Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 15, Issue. 4, April 2026, pg.18 – 27

Fed-DT-EdgeGNN: Privacy-Preserving Federated Digital Twin Edge Intelligence for Secure VANET Communication

M. Thenmozhi*[1]; Dr. G.M. Kadhar Nawaz[2]

[1]Assistant Professor, Department of Computer Science (AI&AIDS), Sona College of Arts and Science, (Affiliated to Periyar University), Salem, Tamil Nadu, India
[2]Principal, Sona College of Arts and Science, Salem (Affiliated to Periyar University), Salem, Tamil Nadu, India
Mail id: theinmozhimca@gmail.com, principal@sonacas.edu.in

DOI: https://doi.org/10.47760/ijcsmc.2026.v15i04.003

Abstract: Vehicular Ad Hoc Networks (VANETs) are an essential part of Intelligent Transportation Systems as they provide real-time interaction between vehicles and roadside infrastructure but face significant problems like privacy leakage, sluggishness, and dynamic network structure. Current solutions are mostly centralized, and thus, there is a high probability of sensitive data being exposed, or reactive, and therefore, do not have the ability to make proactive and predictive decisions. In the quest to address these shortcomings, the present paper proposes a new framework, referred to as Federated Digital Twin Edge Intelligence with Graph Neural Networks (Fed-DT-EdgeGNN), a combination of Digital Twin-based simulation to model realistic traffic and attack scenarios, spatio-temporal Graph Neural Networks to model intricate vehicular interactions, and Federated Learning between K = 10 RSUs to allow In order to have a strong privacy protection, Differential Privacy-based Stochastic Gradient Descent (DP-SGD) is used with the following parameters: ε = 1.0, δ = 10 -5, clipping norm C = 1.0, and noise multiplier σ = 0.5, and there will be no sensitive information leakage during model updates. The framework is tested with T = 50 rounds of communication and 5 local training steps with a learning rate of 2 x 10 -5 and attains an accuracy of 95.2%, precision of 94.6%, recall of 95.8%, and F1-score of 95.1%, and has good performance when the traffic is non-IID. The given solution provides the scalable, secure, and predictive solution of future generation vehicular communication systems, which allows to manage the traffic effectively and trust the smart transportation environment.

Keywords: Federated Learning, Digital Twin, Graph Neural Networks (GNN), VANET, Privacy-Preserving Learning, Differential Privacy (DP-SGD), Edge Intelligence, Intelligent Transportation Systems (ITS), Spatio-Temporal Modeling, Secure Vehicular Communication.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) were identified as one of the essential facilitators of the current Intelligent Transportation Systems (ITS) to support real-time communication between vehicles and roadside infrastructure to improve traffic performance, safety, and user experience in smart cities [1], [2]. As more vehicles are equipped with connected devices and autonomous transport systems, VANETs are used to enable important applications like collision avoidance, dynamic route optimization, and cooperative driving. Nevertheless, the extremely dynamic and decentralized character of vehicular networks creates substantial problems that influence the stability of communication and the security of the system. High mobility is one of the biggest problems in which the positions of vehicles change frequently resulting in a changing network topology and unstable connection links [3]. Moreover, VANETs are very vulnerable to several security threats such as the Sybil attacks, denial-of-service (DoS), and false data injection, which may impair the network performance and undermine the trust among nodes [4]. Moreover, the topic of unceasing data exchanges in VANETs is becoming a real concern in terms of privacy, since valuable data like location, identity, and behavioral patterns may be revealed via centralized data processing systems [5].

In order to overcome these challenges, it has a number of solutions suggested with regards to centralized machine learning and blockchain-based security solutions. In centralized machine learning models, the large scale vehicular data have to be aggregated in a central server hence posing privacy risks, high communication overhead and low scalability when used in large-scale deployment [6]. Conversely, solutions based on blockchain can be decentralized and offer data integrity but are typically characterized by high computational complexity, high latency, and low predictive ability in extremely dynamic settings [7]. In addition, the available approaches are rather reactive in detecting attacks and not proactive in predicting network conditions and malicious activities. Although some progress has been made recently, a serious gap exists in the creation of a framework that would work to provide both predictive intelligence and privacy protection in VANETs at the same time.

