Context-Aware Federated Learning for Intelligent Threat Detection in Software-Defined Vehicular Networks

T. Harshitha[1], B. Ravikumar[1], Ch. Pavani[1], D. Shilpa[1]

[1]Department of Electronics & Communication Engineering, Mother Teresa Institute of Science & Technology, Sanketika Nagar, Kothuru, Sathupally, Khammam, 507303, Telangana, India

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) generate massive volumes of real-time communication data, including packet size, packet rate, latency, vehicle speed, signal strength, and message transmission information. Due to the open wireless communication environment, decentralized architecture, and highly dynamic topology of VANETs, these networks are particularly vulnerable to cyberattacks, malicious intrusions, and anomalous communication activities. Traditional intrusion detection approaches primarily rely on rule-based systems and statistical threshold methods, which often lack adaptability and struggle to identify emerging attack patterns in real-time scenarios. To address these limitations, the proposed framework introduces a hybrid Machine Learning (ML) and Deep Learning (DL)-based intrusion detection system utilizing Classification and Regression Trees (CART) for enhanced attack detection and anomaly prediction. The framework incorporates multiple algorithms, including Linear-CART, Decision Tree-CART, Passive Aggressive-CART, and the K-NeuroFusion CART model. The K-NeuroFusion architecture combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to extract spatial and temporal features from vehicular communication data, while K-Nearest Neighbors (KNN) further improves classification performance. Additionally, the proposed Temporal Echo Fusion Network (TEFN) employs an Echo State Network–Decision Tree Cost Complexity Pruning (ESN-DTCCP) model to perform advanced temporal pattern analysis and anomaly score prediction. The framework supports both classification and regression tasks for identifying normal and malicious communication behaviors while estimating anomaly severity levels. Furthermore, it provides single and batch prediction capabilities along with visualization and exploratory data analysis modules. Implemented using Flask, SQLite, TensorFlow, Scikit-learn, Pandas, NumPy, and Matplotlib, the proposed system offers an accurate, scalable, and efficient solution for intelligent VANET security and anomaly detection.

Keywords: Vehicular Ad Hoc Networks (VANETs), Intrusion Detection System, Deep Learning, Echo State Network (ESN), Network Security, Anomaly Detection.

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have emerged as a fundamental component of intelligent transportation systems, enabling seamless communication among vehicles and roadside infrastructure. By supporting Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, VANETs facilitate the real-time exchange of critical information such as vehicle speed, position, direction, traffic congestion updates, road conditions, accident notifications, and emergency warnings. This continuous flow of information allows vehicles to make informed decisions, thereby enhancing road safety, improving traffic efficiency, reducing travel delays, and minimizing fuel consumption. Furthermore, VANETs play a significant role in supporting advanced transportation applications, including collision avoidance systems, emergency vehicle prioritization, autonomous driving assistance, and intelligent traffic management. As modern transportation systems continue to evolve toward greater connectivity and automation, VANETs serve as a key enabling technology for creating safer, smarter, and more efficient road networks. Despite their advantages, VANETs are highly

susceptible to security threats due to their open wireless communication medium, decentralized architecture, and rapidly changing network topology. Since vehicles continuously join and leave the network, maintaining secure and reliable communication becomes a challenging task. Attackers can exploit these vulnerabilities to launch various cyber-attacks that compromise network performance and user safety. Common threats include message tampering attacks, where transmitted information is altered during communication; denial-of-service attacks, which overwhelm network resources and disrupt communication channels; false data injection attacks, where fabricated information is introduced into the network; replay attacks that resend previously transmitted messages; and Sybil attacks that create multiple fake identities to manipulate network operations. Such malicious activities can result in incorrect traffic information, delayed emergency responses, network congestion, and potentially catastrophic road accidents. Therefore, ensuring the integrity, authenticity, confidentiality, and availability of transmitted data has become a critical requirement for the successful deployment of VANET-based transportation systems.

