FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 2, January, 2026, pp 38 – 44
DOI: https://doi.org/10.33003/fjs-2026-1002-4351

ENHANCED GATED RECURRENT UNIT DEEP LEARNING MODEL FOR VEHICULAR NETWORKS ANOMALY-BASED INTRUSION DETECTION

Tose E. Oziegbe, *Abel E. Edje and Maureen Akazue

[1]Department of Computer Science, Delta State University Abraka, Delta State, Nigeria.

*Corresponding authors' email: edjeabel@delsu.edu.ng

ABSTRACT

The growing connection and dynamic communication patterns of vehicle-to-everything (V2X) systems provide serious security concerns for modern vehicular networks. In vehicle contexts, traditional intrusion detection techniques are insufficient for identifying new assaults and adjusting to quickly evolving network topologies. An improved Gated Recurrent Unit (GRU)-based deep learning model for anomaly-based intrusion detection in vehicular networks is presented in this study. Multi-scale convolutional neural networks (CNN) with variable kernel sizes (3, 5, and 7) for temporal pattern recognition, principal component analysis (PCA) for dimensionality reduction while maintaining 95% variance, multi-head attention mechanisms for focused feature engineering, statistical feature extraction for capturing distributional characteristics of traffic patterns, and adaptive synthetic sampling (ADASYN) for handling imbalanced datasets are all integrated into the suggested architecture. The hybrid GRU-CNN model combines CNN's spatial feature extraction capabilities with bidirectional GRU layers to capture temporal dependencies. The findings of performance evaluation on five publicly accessible datasets (NSL-KDD, CAN_HCRL_OTIDS, Car-Hacking, Network-Traffic, and Road-Traffic) are remarkable, with accuracy rates ranging from 97.09% to 99.99%. The CAN_HCRL dataset exhibits an almost perfect classification. The model successfully detects a variety of attack types, such as denial-of-service, replay attacks, and fake information injection, while maintaining low false positive rates (0.01% to 20.63%) and high ROC-AUC scores (0.9000 to 0.9999). ADASYN greatly increased minority class detection by improving class balance by up to 99.4%. By offering a reliable, real-time intrusion detection solution appropriate for safety-critical autonomous driving applications, this research increases vehicular network security.

Keywords: Gated Recurrent Unit (GRU), Vehicular Ad Hoc Networks (VANETs), Intrusion Detection System (IDS), Adaptive Synthetic Sampling (ADASYN), Principal Component Analysis (PCA)

INTRODUCTION

As a result of large attack surfaces created by numerous communication channels and network interfaces, vehicular networks are faced with a wide range of potential threats. Vehicular industry has changed due to the development of intelligent transportation systems (ITS) and vehicle-to-everything (V2X) technologies of communication, which allow exchange of data in real-time for optimized road safety, autonomous driving, and management of traffic (Khan et al., 2022). Vehicular networks are becoming more and more indispensable on these systems for applications where safety is critical like emergency response coordination, collision avoidance, and cooperative adaptive cruise control, where even minute delays or failure of system can have disastrous results. Denial-of-service attack (DoS) is one of the threats vehicular systems are faced with, it can hamper entire transportation networks. Other anomalous activities include malicious attacks that target communication protocols, unauthorized access to vehicle control systems, and data manipulation that compromises processes of making security decisions (Nguyen et al., 2023). Two types of IDS techniques are: detection based on signatures identification, for known attack patterns recognition, and detection that looks for diversions from ordinary activity, which are termed anomalies. The intrusion approach based on anomalies identification works very notably for vehicular networks. IDSs offers profound security layer for vehicular systems, they provide critical monitoring and threat identification possibilities, (Aung et al., 2023). This goes beyond the security offered by conventional firewalls and authentication techniques. For the dynamic communication patterns that is usually found in vehicular environments, anomaly-based intrusion detection is very proper, it also excels in identifying novel and zero-day attacks that lack previously documented signatures (Xiao et al., 2022). This is true, as automotive behavior varies typically depending on factors like traffic density, road conditions, and time of day. Since vehicular communications exhibit strong time-dependent characteristics where the sequence and timing of messages carry critical information about system state and potential security threats, the efficacy of anomaly-based intrusion detection in vehicular networks essentially depends on the ability to recognize sequential and temporal patterns in network traffic. Time-series data that records the temporal relationships between successive inputs is captured by recurrent neural networks (RNNs), they have become effective tools also because of their innate capacity to preserve internal memory states. Gated Recurrent Units (GRUs) are an enhanced and efficient RNN design that overcomes many of the hurdles of conventional recurrent networks while preserving computational tractability for real-time applications (Kothai et al., 2024). GRUs are architecturally designed to offer in-built resistance to vanishing gradient problem, which often negatively affects the training of deep recurrent networks; and they accomplish detection tasks with fewer parameters and lower computational overhead, enabling quick processing of immense network traffic volumes, essential for timely threat detection. GRUs are very suitable for use in scenarios where memory and processing capacity might be limited, their gating mechanisms efficiently capture long-term dependencies in communication patterns that may span multiple message exchanges (Almahadin et al., 2023). This paper presents an improved GRU-based deep learning model,