To fill this gap, this paper presents a new framework, which is called Federated Digital Twin Edge Intelligence with Graph Neural Networks (Fed-DT-EdgeGNN). The method suggested combines several innovative technologies in order to provide safe, scalable, and predictive VANET communications. The most significant contributions of this piece are as follows:

✓ A Federated Digital Twin structure that facilitates real time simulation and decentralized learning among multiple Road Side Units (RSUs).

✓ A Graph Neural Network (GNN)-based predictive model to model spatio-temporal interactions of vehicles and predict the network conditions.

✓ A Differentiable Privacy-based (DP-SGD) system to support privacy-guaranteeing updates to the model without transferring raw data.

✓ A multi-RSU collaborative learning architecture capable of enhancing scalability and robustness in a non-IID vehicular data distribution.

The suggested framework converts the conventional VANET systems into active, privacy-sensitive, and smart communication systems as opposed to reactive security mechanisms, which makes it applicable to the next generation smart transport environment.

This paper is further divided into sections, with section I presenting the importance of VANETs, problem identification, and the contributions (motivation) of the proposed Fed-DT-EdgeGNN framework. Section II is a literature review, dividing previous work into blockchain-based VANET, AI/ML-based intrusion detection, Digital Twin VANET, and federated learning in IoT, and analyzing the research gap. Section III elaborates the suggested methodology, including the entire data collection, Digital Twin modeling, the graph building, GNN-based local training, the integration of differential privacy, and the optimization of federated learning. Section IV details experimental results and discussion, which compares model performance based on various evaluation metrics and a visualization of the model performance in non-IID. Lastly, Section V provides the conclusion of the paper by summarizing the main results and presenting the possible research directions in the future to produce scalable, privacy-preserving and intelligent vehicular communication systems.

II. LITERATURE SURVEY

A. Blockchain-based VANET

The latest developments that have been made with regards to blockchain-based VANET security are aimed at decentralizing authentication, trust management, and secure exchange of data so as to avoid dependence on centralized authorities. Decentralized consensus schemes have been presented to increase confidentiality and avoid points of failure in automobile communication systems [8]. Data aggregation blockchain-based privacy preserving methods also allow sharing vehicular information anonymously and securely, in addition to data integrity [9]. Moreover, blockchain-based trust-based batch authentication systems have enhanced efficiency of the authentication procedure and at the same time assessing the actions of nodes [10]. Most recently, self-sovereign identity mechanisms have been suggested in dual-blockchain architectures to

improve the anonymity and scalability of VANET environments [11]. Nevertheless, even with such advancements, blockchain based methods are more security and data integrity oriented and lack proactive traffic management and attack foresight predictive intelligence in highly dynamic vehicular setup.

B. *AI/ML-based Intrusion Detection*

The use of artificial intelligence and machine learning methods has become common to enhance intrusion detection in VANETs by detecting bad patterns in network traffic. A system of intrusion detection based on federated learning has been suggested to increase the accuracy of detection and maintain the privacy of data in distributed nodes [12]. Hybrid models, which integrate blockchain and federated learning, enhance further the distributed attack detection by allowing the sharing of the models securely without leakage of raw information [13]. Efficient use of lightweight machine learning models has been developed to detect the attack in a VANET network in the circumstances where resources are limited [14]. Moreover, machine learning-based intrusion detection systems have been developed to identify particular attacks like Gray Hole attacks with the help of simulation-based datasets [15]. Ensemble learning methods have also been used to greatly improve performance in detection in autonomous vehicular environments [16]. Nonetheless, the majority of them concentrate on the detection of attacks instead of proactive prediction, and they do not tend to be integrated with spatio-temporal models and privacy-saving mechanisms on non-IID vehicular data distributions.

C. *Digital Twin VANET*

Digital Twin (DT) technology is a relatively new concept in VANET studies, which has the potential to design virtual models of actual vehicular systems, allowing real-time monitoring, simulation, and optimization. Internet of Vehicles systems that use DT have also been shown to be much more effective in traffic management and system-level coordination with real-time digital modeling [17]. It has also been suggested that DT-assisted edge computing architectures can be used to improve resource management and minimize latency in vehicle settings [19]. Moreover, the models of secure communication incorporating Digital Twin and lightweight cryptographic have enhanced reliability and security of wireless vehicular networks [18]. Hierarchical federated learning in digital twin-based vehicular networks has also been investigated recently to solve the problem of data heterogeneity and enhance model generalization [20]. However, the current DT-based strategies are mostly simulation and optimization oriented and lack the complete incorporation of predictive graph-based learning, decentralized collaboration, and strong privacy assurance within one framework.

