real-time detection, From the perspectives of improved production, dynamic reconfiguration, standardization, and information technological advances, the difficulties facing CPTS in terms of production can be seen. Also, false positives and negatives can occur, leading to misidentifying regular traffic as anomalous or vice versa [4]. Deep learning models can detect known and unknown anomalies, making them a powerful tool for anomaly-based Intrusion Detection Systems (IDS) in CPTS. Anomalies can also be found using various data visualization and exploratory data analysis approaches. Deep learning models are an effective tool for anomaly-based Intrusion Detection Systems (IDS) in CPTS because they can identify both known and unidentified abnormalities. However, deep learning approaches require significant computational resources and may not be suitable for all environments. In addition, anomaly-based IDS faces several challenges, including the need for real-time detection, the complexity of VANET network traffic patterns, and the availability of labeled data for training machine learning models [5]. Also, false positives and negatives can occur, leading to misidentifying normal traffic as anomalous or vice versa.

A family of neural networks with deep connections called convolutional neural networks (CNNs, often referred to as Conv Nets) is frequently used in deep learning to evaluate the perception of images. An artificial neural network that has connections between its nodes is called a recurrent neural network (RNN). that form a engaged chart along a temporal classification. Deep learning methods are now used in various domains, such as medicine, target identification, and natural language processing [6]. Most studies [7] that use the RNN scheme employ the\(LSTM) network, which is more complex, has more parameters, and takes longer to generate than the Gated Recurrent Unit (GRU) network. LSTM predicts the future based on what has happened in the past and what is happening now. Because it depends on long-term memory, it is a common way to find strange behavior [8].

There are no loops connecting any of the nodes in forward feeding networks, a type of neural network made up of neurons. Since all information is only delivered in the same direction, this type of network of neurons is also known as a multi-layer neural network. The feed-forward neural network (FNN) and MixMatch [9] are used to improve the multi-layer bidirectional GRU neural network (MLB-GRU). This network is made by setting the basic GRU neural network to multi-layer (multi-layer) and bidirectional. In the method suggested in this piece, the SMOTE algorithm [10] is first used to improve the data in the training samples. To change the size of the MLB-GRU output vector. Finally, in the supervised learning model Mix Match, a semi-supervised loss item is added to the total loss function. Authentication, integrity, and nonrepudiation should be the three main components of VANET security.

Accuracy in detecting VANET network traffic anomalies could be increased, and the number of false positives has not been brought down to a level that is reasonable. It remains challenging to precisely pinpoint an unidentified assault. This research seeks to use the enhanced GRU neural network [11] to identify unknown attacks, detect abnormal traffic, and improve abnormal traffic detection accuracy. This study suggests a technique for detecting VANET network traffic anomalies that is semi-supervised and is based on a gated recurrent unit neural network (GRU) [12]. This technique can be applied to cyber-physical transportation systems to the resilience and precision of anomaly detection in network traffic should be increased. Existing mechanisms for detecting unknown network attacks using Intrusion Detection Systems (IDS) face significant challenges. Although deep learning techniques have been applied to VANET network traffic anomaly detection [13], they tend to have high false positive rates, and supervised learning dominates model training [14]. The MLB-GRU and an improved feed-forward neural network (FNN) with data oversampling and semi-supervised learning to achieve better accuracy and lower false positive rates in VANET network traffic anomaly detection. A variety of VANET issues, such as misbehavior awareness, broadcast storm avoidance, and driver behavior prediction, may be solved using a naive Bayesian approach [15]. The capability of RNN to identify resource availability patterns based on frequency band utilization time makes it potentially useful as a tool for resources preservation [16]. They are a good choice for separating between regular traffic and network assaults due to their capacity for learning complicated patterns and behaviors [17]. The Internet of Things (IoT) is a vital tool for completing the loop in cyber-physical systems, giving each monitored or controlled physical asset “smartness” and hence more value [18].