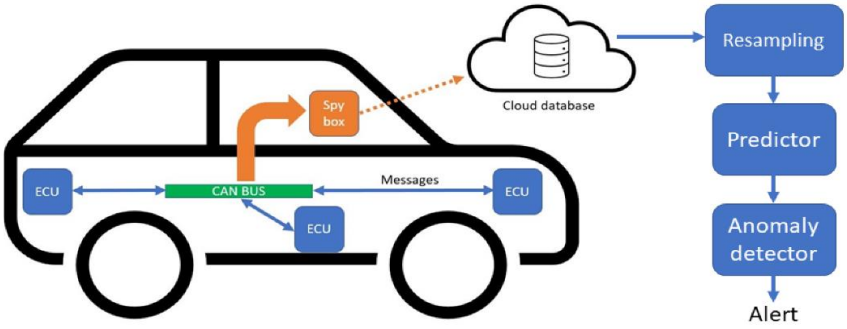

Fig. 1: Anomaly Detection in VANETs

To mitigate these security challenges, researchers have developed various protection mechanisms, including cryptographic techniques, authentication protocols, digital signatures, trust-based frameworks, and intrusion detection systems. However, traditional security approaches often struggle to detect sophisticated and evolving attack patterns in highly dynamic VANET environments. As a result, AI, ML, and DL techniques have gained significant attention for enhancing network security through intelligent attack detection and classification. These approaches can analyze large volumes of vehicular communication data, identify abnormal behaviors, learn complex attack patterns, and provide accurate real-time threat detection. Advanced models can further improve detection performance by reducing false positives and adapting to emerging attack scenarios. Consequently, the integration of intelligent security mechanisms with VANET infrastructure has become a promising research direction for developing robust, reliable, and secure transportation networks capable of supporting future connected and autonomous vehicle ecosystems.

2. LITERATURE SURVEY

Aloqaily et al. [1] introduced an advanced intrusion detection framework for connected vehicular networks operating within smart city infrastructures. Their approach integrated deep learning models to automatically extract meaningful features from large volumes of vehicular communication data, while decision tree algorithms were employed for the final classification of network activities. By combining the strengths of both techniques, the system effectively identified malicious behaviors and cyber threats in highly dynamic network environments. Experimental results demonstrated improved detection accuracy, reduced false alarms, and enhanced capability to process complex communication patterns generated by modern vehicular systems. Refat et al. [2] proposed a computationally efficient intrusion detection mechanism specifically designed for vehicular communication environments with limited

processing resources. The authors utilized temporal traffic analysis to capture communication behavior over time and employed similarity-based anomaly detection techniques to distinguish normal and malicious activities. Their method significantly reduced computational overhead while preserving reliable detection performance. The lightweight architecture made the system suitable for real-time deployment in vehicular networks where rapid response and low latency are critical requirements. Deng et al. [3] presented a novel security solution based on voltage fingerprint analysis for identifying malicious nodes within vehicular communication systems. Instead of relying on traditional software-level authentication mechanisms, the proposed method exploited unique hardware-level electrical characteristics generated by communication devices. By analyzing these voltage signatures, the framework successfully differentiated legitimate vehicles from compromised or malicious entities. The approach provided an additional layer of protection at the physical communication level and demonstrated strong effectiveness in accurately tracing attack origins without requiring predefined device mappings. Ding et al. [4] developed a deep learning-driven intrusion detection framework utilizing Convolutional Neural Networks (CNNs) to automatically learn representative features from vehicular network traffic. The proposed model was designed to process large-scale communication data and identify abnormal patterns associated with cyber-attacks. Through hierarchical feature extraction, the CNN architecture captured complex traffic relationships that are often difficult to detect using conventional methods. Experimental evaluations showed that the framework achieved high detection accuracy, improved classification performance, and efficient real-time processing capabilities in dynamic vehicular environments.

Seo et al. [5] investigated the resilience of ML-based intrusion detection systems against adversarial attacks targeting vehicular communication networks. The researchers generated carefully crafted adversarial samples to assess how detection models respond to manipulated input data. Their findings revealed that many existing detection approaches experience substantial performance degradation when exposed to adversarial conditions. The study highlighted critical security vulnerabilities in current intelligent detection frameworks and emphasized the necessity of developing more robust and attack-resistant anomaly detection models for future vehicular applications. Jeong et al. [6] proposed an unsupervised anomaly detection framework based on neural network architectures for identifying malicious activities in vehicular networks. Unlike supervised approaches that require extensive labeled datasets, their method learned normal communication behavior directly from unlabeled network data. The system calculated anomaly scores by measuring deviations from learned behavioral patterns and flagged suspicious activities accordingly. This capability enabled the framework to detect previously unseen attacks and adapt to continuously evolving network conditions, making it particularly suitable for highly dynamic vehicular communication environments. Peng et al. [7] proposed a CNN-based intrusion detection framework tailored for vehicular communication environments where computational resources and processing capabilities are often limited. The authors focused on designing an optimized network architecture capable of extracting meaningful traffic features while maintaining low computational complexity. By carefully reducing model overhead without sacrificing predictive performance, the proposed system achieved high detection accuracy and faster inference times. Experimental results demonstrated that the framework effectively identified malicious network activities and was suitable for real-time deployment in VANET environments where rapid threat detection is essential.