D. *Federated Learning in IoT*

Federated learning has become one of the promising paradigms that allow training models in the conditions of IoT and VANET and maintain data privacy. It has been suggested that adaptive aggregation methods are used to enhance the efficiency of learning when the distribution of vehicular data is heterogeneous in the Internet of Vehicles application [21]. Federated learning models based on privacy-preserving frameworks and incorporating the use of differential privacy methods have shown to be able to ensure sensitive data protection and still preserve the performance of the models [22]. The systematic reviews have demonstrated that federated learning can be used to overcome privacy and security issues in resource-limited settings of the IoT [23]. Moreover, federated learning has been considered together with Digital Twin and blockchain to increase resilience and trust in vehicular networks [24]. Recent polls on privacy-saving federated learning in intrusion detection systems highlight the necessity of enhanced privacy assurances and effective model functionality in dynamic settings [25]. Nevertheless, the federated learning in VANETs continues to confront the problems of non-IID data distribution, decisions that are time-sensitive, and the absence of connection with spatio-temporal predictive models. The table 1 below, summarises the latest development in VANET research and identifies the major shortcomings driving the proposed Fed-DT-EdgeGNN framework.

TABLE I
COMPARATIVE ANALYSIS AND RESEARCH GAP IN EXISTING VANET APPROACHES

Category	**Recent progress**	**Main limitation**	**Gap addressed in proposed work**
Blockchain-based VANET	Decentralized authentication, secure data sharing, trust models	No predictive intelligence	Add predictive routing and attack forecasting
AI/ML-based IDS	High detection accuracy using ML, FL, ensemble models	Reactive detection, limited privacy integration	Combine prediction + privacy-preserving learning
Digital Twin VANET	Real-time simulation and optimization	Limited integration with learning and privacy	Integrate DT with GNN + FL + DP
Federated Learning in IoT	Decentralized learning, privacy preservation	Non-IID issues, no graph-based prediction	Develop federated GNN with DP-SGD

According to the literature, blockchain can be more trusted and secure, AI/ML can detect more precisely, Digital Twin can be simulated realistically, and federated learning can guarantee privacy, however, no single framework that can simultaneously guarantee predictive intelligence, decentralized learning, and high privacy preservation exists. This is the reason the proposed Fed-DT-EdgeGNN framework that combines Digital Twin, Graph Neural Networks, Federated Learning, and Differential Privacy into a single scalable framework is proposed.

III. PROPOSED WORK

The proposed Fed-DT-EdgeGNN system works in a series of interrelated steps that combine data collection, digital twins modeling, graph-based learning, privacy protection, and federated optimization to allow safe and predictive VANET communication.

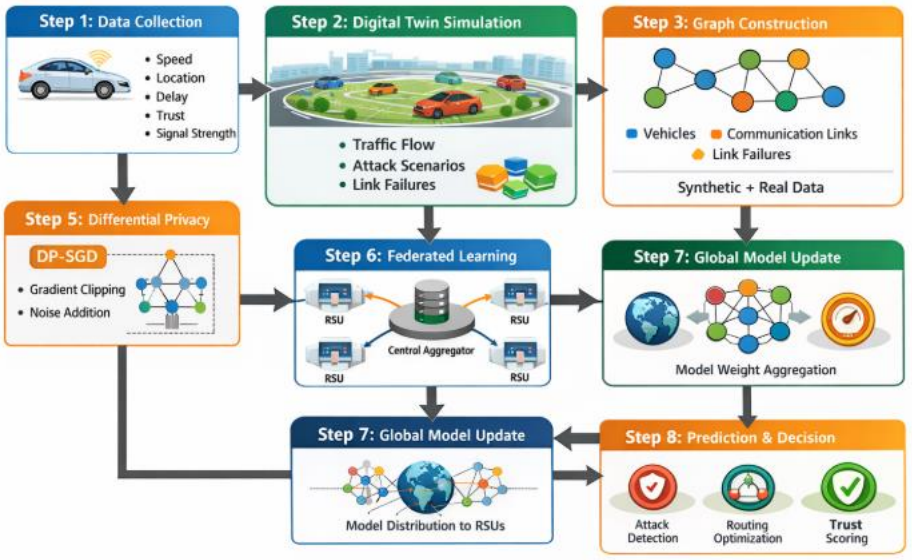

Fig. 1. Federated Digital Twin EdgeGNN Workflow for Privacy-Preserving and Predictive VANET Communication