The gated recurrent unit network is used in VANET network traffic in cyber-physical transportation systems. As there are more Internet of Things (IoT) devices in the digital world, the potential for attack for customer networks has been expanding swiftly. Most of the devices were abused for attacks like Distributed Denial of Services (DDoS) are turned into zombies. Because they are not attractive prospects for cybercriminals, consumer networks are not typically the target of DDoS attacks. However, since they will be transmitting many more packets to the same IP or Port than usual, customer networking equipment functioning as zombies for a DDoS attack can be identified. GRU provides benefits over long short-term memory (LSTM) in several circumstances. For ensuring the security and reliability of cyber-physical transportation systems, deep learning models’ potential to enhance anomaly detection in VANET network traffic using semi-supervised learning and oversampling methodologies is essential. The importance of intelligent transport systems is expanding as a result of the development. The performance and security of the VANET network depend on the ability to spot abnormalities in network traffic. The proposed method uses data oversampling and applies semi-supervised learning

to improve anomaly detection accuracy in network traffic. The paper evaluates the suggested algorithm's efficacy on binary and multi-classification tasks using the NSL-KDD dataset and evaluates the outcomes against those of other approaches already in use. Finally, the paper aims to demonstrate the effectiveness of the proposed GRU-based deep learning model for anomaly detection in network traffic and its potential applications in cyber-physical transportation systems. The paper is organized into 4 sections, initially, Section I provides Introduction section, and Section II covers Research Method; Section III presents Experimental Results; Section IV presents Conclusion.

II. Research Methods

Network traffic has dramatically increased as a result of the growing number of devices connected to the network, making the detection of anomalies in VANET network traffic more important for ensuring the security of cyber-physical transportation systems. However, traditional methods of detecting network anomalies often rely on rule-based systems that can be time-consuming to configure and maintain and may struggle to identify novel or unknown threats. Three sorts of dangers may be distinguished: natural threats, technical threats, and risks brought on by people. Threats are often divided into three groups: those generated by nature, technology, or people. The VANET topics that have been investigated over the past ten years include applications, routing, security/privacy, and mobility management. Recurrent neural networks (RNNs) have the advantage of having memory-like properties.

To address these issues, this paper proposes a GRU-based deep learning model for detecting anomalies in VANET network traffic. Unlike traditional RNNs, GRU merges the input gate and forget gate into a single "update gate" and continuously sends the output result backwards as a memory state, improving access to the network's input and output.

A. SEMI-GRU Method

Based on the GRU model, this paper regards the number of layers and directions of the GRU as parameters that can be adjusted, so the formed MLB-GRU model has more vital expressive ability than the GRU model. First, the input data is converted into binary features. Then the minority class sample is oversampled using the SMOTE method. Then the MLB-GRU and the proposed symmetrical reduction FNN network structure (SR-FNN) are used for feature extraction. Finally, the simplified version of the proposed MixMatch scheme is used to extract the overall loss. As seen in Fig. 1, the suggested SEMI-GRU approach is divided into three primary components: MLBGRU, SR-FNN, and a condensed MixMatch scheme. The three primary phases of SEMI-GRU are data preparation, training, and testing. Each sample will take up 361 bytes of memory after the data preparation is finished, which is done in the training step. To keep the processed data stored we split the input vector corresponding to each piece of data into 19-time steps for the input GRU neural network, with a 19-input size for each time step. To get the crossover,

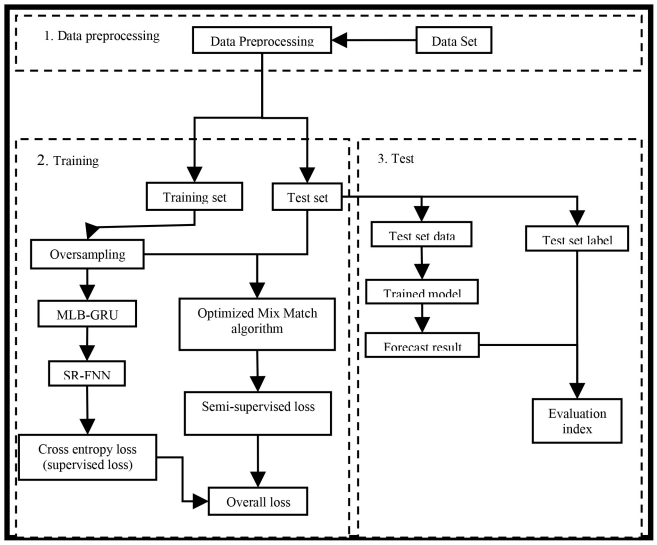


Fig. 1. Structure of the SEMI_GRU method.

the training set that SMOTE oversampled is fed into the model during the training phase. Loss of entropy.