Shahriar et al. [8] introduced a deep learning-based anomaly detection framework utilizing autoencoder networks to uncover hidden and sophisticated attacks within vehicular communication systems. The proposed approach learned the normal characteristics of network traffic during training and reconstructed incoming data during operation. Any significant reconstruction error was treated as an indication of abnormal behavior or potential cyber-attacks. This methodology enabled the detection of

stealthy threats that often bypass traditional signature-based security mechanisms. The experimental findings showed improved capability in identifying complex attack patterns while maintaining reliable detection performance across diverse network scenarios. Anand et al. [9] developed a two-stage intrusion detection framework that combined the predictive power of deep learning models with the interpretability of rule-based systems. In the first stage, neural network models were employed to identify suspicious network activities and classify potential threats. Subsequently, rule extraction techniques were applied to generate understandable decision rules from the learned model behavior. This hybrid strategy not only improved attack detection accuracy but also enhanced transparency by providing explanations for classification outcomes. The proposed framework addressed one of the major limitations of deep learning systems by making security decisions more interpretable and trustworthy. Meng et al. [10] proposed a graph-based anomaly detection technique for securing vehicular communication networks. The researchers represented communication interactions among vehicles as graph structures, where nodes and edges captured the relationships between participating entities. By analyzing graph topology and communication patterns, the system identified abnormal behaviors that deviated from expected network interactions. This approach proved effective in detecting coordinated attacks and complex malicious activities that are difficult to identify through conventional traffic analysis methods. Experimental evaluations demonstrated improved detection performance for network-level threats and enhanced visibility into communication dynamics. Taslimasa et al. [11] presented a hybrid intrusion detection system that integrated both machine learning and deep learning techniques to strengthen network security in vehicular environments. The framework leveraged the complementary strengths of multiple algorithms to improve attack classification and anomaly detection capabilities. By combining different learning models, the system effectively captured both simple and complex traffic patterns while adapting to changing network conditions. The proposed methodology demonstrated enhanced detection accuracy, improved robustness against diverse attack types, and better generalization performance across varying communication scenarios. Amutha et al. [12] proposed a multi-layer intrusion detection framework based on ensemble learning techniques to improve cybersecurity within vehicular communication systems. The framework combined the predictions of multiple classifiers to produce more reliable and accurate intrusion detection results. Through the aggregation of diverse model outputs, the system minimized the impact of individual classifier weaknesses and reduced false positive and false negative rates. The multi-layer architecture enabled comprehensive analysis of network traffic from different perspectives, resulting in enhanced robustness and stability. Experimental studies confirmed that the proposed ensemble-based framework achieved superior performance when compared to individual classification models in complex vehicular network environments.

3. PROPOSED SYSTEM

The research is developed to provide an intelligent and automated solution for anomaly detection in VANET communication. In this research, real-time vehicular network data is collected and processed to identify whether the communication behavior is normal or malicious. The system is designed to improve security, reliability, and accuracy compared to traditional manual and rule-based methods. It uses a combination of data preprocessing, feature analysis, classification, and anomaly score prediction to monitor vehicular communication effectively as demonstrated in Fig. 2. In addition, the project is implemented as a web-based application so that users can easily perform prediction, analysis, and result visualization.

Step 1: Data Collection

The first step in the proposed system is collecting the VANET dataset containing important vehicular communication parameters. The dataset includes features such as timestamp, vehicle ID, packet size, packet rate, vehicle speed, message type, signal strength, latency, anomaly score, and target label. These parameters represent the communication behavior of vehicles in the network. The collected data acts as the foundation for training and testing the system.

Step 2: Data Preprocessing

After data collection, the raw dataset is pre-processed to make it suitable for analysis and model implementation. In this stage, categorical values such as vehicle ID and message type are converted into numerical form. Unnecessary inconsistencies are removed, and the data is organized in a structured format for training and prediction. This step is important because proper preprocessing improves the efficiency and performance of the overall system.