in order to address crucial difficulties of anomaly-based intrusion detection in vehicular networks. It combines the temporal modeling capabilities of GRUs with architectural improvements that increase detection accuracy, reduce false positive rates, and preserve the real-time performance requirements of safety-critical vehicular applications.

Related Literature Review

VeReMiNet, developed by Saudagar et al. (2023), was an amalgamated novel IDS model for detecting intrusions in VANETs through the use of Deep Neural Networks. Their approach was tested on VeReMi dataset and it focused on identifying position falsification anomalies and discovering silent threat data patterns. Upgraded performance was demonstrated by the system in training time, validation, accuracy, and precision metrics. Nevertheless, there was the possibility of inaccurate predictions from incorrect data representation in datasets. Hybrid CNN-GRU-based intrusion detection system proposed by Kothai et al. (2024) for secure communication in VANETs solved overfitting and low-velocity problems while disallowing data transmission disruption. The system resolved these issues effectively, achieving strong performance in precision, recall, f1-score, and accuracy. The researchers noted that extensive development time was required for model creation. Attaining reduced communication overhead and diverse anomalies detection over traditional detection mechanisms, (Arya et al., 2023) addressed complexity of VANETs intrinsic vulnerability to cyberattacks. They used a federated learning technique to develop local, deep learning-based IDS classifiers for VANET data streams; they then shared their locally learned classifiers upon request, significantly reducing communication overhead with neighboring vehicles: then, an ensemble of federated heterogeneous neural networks was constructed for each vehicle, including locally and remotely trained classifiers. Zhang et al., (2024) acquired reduced costs for storage, and lesser data redundancy by executing dimensionality reduction using Gaussian Random Incremental Principal Component Analysis (GRIPCA)--Optimal Weighted Extreme Learning Machine (OWELM) algorithm to resolve drawbacks of detection challenges that consumes time. This was posed by substantial generated data within vehicular network but there was crucial necessity to implement synthetic minority oversampling technique (SMOTE), to randomly oversample unbalanced data within the internet of vehicles (IOV); in order to balance samples, improve model capability and identify minority categories that was pending. Hsu et al. (2021) addressed the ineffectiveness of traditional rule-based algorithms in detecting misbehavior in VANETs by developing an integrated algorithm combining CNN, LSTM, and Support Vector Machines (SVM). Tested on the VeReMi Extension dataset, their approach provided integrated and diversified misbehavior detection capabilities but they discovered datasets with very imbalanced classes could lead to erroneous conclusions. Performance was measured using f1-score, accuracy, and precision. Obtaining reduced operation time while maintaining detection accuracy, using Lightweight Neural Network (LNN) algorithm to ameliorate complexity of timelines in In-Vehicle networks; (Ding et al., 2023) in "Intrusion Detection for In-Vehicle CAN Bus Based on Lightweight Neural Network" experienced constrained and limited capability to represent features in complex tasks. Redundant neuron screening method and model compression algorithm for layer-by-layer neuron pruning was also designed.

MATERIALS AND METHODS

This model employed a hybrid GRU--CNN algorithm for anomaly-based intrusion detection, statistical feature extractor for feature extraction, a convolutional neural network (CNN) algorithm with variable kernel sizes (3, 5, & 7) for additional feature extraction, principal component analysis (PCA) for dimensionality reduction, multi-head attention mechanism for focused feature engineering, and adaptive synthetic sampling (ADASYN) for dataset balancing. To assess the performance of the model, accuracy, precision, recall, f1-score, ROC, and false positive rate (FPR) were the metrics used. For anomaly-based intrusion detection, the classification algorithms were chosen based on their characteristics and ability to adapt dynamically, and produce enhanced results. Additionally, the classification methods demonstrated excellent promise and optimized performances when applied to various datasets. The NSL-KDD, CAN_HCRL_OTIDS, Car-Hacking, Network-Traffic, and Road-Traffic datasets were chosen for this study. These datasets are accessible to the general public from standard academic repositories, and can also be obtained from Kaggle.com. The datasets were selected based on their prevalence traits and primary vehicular characteristics.