B. Data Preprocessing

This study uses NSL-KDD dataset [19] for testing intrusion detection systems (IDS) in network security. In data preprocessing converts the original data set into numerical data processed by the neural network. For the RNN network, the dimension of the input data is [num_steps, input_dim], where num_steps represent the number of loop inputs, and in-put_dim represents the dimension of the input vector. The NSL-KDD dataset contains three discrete features: protocol_type, service and flag. The NSL-KDD dataset contains 42 features. After mapping the discrete features to continuous natural numbers, all fields in the dataset are converted to numeric types: Int64 and Float64; each value occupies 8 bytes. Therefore, the 42 fields of each sample in the NSL-KDD dataset will occupy 336 (42*8) bytes of memory,

C. Sample Oversampling

A category imbalance in the training set prevents the model from learning the category's traits from the category with few samples. Sample oversampling is unnecessary because the deep neural network prefers to learn from more parts. If affecting others, expand the minority class sample size. Unsupervised auto-encoder networks, generative encounter networks, and flip transformations oversample. These methods have unfavorable results. Random oversampling begins with minority class samples and adds tested samples to the data set. This method is primary but easily overfits. SMOTE improves random oversampling. It creates new models by interpolating minority class samples. Algorithm flow:

(1) For each minority class sample, compute its Euclidean distance to all models in the sample set and find its k-nearest neighbours.

(2) Use the sample imbalance ratio to calculate the sampling amplification N. Select several samples from each minority

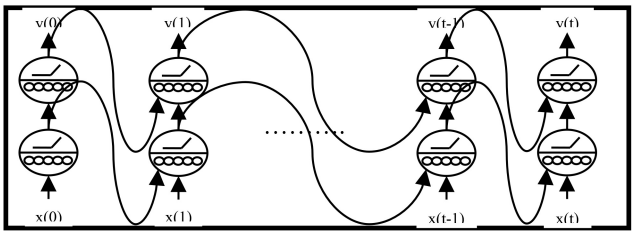


Fig. 2. Multi-layer GRU neural network.

class sample x's k closest neighbours, assuming the neighbour is o.

(3) Calculate formula (1) with the original sample for each randomly chosen neighbour o to create a new model.

$$x_{\text{new}} = o + \text{rand}(0, 1) * |o - x_{\text{n}}| \tag{1}$$

The R2L attack category contains 995 samples, and the U2R attack category includes 52. Compared with other attack categories, the attack samples are fewer. This paper uses the SMOTE algorithm to analyze These two attack categories that are processed; the oversampling of R2L attack samples is ten times the original, and the oversampling of U2R attack samples is 100 times the original.

D. Multilayer Bidirectional GRU Model (MLB-GRU)

The advantage of GRU over LSTM is that it can capture long-term dependencies with fewer parameters, and the training speed of the model is faster.

Fig. 2 is a schematic diagram of a multilayer GRU neural network. Here, the input time step is carried out from left to right. The figure shows a one-way input, but the information can be two-way; the input vector follows the direction from right to left—sequential input. Without loss of generality, the number of layers of the GRU shown in the figure is 2, and the number of layers can be adjusted during the actual training process.

$$\begin{cases} z_t = \sigma\left(W_z.\left[y_{t-1},\ x_t\right]\right) \\ r_t = \sigma\left(W_r.\left[y_{t-1},\ x_t\right]\right) \\ \widetilde{y}_t = \sigma\left(W.\left[r_t * y_{t-1},\ x_t\right]\right) \\ y_t = (1 - z_t) * y_{t-1} + z_t * \widetilde{y}_t \end{cases} \tag{2}$$