Step 3: Model Implementation

In this step, the system applies different algorithms for both classification and regression tasks. Classification is used to identify whether the network data belongs to the Normal or Attack category, while regression is used to predict the anomaly score. Multiple techniques are implemented and compared to analyze their performance. This step forms the core part of the project, where intelligent analysis is performed on vehicular communication data.

Step 4: Training and Testing

Once the models are implemented, the dataset is divided into training and testing sets. The training data is used to teach the system how to recognize patterns, while the testing data is used to evaluate its performance. During this process, the system learns the difference between normal and abnormal communication behavior. This step ensures that the project can provide reliable predictions on unseen data.

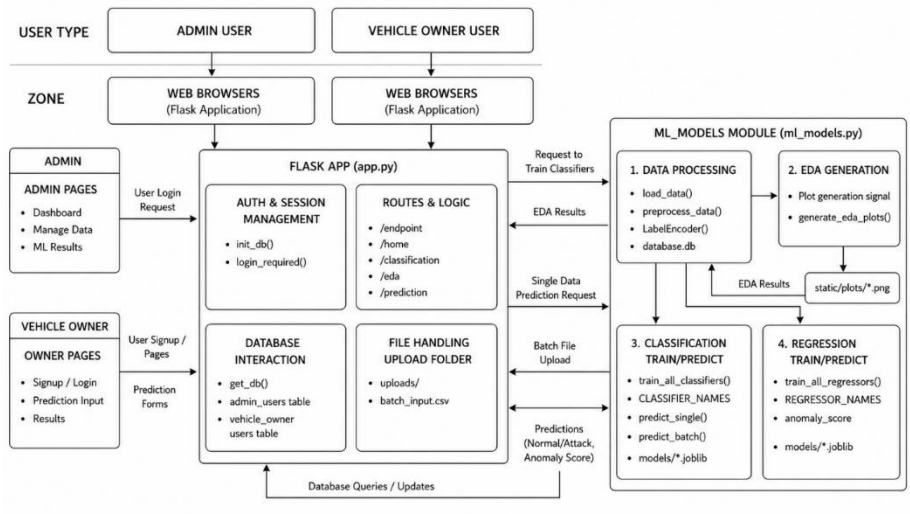

Fig. 2: Proposed system architecture.

Step 5: Prediction and Detection

After successful training, the proposed system is used for prediction. It accepts input data either as a single record or as a batch file and processes it through the trained system. Based on the input features, the system predicts the communication status as Normal or Attack and also provides the anomaly score. This step enables real-time and practical anomaly detection in vehicular network environments.

Step 6: Web-Based Deployment and Result Visualization

In the final step, the complete project is deployed as a web-based application using Flask. The system provides interfaces for admin and vehicle users to access dataset details, perform predictions, and view analysis results. It also includes graphical visualizations such as EDA plots, confusion matrices, ROC curves, and comparison results. This step makes the project user-friendly, interactive, and suitable for practical usage.

3.1 Architecture

The proposed architecture for the intelligent VANET intrusion detection system integrates Machine Learning (ML), Deep Learning (DL), deterministic temporal learning, and hybrid classification-regression models within a secure and user-interactive web framework. The system consists of two major components: the Administrator Module and the Vehicle Owner/User Module, connected through a Flask-based web application integrated with an SQLite database for authentication and secure data management. The Administrator Module is responsible for dataset management, model training, performance evaluation, and visualization. It includes functionalities such as Admin Sign-Up and Login, EDA, Classification, Regression, and Model Comparison. The framework implements multiple CART-based models including Linear-CART, DT-CART, PA-CART, the K-NeuroFusion CART model, and the advanced TEFN extension model. The K-NeuroFusion CART model. The TEFN model for optimized temporal feature learning and enhanced prediction accuracy. The Vehicle Owner/User Module allows authenticated users to perform real-time single and batch predictions using uploaded vehicular communication data. The system predicts both communication class (Normal or Attack) and anomaly severity scores. Additionally, automated visualization and performance analysis modules provide insights into traffic behavior, latency, signal strength, packet transmission, and anomaly distributions. This architecture provides a scalable, intelligent, and secure framework for real-time VANET cyberattack detection and anomaly analysis.