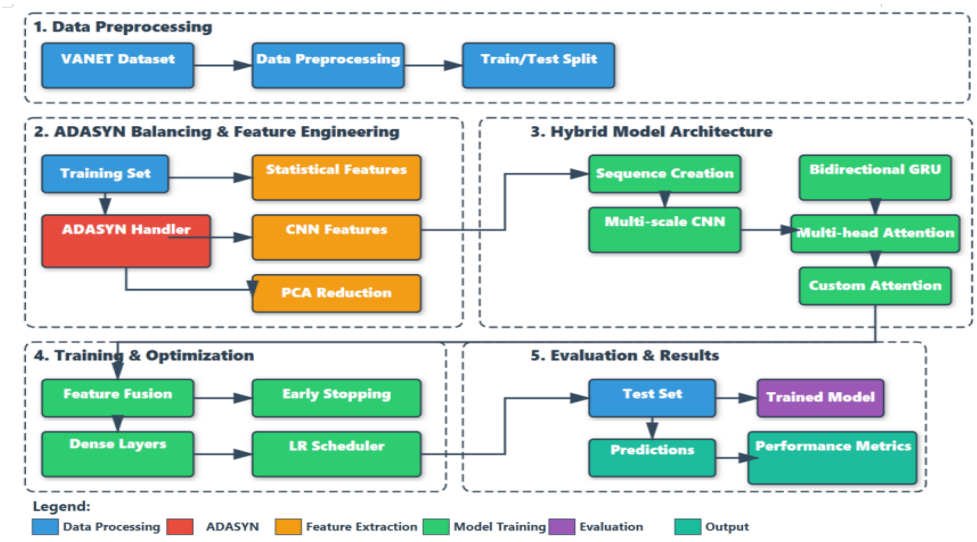

Figure 1: Methodology Framework, Adapted Structured Pattern from Almahadin et al., (2023)

Program Paradigm and Experimental Configuration

Visual Studio Code (VS code) serves as the integrated development environment (IDE), amidst the whole project development lifecycle, (Gupta et al., 2024). It supports entire completion of code which makes up the creation of intricate GRU model structures by recommending necessary tensorflow parameters and functions, through IntelliSense (Martinez et al., 2024). This integrated terminal supports the monitoring of model performance in real-time and the unhindered processing of training scripts. Tracking of experimental modifications to hyperparameters are captured faster with integration version control through Git. Management of different iterations of the IDS model is also handled (Thompson et al., 2024). This anomaly-based IDS was created using python. When GRU-based models are developed for security applications that deals with vehicular networks, the named language is utilized because of its wide data science libraries coverage and machine learning features (Rahman et al., 2024). Python has vast community support, which guarantees access to in-built modules for managing delicate data preprocessing tasks unique to vehicular network traffic patterns (Kim et al., 2024). Seaborn, matplotlib, scikit-learn (sklearn), imbalanced-learn (imblearn), and tensorflow are some of the python libraries utilized, to mention a few.