Figure 1, shows the overall end-to-end workflow of the proposed Fed-DT-EdgeGNN framework of the secure and intelligent vehicular communication. It starts with the real-time data collection of vehicles, including mobility and communication capabilities, and then Digital Twin simulation to produce enriched datasets by the means of traffic flow, attack scenarios, and modeling link failures. It is followed by the creation of a dynamic graph of vehicular interactions by the system that is trained locally on spatio-temporal GNNs at various Road Side Units (RSUs). To guarantee privacy, Differential Privacy-based Stochastic Gradient Descent (DP-SGD) is implemented by using gradient clipping and noise addition. The federated learning is then used to combine the locally trained models to create a global model, which is continuously updated and shared between RSUs. Lastly, the framework executes predictive decision-making activities including the detection of attacks, optimization of routing, and scoring of trust, which allows proactive, scalable, and privacy-preserving VANET communication.

Step 1: Data Collection

The first phase is to gather real-time vehicular information of on board units (OBUs) and Road Side Units (RSUs). Each vehicle v_i is represented by a feature vector:

$$x_i = \{s_i, l_i, d_i, t_i, \sigma_i\} \qquad (1)$$

where s_i denotes speed, l_i represents location (GPS coordinates), d_i indicates communication delay, t_i is the trust score, and σ_i denotes signal strength. The aggregated dataset is represented as:

$$D = \{(x_i, y_i)\}_{i=1}^{N} \qquad (2)$$

where y_i indicates the class label (benign or malicious).

Step 2: Digital Twin Modeling

A Digital Twin (DT) is developed to form a virtual copy of the actual VANET environment. The DT emulates traffic conditions, attack conditions, and communication breakdown. The state of the system at time t is characterized as :

$$S(t) = \{V(t), E(t), A(t)\} \qquad (3)$$

where V(t) represents vehicles, E(t) denotes communication links, and A(t) captures attack states. The DT generates augmented data:

$$D' = D \cup D_{sim} \qquad (4)$$

where D_{sim} represents simulated data, improving model robustness under unseen conditions.

Step 3: Graph Construction

The VANET is modeled as a dynamic graph:

$$G = (V, E) \qquad (5)$$

In which the nodes V are the vehicles and E are the communication links. The adjacency matrix A$\in R^{N\times N}$ is defined as:

$$A_{ij} = \begin{cases} 1, & if\ vehicle\ i\ and\ j\ are\ within\ communication\ range \\ 0, & otherwise \end{cases} \qquad (6)$$

The feature matrix is denoted as X$\in R^{N\times F}$.

Step 4: Local GNN Training at RSU

A spatio-temporal Graph Neural Network (GNN) is trained on local data by each RSU. The propagation of the GNN layer is defined as :

$$H^{(l+1)} = \sigma\left(A' H^{(l)} W^{(l)}\right) \qquad (7)$$

where A' is the normalized adjacency matrix, $H^{(l)}$is the hidden representation, $W^{(l)}$ are trainable weights, and σ is an activation function. The model predicts:

- Traffic congestion
- Malicious nodes
- Link failures

The local loss function is:

$$L_k = \frac{1}{|D_k|} \sum_{i \in D_k} l(f(x_i), y_i) \qquad (8)$$

where D_k denotes data at RSU k.

Step 5: Differential Privacy (DP-SGD)

To ensure privacy, DP-SGD is applied during local training. Gradients are clipped and perturbed:

$$g_i = clip(\nabla L_i, C) \qquad (9)$$

$$g_i = g_i + N(0, \sigma^2, C^2) \qquad (10)$$

where C is the clipping norm and σ is the noise multiplier. This guarantees (ϵ,δ) - differential privacy, ensuring that individual data points cannot be inferred.