The yt of all time steps are spliced together to form the output vector. Since it is a bidirectional GRU neural network, assuming that the forward output vector is $\overrightarrow{output}$, and the reverse output vector is $\overleftarrow{output}$, then the final output vector, Such as formula (3)

$$\text{output} = \text{concat}\left(\overrightarrow{output}, \overleftarrow{output}\right). \tag{3}$$

E. Symmetrically Reduced FNN Network Structure

In this paper, according to its structural characteristics, a feed-forward neural network structure is designed, named Symmetrical Reduction Feed Forward Neural Network (SR-FNN). Inside the network, the parameters are unidirectionally propagated through. Different from the cyclic neural network, it does not form a directed ring inside, and the output vector of the upper layer GRU network model can be input into the

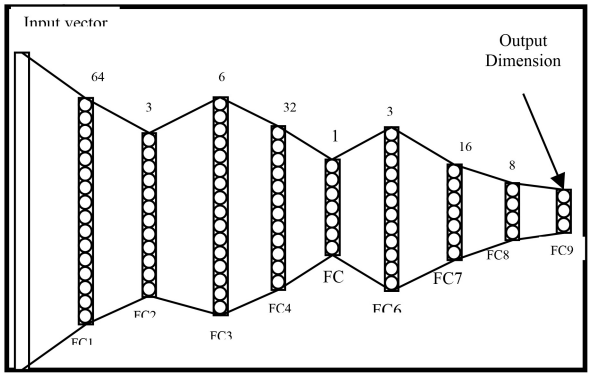


Fig. 3. SR-FNN network structures.

structure to adjust the dimension of the output vector. The network structure of FNN is shown in Fig. 3.

It can be seen from Fig. 3 that the proposed FNN network structure contains a total of 9 fully connected layers, in which the input vector comes from the output of the upper GRU neural network. The FNN structure includes three networks spliced together by three fully connected layers. The first group of network structures includes FC1, FC2 and FC3; the second group comprises FC4, FC5 and FC6; and the third group includes FC7, FC8 and FC9. Among them, the output dimensions of FC1 and FC3 in the first group of network structures are the same. The output dimensions of FC4 and FC6 in the second group are the same, and the output dimensions of FC7, FC8 and FC9 in the third group are decreasing. The output dimension of the last fully connected layer, FC9, in the third group of network structures is set as the VANET network traffic category. The output dimensions of the first group and the second group of network structures are first reduced to half of the original size and then restored to the previous size. Experiments show that the design of this dimension is reduced first and then converted to Improved model performance.

F. Semi-Supervised Training

An emerging paradigm in the advancement of machine intelligence is semi-supervised learning. A type of machine learning known as semi-supervised machine learning creates models utilizing both a significant amount of unlabeled data and a small amount of tagged data. Semi-supervised learning can learn with a large amount of unlabeled data and a minimal amount of labelled data—the MixMatch method proposed by Berthelot et al. The prediction accuracy approaches supervised learning. The MixMatch process integrates the advantages of various semi-supervised methods, such as supporting self-consistent regularization, minimizing the entropy of unlabeled data, using Weight decay instead of L2 regularization, and using Mixup—This method of data augmentation.

Based on the MixMatch method, we propose a simplified version of the MixMatch process, which adds a semi-supervised loss item to the overall loss function to improve the generalization ability and effect of the model. In the original MixMatch scheme, a training batch (Batch) The marked data

x of the collection and the unmarked data u of a set are augmented, and the increased data x′ of 1 batch and u′ of K batches are respectively obtained. In this paper, the Batch of marked data The Batch of the unmarked data is set equal to that of the unmarked data so that after the unmarked data augmentation operation is completed, it is unnecessary to divide it into K parts on average. The specific process is shown in Algorithm 1. As is easily observed in Algorithm 1, the labelled training data and unlabeled test data are merged and fed into the deep neural network in the presented simplified MixMatch method. The acquired semi-supervised loss item will be returned at the conclusion of the method, allowing the semi-supervised loss and the supervised loss to be optimised jointly, improving the model's capacity to generalise and its impact.