3.2 ESN-DTCCP

ESN-DTCCP is an advanced hybrid anomaly detection and prediction model developed for intelligent Vehicular Ad Hoc Network (VANET) security analysis. The model combines the temporal learning capability of Echo State Networks (ESN) with the optimized structural learning of Decision Tree Cost Complexity Pruning (DTCCP) to improve attack detection accuracy and anomaly score prediction. The ESN component is responsible for extracting complex temporal and sequential communication patterns from VANET data such as packet rate, latency, vehicle speed, and signal strength. The DTCCP component then performs optimized classification and regression using pruned boosted decision-tree learning, which reduces overfitting and improves prediction stability.

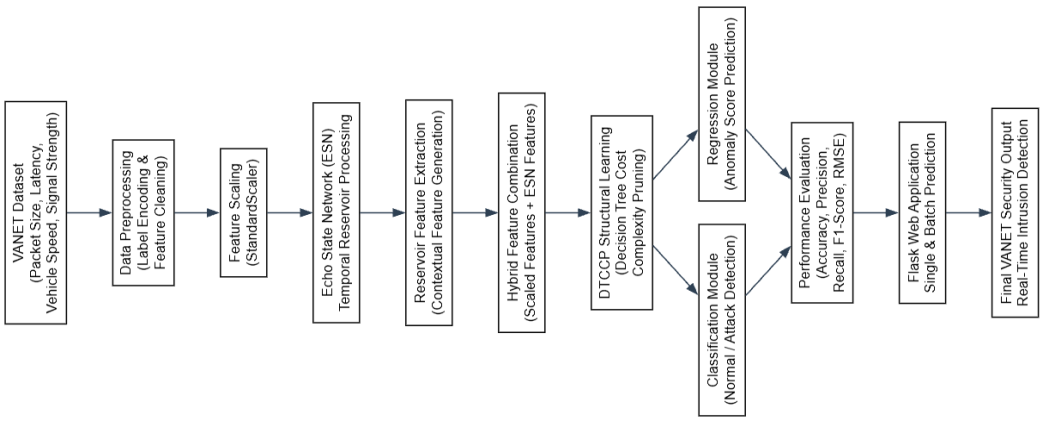

Fig. 3: Internal working flow of Extension TEFN model

Step 1: Data Collection and Preprocessing

The VANET dataset containing features such as packet size, packet rate, vehicle speed, latency, signal strength, and message type is collected and preprocessed. Categorical attributes like vehicle ID and message type are converted into numerical values using Label Encoding techniques.

After encoding, the dataset is normalized using StandardScaler to ensure all features are transformed into a uniform scale. This preprocessing step improves learning efficiency and stabilizes the model training process.

Step 2: Feature Scaling and Input Transformation

The preprocessed dataset is passed through feature scaling operations to standardize numerical ranges and eliminate feature imbalance issues. Standardization helps the ESN reservoir process sequential communication patterns more effectively.

The transformed input features are then prepared as multidimensional vectors which are supplied to the Echo State Network for temporal state generation and contextual feature extraction.

Step 3: Echo State Network (ESN) Reservoir Processing

The Echo State Network creates a large deterministic reservoir structure that captures temporal dependencies and communication behavior patterns present in VANET traffic. The reservoir continuously updates its internal states using nonlinear activation functions.

The ESN generates high-dimensional temporal reservoir features from the sequential network data. These extracted contextual features help the system understand evolving attack behaviors and dynamic communication characteristics.

Step 4: Reservoir Feature Extraction

The internal reservoir states generated by the ESN are collected and converted into feature vectors. These reservoir features contain important temporal and contextual information extracted from the VANET communication flow.

The generated ESN features are combined with the original scaled input features to form a hybrid feature representation. This improves the learning capability of the final classification and regression model.

Step 5: DTCCP Structural Learning

The hybrid feature vectors are supplied to the DTCCP module, which uses optimized boosted decision-tree learning with Cost Complexity Pruning techniques. The pruning mechanism removes unnecessary branches and reduces model complexity.

DTCCP learns nonlinear relationships between communication features and attack behaviors. This step improves classification accuracy, anomaly prediction precision, and overall generalization performance.

Step 6: Classification and Regression Prediction

The trained ESN-DTCCP classifier predicts whether the communication pattern belongs to the Normal or Attack category. Simultaneously, the regression module predicts the anomaly severity score associated with the communication behavior.

The final outputs are displayed through the Flask-based web application for both single prediction and batch prediction functionalities. This enables real-time intelligent intrusion detection in VANET environments.