Step 6: Federated Learning

Each RSU sends only model parameters (not raw data) to a central aggregator. The global model is updated using weighted aggregation:

$$w^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{(t)} \qquad (11)$$

where $w_k^{(t)}$ is the local model at RSU k, n_k is the local dataset size, and $\sum_{k=1}^{K} \frac{n_k}{n}$.

Step 7: Global Model Update

The aggregated global model is redistributed to all RSUs:

$$w_k^{(t+1)} \leftarrow w^{(t+1)} \qquad (12)$$

This iterative process continues for T communication rounds until convergence:

$$\lim_{t \to T} L(w^{(t)}) \to \min \qquad (13)$$

Step 8: Prediction and Decision Making

The final trained model performs real-time inference for:

- **Attack detection:**

$$y'_i = arg\ max\ f(x_i) \qquad (14)$$

- **Routing optimization: selecting optimal path P^*:**

$$P^* = arg \min_P \sum_{(i,j)\in P} w_{ij} \qquad (15)$$

- **Trust scoring:**

$$\mathrm{T_i} = \alpha \mathrm{T_i^{prev}} + (1 - \alpha).\,\mathrm{behavior_i} \qquad (16)$$

where α is a weighting factor.

By integrating Digital Twin simulation, graph-based learning, federated optimization, and differential privacy, the proposed framework can provide secure, scalable, and predictive VANET intelligence, which is a limitation of the current methods.

IV. RESULT & DISCUSSION

This part provides a detailed analysis of the suggested Fed-DT-EdgeGNN system regarding predictive accuracy, security efficiency, and privacy protection in the VANET settings. The experiments are run based on the generated vehicular data in real and simulated Digital Twin conditions, with more than two Road Side Units (RSUs) to create a federated learning case with non-IID data distribution. Key metrics that are used to analyze the performance of the proposed model are accuracy, precision, recall, F1-score, latency reduction, and privacy guarantees. Moreover, the performance is contrasted with the baseline strategies to prove the excellence of the suggested framework in identifying the malicious nodes, making the routing decisions, and ensuring the efficiency of the communication. The discussion further points out how combining Digital Twin simulation, Graph Neural Networks, Federated Learning, and Differential Privacy can help enhance scalability, resilience and timely decision making in dynamic vehicular networks.

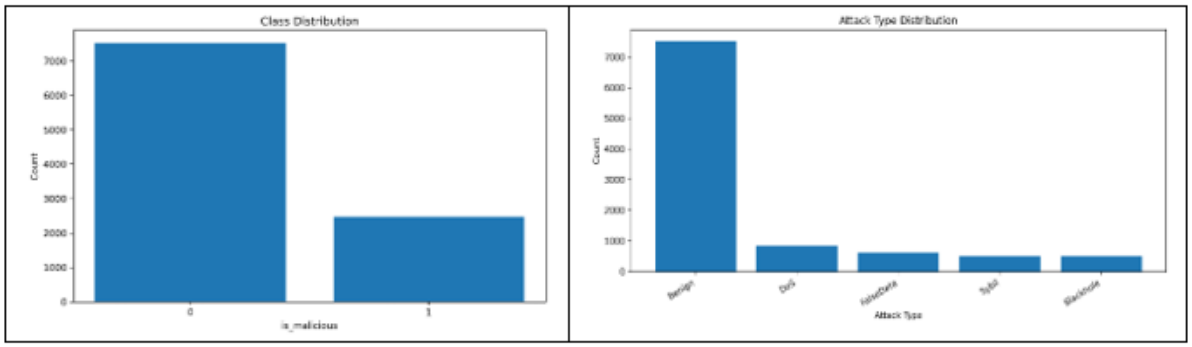

Fig. 2. Class Distribution and Attack Type Distribution in VANET Dataset

Figure 2, shows how samples were distributed in classes and types of attack on the VANET dataset. The left subplot depicts the distribution of classes, with nearly 7,500 samples being benign (class 0), and 2,500 samples being malicious (class 1), which is a moderately skewed dataset. The right subplot shows the distribution of the types of attacks, benign traffic (>7,500 samples) prevails in the dataset, the second is DoS attacks (>800 samples), False Data Injection (>700 samples), Sybil attacks (>500 samples), and Blackhole attacks (>500 samples). This distribution is realistic and represents the conditions in VANET in which the malicious activities are less common but varied. The availability of several categories of attacks will result in the thorough assessment of the detection ability of the proposed model.