G. Algorithm 1 Optimized MixMatch Algorithm

Input: x,y,u
Output: loss

1. for (x_b, y_b) in (x, y) do
2. p_b = One-hot(y_b)
3. u_b=next(u)
4. $\overline{q}_b$ = model(y|u_b;θ)
5. q_b= (softmax($\overline{q}_b$)^2) / (sum(softmax($\overline{q}_b$)^2)
6. inputs=concatenate(x_b,u_b)
7. m_inputs = MixUp(inputs, shuffle(inputs))
8. targets=concatenate(p_b,q_b)
9. m_targets=MixUp(targets,shuffle(targets))
10. logits_x=model
11. (y|m_inputs[0])
12. logits_u=model
13. (y|m_inputs[1])
14. $loss_1$=-m_targets[0]∗log(softmax(logits_x))
15. $loss_2$=MSE(logits_u,m_targets[1])
16. loss=$loss_2$+$loss_2$
17. return loss
18. End for.

III. Experimental Results

The software environment used in the experiment is Ubuntu18.04 operating system, Pytorch1.9.1 and Cuda9.0. For usage with graphics processing units (GPUs) in general computer science, NVIDIA developed a distributed computation framework and coding language known as CUDA®. With CUDA, programmers may drastically speed up computational programs by utilizing GPU characteristics. In deep learning, Accuracy rate, precision rate, recall rate, and F1-Score are frequently used to measure performance. This experiment will use these indicators to evaluate the SEMI-GRU method. Computer simulation is the technique of simulating another system's behavior using technology such as computers to reflect a first system's dynamic response. In a simulation, which means that computer software is used to simulate or represent a real system mathematically. An algorithm or computer program that predicts the evolution of a modelled system in response to input signals is known as a computer simulation model.

TABLE I
Performance Evaluation of SEMI-GRU Method

Model	Accuracy	Precision	Recall	F-Measure	False alarm
4-Layer	82.75	91.62	72.07	80.68	3.14
5-Layer	83.79	91.18	73.99	81.69	3.25
6-Layer	83.73	90.16	73.96	81.26	3.36
7-Layer	83.08	91.36	73.05	81.18	3.67
8-Layer	83.31	93.80	73.08	82.15	3.15

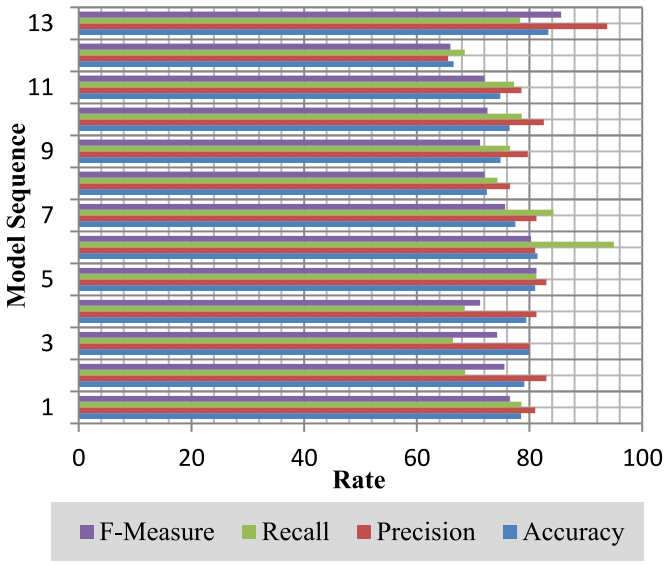


Fig. 4. Performance evaluation of SEMI-GRU Method.

This paper conducts model training and evaluation on the NSL-KDD dataset. It has five-category and two-category research will be carried out. The five-category will be refined into four attack categories, and the two-category will be divided into four.