9.3 Result Description

The results of the proposed system demonstrate the successful implementation of a web-based VANET anomaly detection platform with secure user access and intelligent prediction capabilities. The system integrates data preprocessing, EDA, ML/DL model execution, and result visualization into a unified interface. The application ensures efficient interaction between users and backend models such as LR CART, DT CART, PA CART, K-NeuroFusion CART and TEFN.

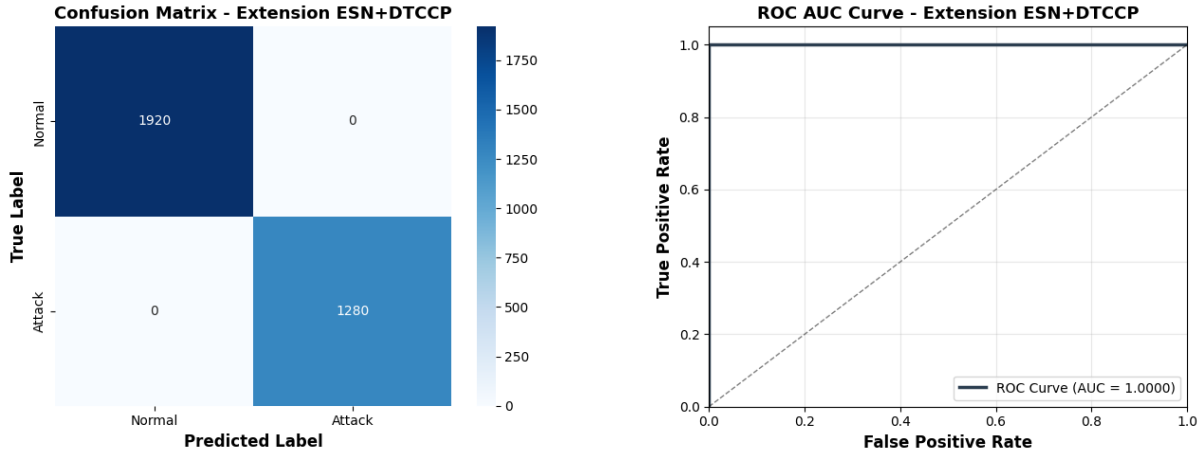

Fig. 4: Obtained Confusion Matrix and ROC Curve of TEFN CART Model

Fig. 4 illustrates the obtained Confusion Matrix and ROC Curve of the Temporal Echo Fusion Network (TEFN) CART model used for VANET intrusion detection. The confusion matrix demonstrates the model's capability to accurately classify Normal and Attack communication patterns with minimal misclassification errors. The ROC curve indicates the strong discriminative performance of the proposed model, achieving a high Area Under Curve (AUC) value for attack detection. The integration of Echo State Network (ESN) temporal feature extraction with Decision Tree Cost Complexity Pruning (DTCCP) significantly improves classification stability and prediction accuracy.

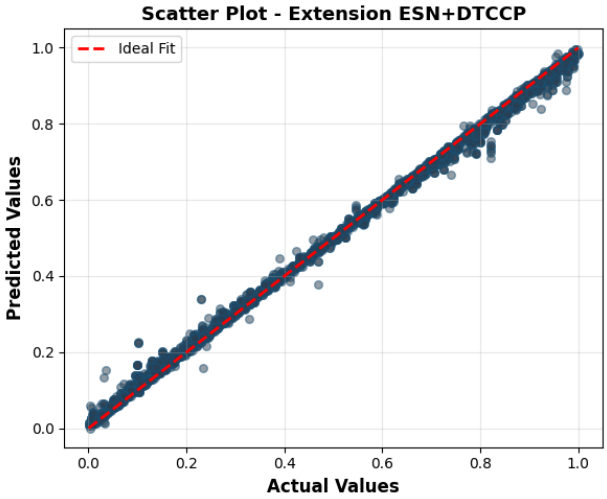

Fig. 5: Obtained Scatter Plots of Various CART Model TEFN.

The figure presents a scatter plot of actual values versus predicted values obtained using the Extension TEFN model. The data points are closely aligned along the diagonal reference line, indicating strong agreement between actual and predicted outputs. This alignment demonstrates the model's high prediction accuracy and effective regression performance. A small number of points show slight deviations from the reference line, representing minor prediction errors. The plot confirms that the

proposed model provides reliable and consistent anomaly prediction performance for VANET intrusion detection.