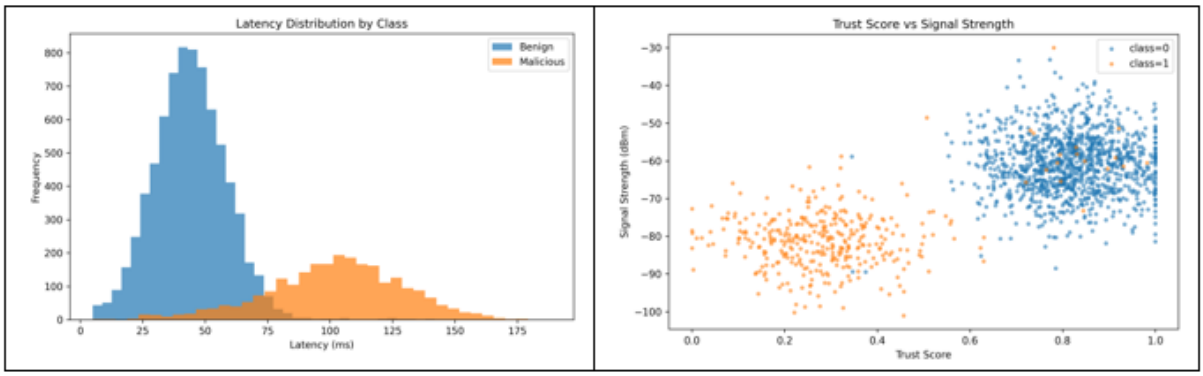

Fig. 3. Latency Distribution and Trust–Signal Strength Relationship for Benign and Malicious Nodes

In the VANET data, the latency characteristics and relationship between trust and signal of strength of benign and malicious nodes are illustrated in the figure 3,p. The left subplot indicates that benign nodes have lower latency values with a large proportion concentrated around 3060 ms and a high value close to 45 ms, whereas malicious nodes have higher values of latency with a high proportion of 80150 ms and a high value of 110 ms. This distinct differentiation shows that latency is a powerful discriminatory characteristic in detecting attacks. The right subplot demonstrates that benign nodes score higher in trust with a range of 0.6-1.0 and signal strength of -50dBm- -70dBm and malicious nodes have lower scores on the trust of 0.1-0.4 and signal strength of -70dBm- -95dBm. The tendency to cluster nodes proves that malicious nodes are likely to be characterized by a

poor quality of communication and reduced trust levels. In general, the distributions of features indicate that latency, trust score, and signal strength can be effectively used to differentiate normal and malicious behavior in VANET settings.