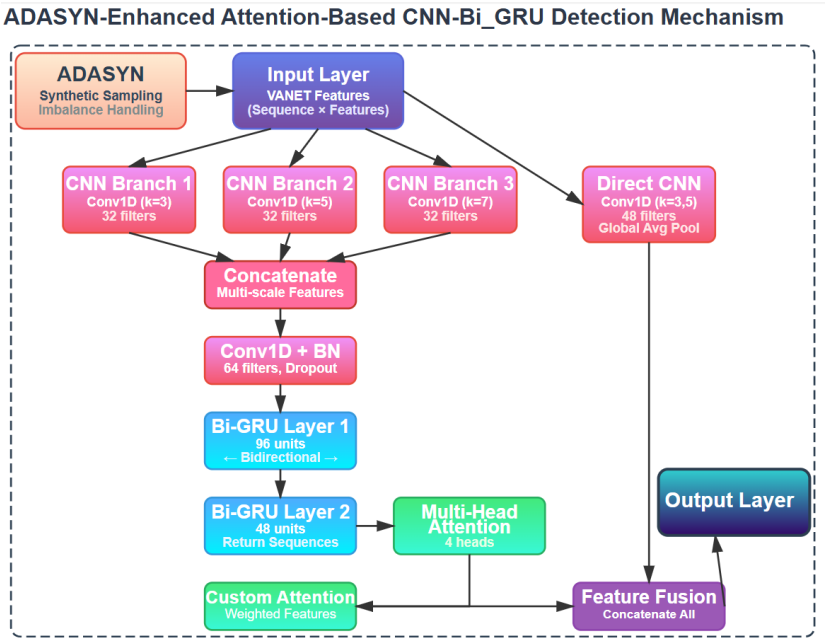

Figure 2: Hybrid CNN-Bi_GRU Schematic Diagram

Evaluation Metrics and Performance

The evaluative comparison of the proposed method on different datasets was done based on the performance measures of classification accuracy, precision, recall, f1-score, false positive rates and ROC.

RESULTS AND DISCUSSION

Table_1 shows the prediction performance of proposed model with five diverse datasets. The result from the table shows CAN-HCRL-OTIDS has the lowest FPR value, and the highest values for accuracy, precision, recall, f1-score and ROC. Network Traffic dataset has next best performance, followed by Road Traffic dataset, Car hacking dataset and then NSL-KDD dataset. The corresponding datasets results of this research, are displayed graphically in figure 3, figure 4 and figure 5; figure 6 shows their comparison. Table 2 shows the performance of each dataset, considering their specific attack types and table 3 shows ADASYN percentage improvements on each dataset. The ROC curves for CAN-HCRL-OTIDS and Road Traffic datasets are shown in figure 7, and their corresponding confusion matrices are shown in figure 8. All the other datasets displayed similar performances.

Table 1: ADASYN Enhanced Attention-Based Bi_GRU IDS Results with Five Different Datasets

Datasets	Accuracy	Precision	Recall	F1-score	FPR	ROC
Road Traffic	0.9903	0.9897	0.9903	0.9898	0.0050	0.9997
CAN HCRL	0.9999	0.9999	0.9999	0.9999	0.0001	0.9999
Network Traffic	0.9930	0.9929	0.9930	0.9919	0.0032	0.9991
Car HD	0.9783	0.9706	0.9783	0.9727	0.0038	0.9641
NSL-KDD	0.9709	0.9669	0.9709	0.9673	0.0063	0.9000

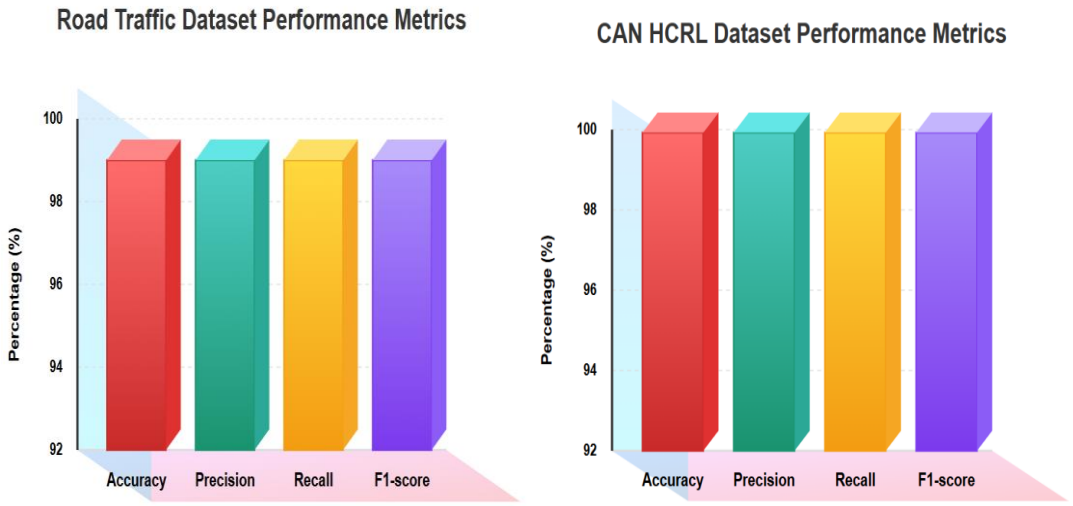

Figure_3 Prediction Performance of Anomaly-based Intrusions with Hybrid CNN-GRU Algorithm on Road Traffic Dataset and CAN HCRL Dataset