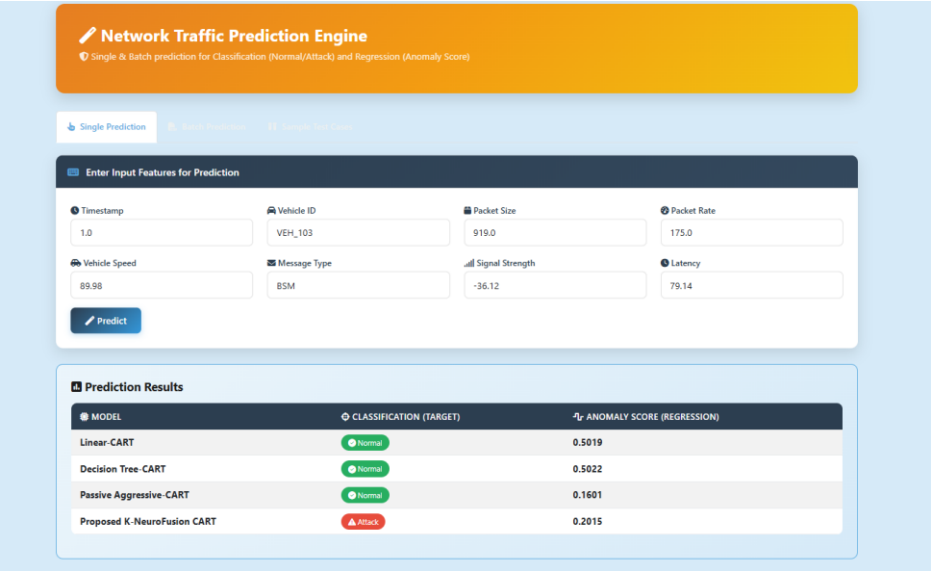

Fig. 9.12: Predictions on Sample Test Data

The performance comparison of various classification models is presented in Table 1. Among the traditional models, LR Classification and DT Classification achieved an accuracy of 60.00%, with precision, recall, and F1-score values of 36.00%, 60.00%, and 45.00%, respectively. PA Classification showed a slight variation, attaining 55.97% accuracy with improved precision of 51.91% and an F1-score of 51.72%. In contrast, the K-NeuroFusion Classification model demonstrated outstanding performance, achieving 99.78% across all evaluation metrics. Furthermore, the proposed TEFN Classification model achieved the highest performance with 100.0% accuracy, precision, recall, and F1-score, indicating its superior capability in accurately detecting and classifying VANET communication patterns. These results confirm the effectiveness of the proposed hybrid framework over conventional classification approaches.

Table 1: Classification Performance Comparison

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
LR Classification	60.00	36.00	60.00	45.00
DT Classification	60.00	36.00	60.00	45.00
PA Classification	55.97	51.91	55.97	51.72
K-NeuroFusion Classification	99.78	99.78	99.78	99.78
TEFN Classification	100.0	100.0	100.0	100.0

The regression performance comparison of different models is presented in Table 2. The traditional LR Regression and DT Regression models produced similar results, with MAE values of 0.245 and 0.2452, RMSE values of 0.2831, and negative R^2-Scores, indicating poor predictive performance. PA Regression exhibited the weakest performance, recording the highest error values and an R^2-Score of -

0.6115. In contrast, the K-NeuroFusion Regression model significantly improved prediction accuracy, achieving a low MAE of 0.0114, RMSE of 0.0394, and an R^2-Score of 0.9806. The proposed TEFN Regression model delivered the best overall performance with the lowest MAE (0.01), MSE (0.0003), RMSE (0.0159), and the highest R^2-Score (0.996). These results demonstrate that the proposed TEFN model provides highly accurate anomaly severity prediction and substantially outperforms conventional regression approaches.