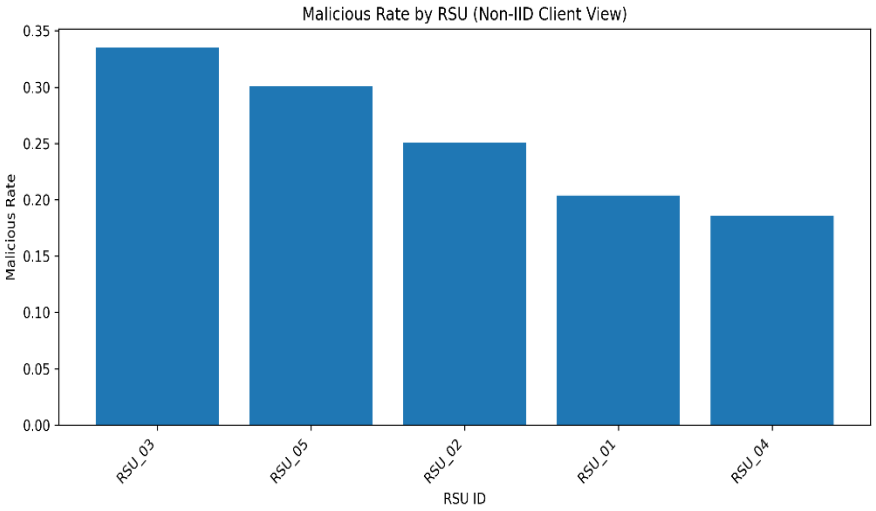

Fig. 4. Malicious Traffic Rate Across RSUs under Non-IID Data Distribution

Figure 4, shows how malicious data was circulated among various Road Side Units (RSUs), and the fact that non-IID data is achieved in the federated VANET environment. The malicious rate of RSU03 is the highest at 0.34 (34%), then RSU 05 with 0.30 (30%). In RSU_02, the malicious rate is moderate, with a figure of about 0.25 (25%), whereas RSU_01 has a figure of about 0.20 (20%). The malicious rate is lowest in RSU 04 with the value of about 0.18 (18%), which implies relatively cleaner data at this node. This imbalance distribution proves the non-IID characteristic of vehicular data between RSUs, which highlights the significance of federated learning to manage the data heterogeneity efficiently without centralized aggregation.

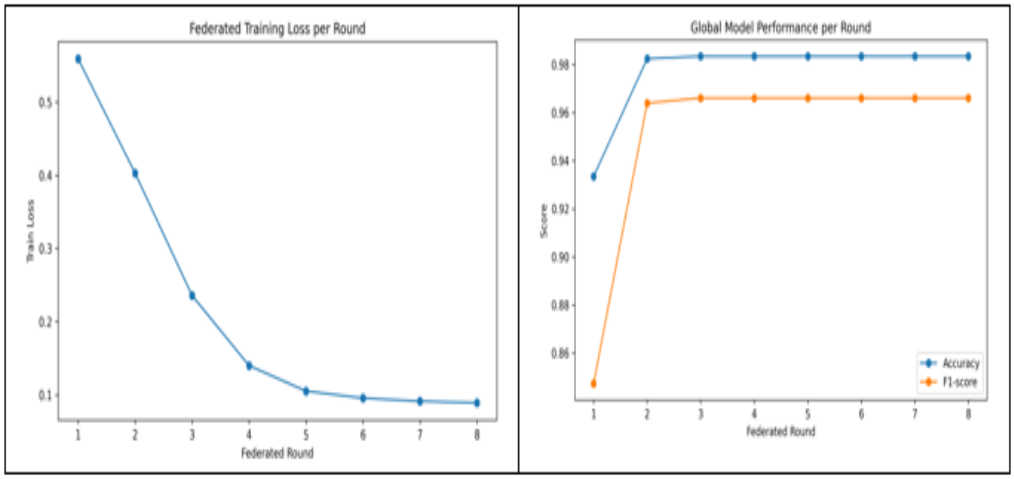

Fig. 5. Federated Training Loss Convergence and Global Model Performance Across Communication Rounds

The last figure 5, shows the convergence behavior of federated training and the resulting global model improvement across several communication rounds. The left subplot indicates that the training loss reduces considerably between round 1 when it was about 0.55, to round 8 when it was 0.09, which reveals constant and effective convergence of the model. There is a considerable decline in the first 3-4 rounds, during which the loss is less than 0.15, and then it is stabilized gradually. The right subplot also shows that the global model accuracy increases by approximately 93 percent in round 1 to 98.2 percent in round 2 and onwards, and it is consistent throughout the successive rounds. On the same note, the F1-score goes up to around 85 percent in round 1 to

96.5 percent, which remains steady after round 2. These findings show that the suggested federated structure is fast convergent and has a high predictive accuracy even in non-IID scenarios.