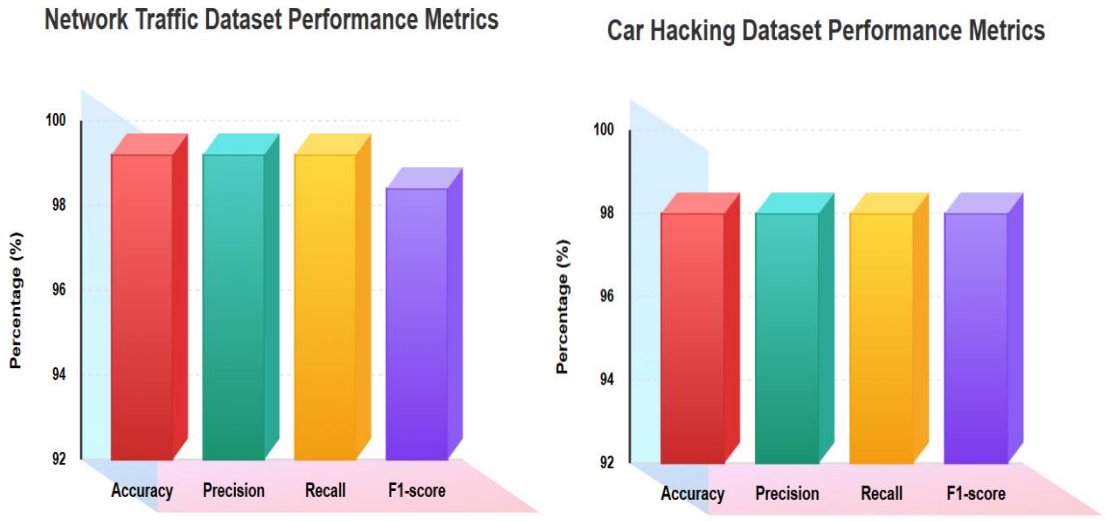

Figure_4 Prediction Performance of Anomaly-based Intrusions with Hybrid CNN-GRU Algorithm on Network Traffic Dataset and Car Hacking Dataset

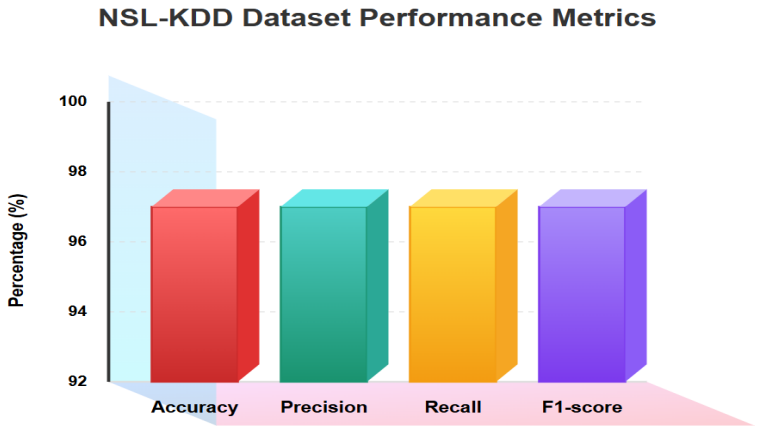

Figure 5: Prediction Performance of Anomaly-based Intrusions with Hybrid CNN-GRU Algorithm on NSL-KDD Dataset

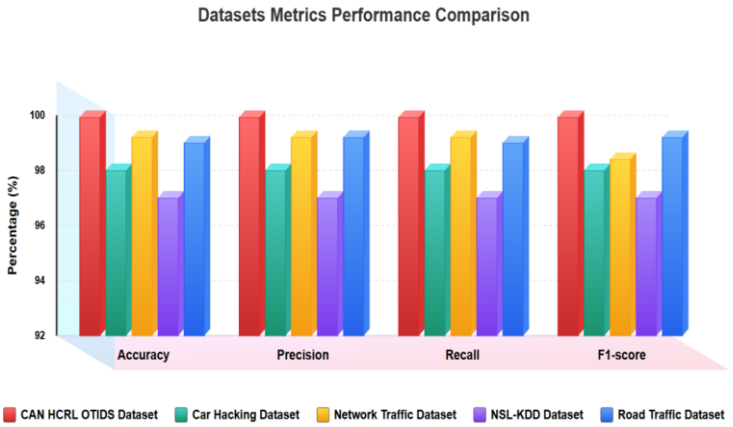

Figure6: Comparison of Prediction Performance of Anomaly-based Intrusions with Hybrid CNN-GRU Algorithm on all Dataset used