Table 2: Regression Performance Comparison

Model	MAE	MSE	RMSE	R^2-Score
LR Regression	0.245	0.0801	0.2831	-0.0024
DT Regression	0.2452	0.0801	0.2831	-0.0025
PA Regression	0.2953	0.1288	0.3589	-0.6115
K-NeuroFusion Regression	0.0114	0.0016	0.0394	0.9806
TEFN Regression	0.01	0.0003	0.0159	0.996

5. CONCLUSION

This research successfully implements an intelligent VANET intrusion detection and anomaly prediction framework by integrating ML, DL, and hybrid temporal learning techniques. The framework encompasses data preprocessing, EDA, model training, performance evaluation, visualization, and real-time prediction within a secure Flask-based web application. Multiple models, including Linear-CART, DT-CART, PA-CART, K-NeuroFusion CART, and the proposed TEFN model, are developed and evaluated for both classification and regression tasks. The system analyzes vehicular communication data using key VANET features such as packet size, packet rate, vehicle speed, latency, signal strength, message type, and anomaly score. Experimental results demonstrate that the proposed TEFN model outperforms conventional ML and hybrid approaches by leveraging CNN-LSTM-based deep feature extraction, KNN prediction mechanisms, deterministic ESN, and DTCCP techniques for enhanced temporal pattern learning. The framework effectively classifies communication behavior into Normal and Attack categories while accurately predicting anomaly severity scores for intelligent threat assessment. Furthermore, the developed application provides secure user authentication, efficient model management, and real-time single and batch prediction capabilities, making it a reliable and scalable solution for intelligent transportation systems and next-generation secure vehicular communication environments.

REFERENCES

[1] Aloqaily, M.; Otoum, S.; Ridhawi, I.A.; Jararweh, Y. An Intrusion Detection System for Connected Vehicles in Smart Cities. Ad Hoc Networks, 2019, 90, 101842. (Hybrid Deep Belief Network + Decision Tree IDS)

[2] Refat, R.U.D.; Elkhail, A.A.; Malik, H. A Lightweight Intrusion Detection System for CAN Protocol Using Neighborhood Similarity. In Proceedings of CDMA 2022, Riyadh, Saudi Arabia, 2022.

[3] Deng, Z.; Xun, Y.; Liu, J.; Li, S.; Zhao, Y. A Novel Intrusion Detection System for Next Generation In-Vehicle Networks. In Proceedings of GLOBECOM 2022, Rio de Janeiro, Brazil, 2022.

[4] Ding, W.; Alrashdi, I.; Hawash, H.; Abdel-Basset, M. DeepSecDrive: An Explainable Deep Learning Framework for Real-Time Detection of Cyberattack in In-Vehicle Networks. Information Sciences, 2024, 658, 120057.

[5] Seo, E.; Kim, J.; Lee, W.; Seok, J. Adversarial Attack of ML-Based Intrusion Detection System on In-Vehicle System Using GAN. In Proceedings of ICUFN 2023, Paris, France, 2023.

[6] Jeong, S.; Kim, H.K.; Han, M.L.; Kwak, B.I. AERO: Automotive Ethernet Real-Time Observer for Anomaly Detection in In-Vehicle Networks. IEEE Transactions on Industrial Informatics, 2023, 20, 4651–4662.

[7] Peng, R.; Li, W.; Yang, T.; Huafeng, K. An Internet of Vehicles Intrusion Detection System Based on a Convolutional Neural Network. In Proceedings of ISPA/BDCloud/SocialCom/SustainCom 2019, Xiamen, China, 2019.

[8] Shahriar, M.H.; Xiao, Y.; Moriano, P.; Lou, W.; Hou, Y.T. CANShield: Deep Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal Level. IEEE Internet of Things Journal, 2023, 10, 22111–22127. The framework employs deep autoencoder networks for signal-level anomaly detection.

[9] Anand, M.; Kumar, S.P.; Selvi, M.; SVN, S.K.; Ram, G.D.; Kannan, A. Deep Learning Model Based IDS for Detecting Cyber Attacks in IoT Based Smart Vehicle Network. In Proceedings of ICSCDS 2023, Erode, India, 2023.

[10] Meng, Y.; Li, J.; Liu, F.; Li, S.; Hu, H.; Zhu, H. GB-IDS: An Intrusion Detection System for CAN Bus Based on Graph Analysis. In Proceedings of ICCC 2023, Dalian, China, 2023.

[11] Taslimasa, H.; Dadkhah, S.; Neto, E.C.P.; Xiong, P.; Iqbal, S.; Ray, S.; Ghorbani, A.A. ImageFed: Practical Privacy Preserving Intrusion Detection System for In-Vehicle CAN Bus Protocol. In Proceedings of BigDataSecurity/HPSC/IDS 2023, Xi'an, China, 2023.

[12] Amutha, S.; Ramathilagam, A. Improved IDS for Vehicular Ad-Hoc Network Using Deep Learning Approaches. In Proceedings of ICACRS 2023, Tiruchengode, India, 2023.