A. Results Analysis

This study examined and evaluated the performance of the SEMI-GRU approach employing different GRU layers on the NSL-KDD dataset using the five performance comparison categories indicated in Table I. Layers of the GRU model were built, and trials were carried out separately. Layers of the GRU model were built, and trials were carried out separately. The results of the experiment demonstrated that the NSL-KDD dataset was outperformed by the 5-layer and 8-layer GRU models. Ongoing research is required to increase the precision and potency of anomaly detection systems in real-world scenarios. Experiment findings showed that the 5-layer and 8-layer GRU models outperformed the NSL-KDD dataset. The 5-layer GRU model had the best accuracy rate of 83.79% among the comparison methods. However, in the deepest layer, the false alarm rate fell to 3.15%, which was not significantly different from the 3.14% false alarm rate in the 4-layer GRU model, as shown in Fig. 4.

Table II lists the five-category performance comparison between the SEMI-GRU and other methods on the NSL-KDD dataset. It can be seen from the table that, except for the

TABLE II
COMPARISON OF SEMI-GRU METHOD WITH RECENT WORK

S. no.	Model	Accuracy	Precision	Recall	F-Measure
1.	AlertNet[20]	78.5	81	78.56	76.52
2.	DNN[21]	79.1	83	68.56	75.58
3.	ANN[22]	79.9	80	66.41	74.25
4.	CNN[23]	79.4	81.25	68.52	71.26
5.	MCNN[24]	81	83	81.26	81.23
6.	MCNN-DFS[25]	81.4	81	95	80.25
7.	MDNN	77.5	81.25	84.23	75.65
8.	Naïve Bayes	72.45	76.53	74.28	72.06
9.	J48	74.9	79.68	76.54	71.25
10.	Random Forest	76.45	82.56	78.64	72.56
11.	Bagging	74.84	78.56	77.25	72.06
12.	Ada-boost	66.5	65.56	68.53	65.96
13.	**SEMI-GRU**	**83.32**	**93.8**	**78.36**	**85.62**

TABLE III
COMPARISON OF BINARY CLASSIFICATION PERFORMANCE OF SEMI-GRU METHOD

Model	Accuracy	Precision	Recall	F-Measure	False alarm rate
5 Layers, Batch128	88.13	97.05	81.63	88.67	3.27
5 Layers, Batch512	92.18	93.74	92.43	93.08	8.16
6 Layers, Batch512	90.89	96.80	86.88	91.57	3.80

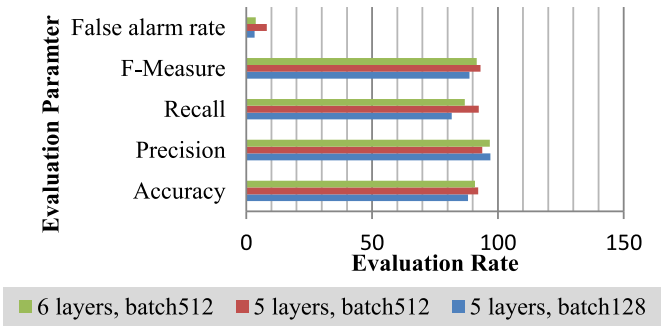


Fig. 5. Comparison of binary classification performance of SEMI-GRU Method.

single index of recall rate, the method proposed in this paper can achieve the highest accuracy rate among all comparison methods. (83.31%), the highest precision rate (93.80%) and F value (82.15%). This shows that SEMI-GRU has a good effect on the five classifications of the NSL-KDD dataset.

A performance evaluation of the SEMI-GRU method's GRU layers and batch sizes for binary categorization of the NSL-KDD dataset is shown in Table III. In the exercise, two GRU networks with 5 and 6 layers and 128 and 512 batch sizes were created. To assess their impacts on the performance of the model, the batch size and layer count were combined. According to the testing findings, the same 5-layer GRU network performed better with 512 batches than with 128. Additionally, when the batch size was 512, specific trends in the effects of the 5-layer and 6-layer GRU models could be seen. In particular, the 5-layer GRU model outperformed the 6-layer GRU model in terms of accuracy rate, recall rate, and F value, but it also had a greater false alarm rate. We can therefore draw the conclusion that improved model performance will lead to a more reliable ability to detect anomalous traffic. At the same time, though, it might also result in a greater chance of routine traffic being mistaken for abnormal. According to the experimental findings depicted in Fig. 5, the 6-layer GRU model may be more efficient at spotting abnormal traffic while minimizing false alerts, despite the accuracy rate, recall rate, and F value of the 5-layer GRU model being slightly higher.