Table 2: ADASYN Enhanced Attention-Based Bi_GRU IDS Results with Five Different Datasets for Specific Attack Types

ROAD TRAFFIC DATASET				
Attack Type	Accuracy	Precision	Recall	F1-score
Dos Attack	0.9903	0.9994	1.0000	0.9997
False Info	0.9903	0.9857	0.9924	0.0891
CAN-HCRL-OTIDS DATASET				
Attack Type	Accuracy	Precision	Recall	F1-score
Class_0	0.9999	0.9999	0.9999	0.9999
Class_1	0.9999	0.9999	0.9999	0.9999
Class_2	0.9999	0.9999	0.9999	0.9999
Class_3	0.9999	0.9999	0.9999	0.9999
NETWORK TRAFFIC DATASET				
Attack Type	Accuracy	Precision	Recall	F1-score
Dos Attack	0.9930	0.9994	0.9949	0.9972
False Info	0.9930	0.9381	0.9100	0.9239
Replay Attack	0.9930	0.9946	0.9991	0.9968
CAR HACKING DATASET				
Attack Type	Accuracy	Precision	Recall	F1-score
Dos Attack	0.9783	0.9818	0.9962	0.9890
NSL-KDD DATASET				
Attack Type	Accuracy	Precision	Recall	F1-score
Replay Attack	0.9709	0.9792	0.9920	0.9856

Table 3: ADASYN Improvement Results On the Datasets Used

ROAD TRAFFIC DATASET				
Class Distributions	Class_0	Class_1	Class_2	
Original Class Distribution	6499	5490	211	
Balanced Class Distribution	6499	5490	3257	
Adasyn Improvement 93.5%				
CAN HCRL DATASET				
Class Distribution	Class_0	Class_1	Class_2	Class_3
Original Class Distribution	5975	1777	1616	2632
Balanced Class Distribution	5975	1777	1616	2632
Adasyn Improvement 0.00%				
NETWORK TRAFFIC DATASET				
Class Distribution	Class_0	Class_1	Class_2	Class_3
Original Class Distribution	7097	398	51	4454
Balanced Class Distribution	7097	3555	3546	4454
Adasyn Improvement 98.6%				
CAR HACKING DATASET				
Class Distribution	Class_0	Class_1		
Original Class Distribution	11749	251		
Balanced Class Distribution	11749	5893		

Adasyn Improvement 95.7%			
NSL-KDD DATASET			
Class Distribution	Class_0	Class_1	Class_2
Original Class Distribution	37	365	11598
Balanced Class Distribution	5794	5767	11598
Adasyn Improvement 99.4%			

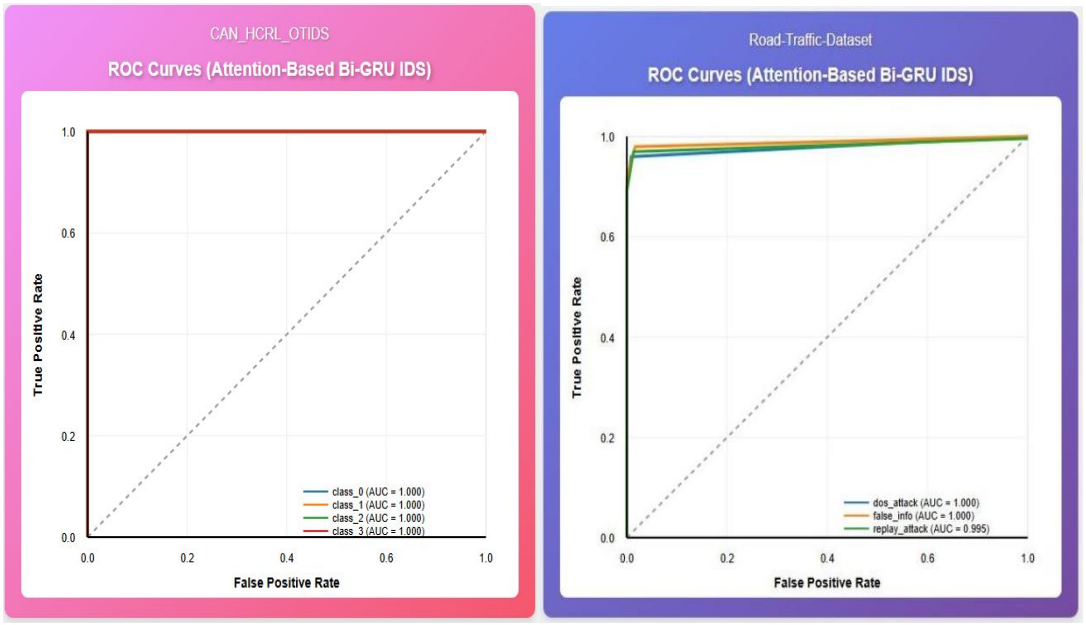

Figure_7 ROC-curve Prediction Performance of Anomaly-based Intrusions with Hybrid CNN-GRU Algorithm on CAN HCRL Dataset and Road Traffic Dataset

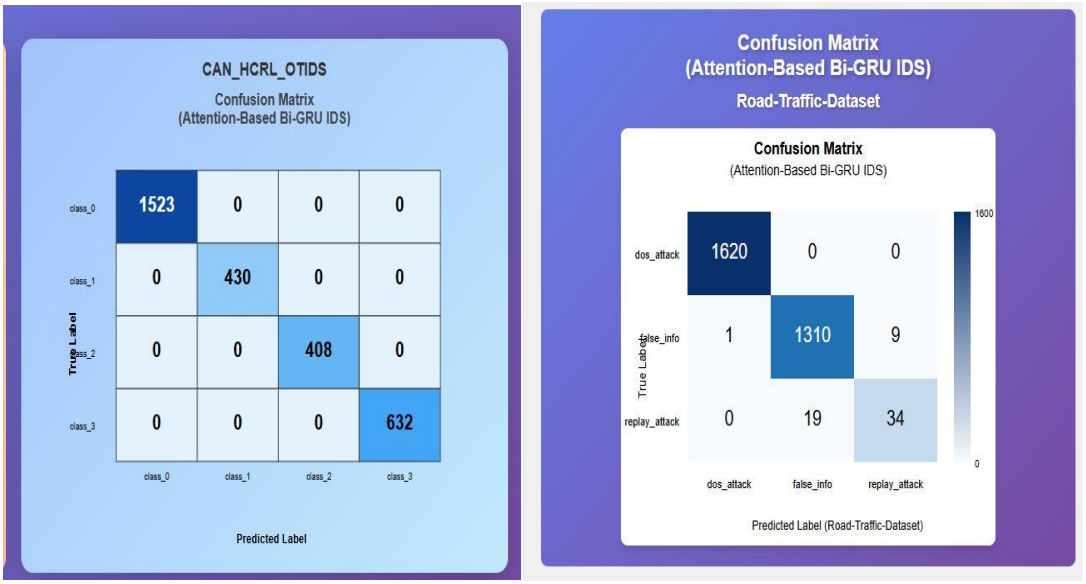

Figure8: Confusion Prediction Performance of Anomaly-based Intrusions with Hybrid GRU-CNN Algorithm on CAN HCRL Dataset and Road Traffic Dataset

Contributions to Knowledge

This research work has made significant contributions to the body of scientific knowledge:

i. The research has shown that convolutional layers with variable kernel sizes efficiently captures temporal patterns at different granularities and executes multi-branch processing for optimal performance.

ii. The research developed an Attention-based Bi-directional Gated Recurrent Unit model for identification and detection of anomaly-based intrusion in vehicular networks.

CONCLUSION

This research successfully developed an enhanced GRU-based deep learning model for anomaly-based intrusion detection in vehicular networks, addressing critical security challenges in modern intelligent transportation systems. The proposed hybrid GRU-CNN architecture augmented with

statistical feature extraction, multi-scale feature extraction, PCA dimensionality reduction, multi-head attention mechanisms, and ADASYN balancing, demonstrated exceptional performance across five diverse datasets. The model achieved remarkable accuracy rates ranging from 97.09% to 99.99%, with the CAN HCRL dataset showing near perfect classification performance. The integration of bidirectional GRU layers effectively captured temporal dependencies in vehicular network traffic, while the attention mechanism enhanced focus on security-critical features. The extremely low false positive rates, particularly the 0.01% achieved on CAN-HCRL-OTIDS dataset, validates the model's reliability for real-time deployment in safety-critical vehicular environments. These results confirm that the proposed architecture provides a robust, efficient solution for protecting vehicular networks against evolving cyber threats while maintaining the computational efficiency necessary for real-time intrusion detection in resource-constrained vehicular computing environments.