IV. CONCLUSION

Detecting VANET network traffic abnormalities is necessary for locating cyber threats. Statistical techniques, Technologies for machine learning and deep learning can all be applied to identify anomalies, each with their own benefits and drawbacks. Deep learning models are an effective tool for anomaly-based intrusion detection systems because they can identify both known and unidentified abnormalities. However, they require a lot of processing power and might not work in all circumstances. The market can be effectively introduced to consumer electronics technologies in one of two ways: either there is an obvious advantage for the customer in utilising this technology, or it is required by a regulatory order that forbids the use of alternatives. Consumers will ultimately pay for rising service costs through higher market prices for retail services. Providers may always charge consumers a high price for their services. Real-time detection, the intricacy of VANET network traffic patterns, and the accessibility of labeled data are issues with anomaly-based IDS. To increase the efficacy and precision of identifying anomalies systems in practical situations, ongoing study is necessary. Enhancing the effectiveness of deep learning models is also essential in light of the category imbalances in datasets used for anomaly detection. In this paper, the SEMI-GRU method for detecting VANET network traffic anomalies is suggested. When compared to the technique of comparing various data sets, it has the most comprehensive effect and a low false-positive rate. It is also relevant to actual network traffic. Identify systemic traffic abnormalities. SEMI-GRU can use data from throughout instruction, both the training set and the test set. It has a low false alarm rate, effective feature extraction from the source data, and efficient data preprocessing capabilities. In the following step, SEMI-GRU will continue to be improved. To reduce the original data's dimensionality, we will use unsupervised learning. This will improve SEMI-GRU performance by lowering the interference from irrelevant data characteristics during training.

REFERENCES

[1] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learning system to intrusion detection," *Big Data Mining Anal.*, vol. 3, no. 3, pp. 181–195, Sep. 2020, doi: 10.26599/BDMA.2020.9020003.

[2] W. Wang et al., "Anomaly detection of industrial control systems based on transfer learning," *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 821–832, Dec. 2021, doi: 10.26599/TST.2020.9010041.

[3] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 68–71, Jun. 2019, doi: 10.1109/LNET.2019.2901792.

[4] A. Oseni et al., "An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 1000–1014, Jan. 2023, doi: 10.1109/TITS.2022.3188671.

[5] J. F. Cañola Garcia and G. E. T. Blandon, "A deep learning-based intrusion detection and preventation system for detecting and preventing denial-of-service attacks," *IEEE Access*, vol. 10, pp. 83043–83060, 2022, doi: 10.1109/ACCESS.2022.3196642.

[6] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[7] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, doi: 10.1109/TII.2020.3023430.

[8] D. Kaur, A. Anwar, I. Kamwa, S. Islam, S. M. Muyeen, and N. Hosseinzadeh, "A Bayesian deep learning approach with convolutional feature engineering to discriminate cyber-physical intrusions in smart grid systems," *IEEE Access*, vol. 11, pp. 18910–18920, 2023, doi: 10.1109/ACCESS.2023.3247947.

[9] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep generative learning models for cloud intrusion detection systems," *IEEE Trans. Cybern.*, vol. 53, no. 1, pp. 565–577, Jan. 2023, doi: 10.1109/TCYB.2022.3163811.

[10] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, "Federated intrusion detection in blockchain-based smart transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2523–2537, Mar. 2022, doi: 10.1109/TITS.2021.3119968.

[11] K. Wang, A. Zhang, H. Sun, and B. Wang, "Analysis of recent deep-learning-based intrusion detection methods for in-vehicle network," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 1843–1854, Feb. 2023, doi: 10.1109/TITS.2022.3222486.

[12] Z. Wang, X. Xie, L. Chen, S. Song, and Z. Wang, "Intrusion Detection and network information security based on deep learning algorithm in urban rail transit management system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2135–2143, Feb. 2023, doi: 10.1109/TITS.2021.3127681.

[13] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecurity: A review," *IEEE Access*, vol. 10, pp. 19572–19585, 2022, doi: 10.1109/ACCESS.2022.3151248.

[14] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[15] X. Guo, Y. Chen, L. Cao, D. Zhang, and Y. Jiang, "A receiver-forwarding decision scheme based on Bayesian for NDN-VANET," *China Commun.*, vol. 17, no. 8, pp. 106–120, 2020.

[16] N. Bahra and S. Pierre, "RNN-based user trajectory prediction using a preprocessed dataset," in *Proc. 16th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)(50308)*, Oct. 2020, pp. 1–6.

[17] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," 2018, *arXiv:1802.09089*.

[18] G. Bovenzi, G. Aceto, D. Ciuonzo, A. Montieri, V. Persico, and A. Pescapé, "Network anomaly detection methods in IoT environments via deep learning: A fair comparison of performance and robustness," *Comput. Security*, vol. 128, May 2023, Art. no. 103167.

[19] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine," *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1634–1646, Jul./Sep. 2022.

[20] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4507–4518, Jul. 2021.

[21] H. Lundberg et al., "Experimental analysis of trustworthy in-vehicle intrusion detection system using explainable artificial intelligence (XAI)," *IEEE Access*, vol. 10, pp. 102831–102841, 2022, doi: 10.1109/ACCESS.2022.3208573.

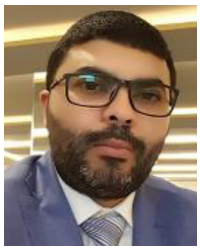
[22] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021, doi: 10.1109/JIOT.2020.2996590.

[23] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018, doi: 10.1109/ACCESS.2017.2782159.

[24] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "A novel two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[25] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021.

Ghayth ALMahadin is currently working with the Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Jordan. He is a conscientious, highly innovative, creative, and self-motivated researcher in machine learning/computational intelligence.



Yassine Aoudni is currently working with the Computer and Embedded Systems Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax, Tunisia. His area of interest includes embedded systems, image segmentation, biometrics, and image processing.

Mohammad Shabaz is working as an Assistant Professor with the Model Institute of Engineering and Technology, Jammu, India. He has published over 100+ research papers in various journals indexed in scopus/Web of science, five Indian patents, and three Australian patents. His area of interest is application of computer science in interdisciplinary domains.

Anurag Vijay Agrawal is currently working with the Electronics and ICT Academy, Department of Electronics and Communication Engineering, Indian Institute of Technology Roorkee, Roorkee, India. His current research interests include MIMO/massive MIMO communications, digital predistortion, and high-speed train communications.

Ghazaala Yasmin (Member, IEEE) is currently working with the School of Computer Science Engineering and Technology, Bennett University, Greater Noida. Her area of interest includes machine learning, data mining, NLP, and deep learning.

Esraa Saleh Alomari is currently working with the College of Education for Pure Sciences, Wasit University, Al-Kut, Iraq. Her area of interest includes network security, communication networks, and communication science.

Hamza Mohammed Ridha Al-Khafaji (Senior Member, IEEE) has been a Faculty Member with the Biomedical Engineering Department, College of Engineering and Technologies, Al-Mustaqbal University, Hillah, Iraq, since September 2015. He has published more than 80 articles, mainly on optical fiber communication systems, next-generation wireless networks, Internet of Things, and optimization algorithms.

Debabrata Dansana is currently working with the Department of Computer Science, Rajendra University, Balangir, India. His area of interest includes cognitive radio ad-hoc networks, machine learning, artificial intelligence, and IoT.

Renato Racelis Maaliw, III (Senior Member, IEEE) is an Associate Professor with the College of Engineering, Southern Luzon State University, Lucban, Philippines. His area of interest is in computer engineering, Web technologies, software engineering, data mining, machine learning, and analytics.