REFERENCES

Aidil Redza Khan; Mohd Faizal Jamlos; Nurmadiha Osman; Muhammad Izhar Ishak: "DSRC Technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT System for Intelligent Transportation System (ITS): A Review". January 2022. https://doi.org/10.1007/978-981-33 -4597.-3_10

Thanh Nguyen Canh; Xiem HoangVan: "Machine Learning-Based Malicious Vehicle Detection for Security Threats and Attacks in Vehicle Ad-Hoc Network (VANET) Communications". Corpus ID: 267028266. https://doi.org/10.1109/RIVF60135.2023.10471804

Yan Lin Aung; Shanshan Wang; Wang Cheng: " Intrusion Detection System for In-Vehicle Networks". Information Security: 26th International Conference, ISC 2023, Groningen, The Netherlands, November 15–17, 2023, ProceedingsNov 2023Pages 79–98. https://doi.org/10.1007/978-3-031-491870_5

Junchao Xiao; Lin Yang; Fuli Zhong; Hongbo Chen: "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework". May 2022Applied Intelligence 53(2). https://doi.org/10.1007/s10489-022-03412-8

Ghayth ALMahadin; Yassine Aoudni; Mohammad Shabaz; Anurag Vijay Agrawal; Ghazaala Yasmin; Esraa Saleh Alomari; Hamza Mohammed Ridha Al-Khafaji; Debabrata Dansana; Renato R. Maaliw III: "VANET Network Traffic Anomaly Detection using GRU-Based Deep Learning Model". https://doi.org/10.1109/TCE.2023.3326384

Saleha Saudagar; Rekha Ranawat: "An Amalgamated Novel IDS Model for Misbehaviour Detection using VeReMiNet". https://doi.org/10.1016/j.csi.2023.103783

Kothai G; Poovammal E: "A hybrid CNN-GRU-based intrusion detection system for secure communication in vehicular adhoc network". https://doi.org/10.1080/19393555.2024.2361244

Monika Arya; Hanumat Sastry; Bhupesh Kumar Dewangan; Mohammad Khalid Imam Rahmani ; Surbhi Bhatia; Abdul Wahab Muzaffar; Mariyam Aysha Bivi: "Intruder Detection in VANET Data Streams Using Federated Learning for Smart City Environments". Electronics 2023, 12(4), 894; https://doi.org/10.3390/electronics12040894

Kaijun Zhang; Jiayu Yang; Yangfei Shao; Lehua Hu: "Intrusion Detection Model for Internet of Vehicles Using GRIPCA and OWELM". January 2024IEEE Access PP (99):1-1. https://doi.org/10.1109/ ACCESS.2024.3368392

Hsiao-Yuan Hsu; Nai-Hsin Cheng; Chun-Wei Tsai: "A Deep Learning-Based Integrated Algorithm for Misbehavior Detection System in VANETs". ACM ICEA '21: Proceedings of the 2021 ACM International Conference on Intelligent Computing and its Emerging Applications December 2021Pages 53–58. https://doi.org/10.1145/3491396.3506509

Defeng Ding; Yehua Wei; Can Cheng; Jing Long: "Intrusion Detection for In-Vehicle CAN Bus Based on Lightweight Neural Network". Journal of Circuits, Systems and ComputersVol. 32, No. 07, 2350110 (2023). https://doi.org/10.1142/S0218126623501104

Gupta, R., & Singh, A. (2024). Comparative analysis of integrated development environments for machine learning project development. *International Journal of Software Engineering and Applications*, 15(2), 45-62. https://doi.org/10.5121/ijsea.2024.15204

Martinez, L., Chen, W., & Park, S. (2024). Enhancing deep learning development efficiency through intelligent code completion systems. *IEEE Software*, 41(3), 78-86. https://doi.org/10.1109/MS.2024.3367842

Thompson, J., Anderson, M., & Roberts, K. (2024). Version control best practices for machine learning model development and hyperparameter optimization. *ACM Transactions on Software Engineering and Methodology*, 33(2), Article 48. https://doi.org/10.1145/3632146

Rahman, M. A., Hossain, M. S., & Islam, N. (2024). Machine learning library ecosystems for cybersecurity applications: Performance analysis and selection criteria. *Expert Systems with Applications*, 241, 122634. https://doi.org/10.1016/j.eswa.2023.122634

Kim, J., Lee, S., & Choi, H. (2024). Rapid prototyping methodologies for deep learning-based network intrusion detection systems. *Neural Computing and Applications*, 36(8), 4321-4338. https://doi.org/ 10.1007/s00521-023-09234-x