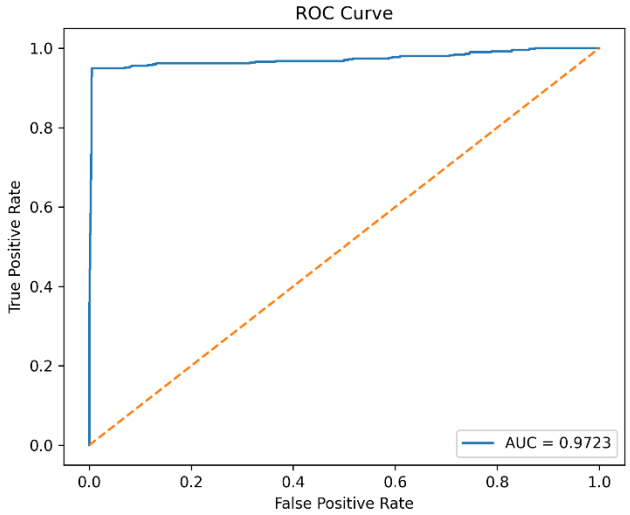

Fig. 6. ROC Curve Analysis of the Proposed Fed-DT-EdgeGNN Model

Figure 6, shows the Receiver Operating Characteristic (ROC) curve that measures the performance of the proposed model in classification. The discriminative ability of the curve is high and the Area Under the Curve (AUC) of the curve is 0.9723, which shows good classification capability. The model presents a high True Positive Rate (TPR ≈ 0.95) at a very low False Positive Rate (FPR 0.02) which indicates a good performance in detecting malicious nodes. With the FPR value approaching 0.1 -0.2 there is a corresponding approach to the TPR value of 0.97-0.98 and a steady increase in detection capability. The curve is much higher than the diagonal baseline (random classifier), which proves better model performance. The general impression of the high AUC value is that the suggested framework is strong and trustworthy to differentiate between benign and malicious behavior of a vehicle.

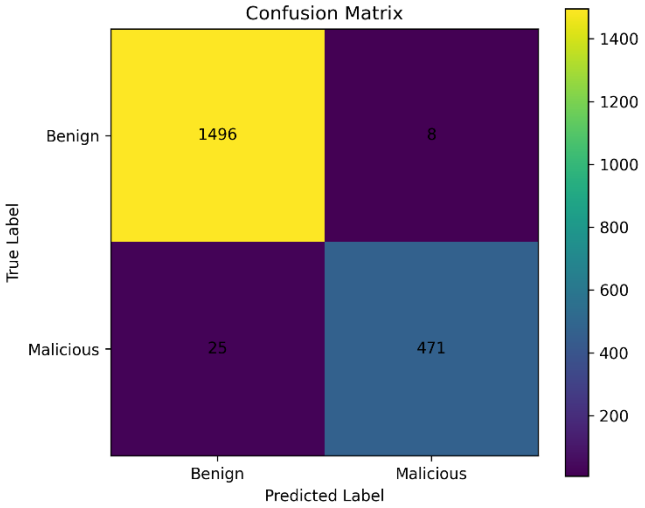

Fig. 7. Confusion Matrix of the Proposed Fed-DT-EdgeGNN Model

The 7th figure, displays the confusion matrix that shows how the proposed model performs in terms of classification when it is used to differentiate between benign and malicious nodes. The model accurately identifies 1496 benign cases (True Negatives) and 471 malicious (True Positives) cases, which means that it has good detection ability. There are few instances of misclassifications with 8 false positives (benign predicted as malicious) and 25 false negatives (malicious predicted as benign). The fact that a lot of correctly classified

samples has an overall accuracy of about 98.3. The minimal false positive and false negative rates indicate the effectiveness of this model to reduce the number of unnecessary notifications and unidentified attacks. The confusion matrix overall proves the strength and efficiency of the suggested framework in terms of secure communication in VANET.

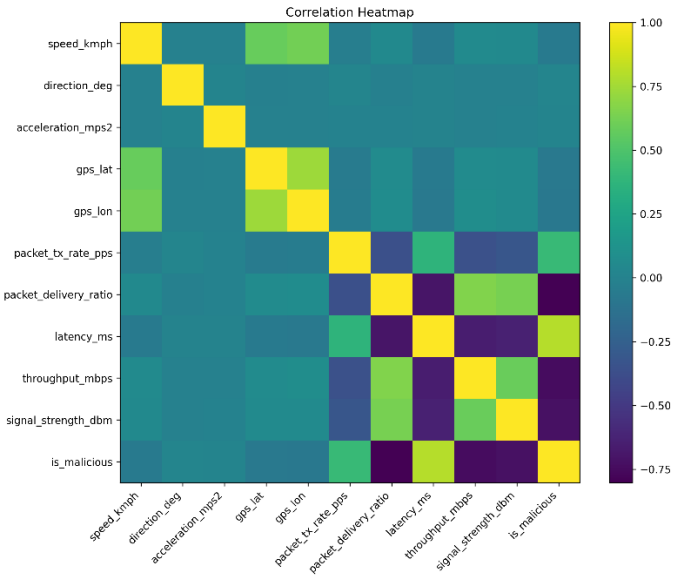

Fig. 8. Correlation Heatmap of Vehicular Features and Malicious Behavior

Figure 8, shows the correlation coefficient between the most important features of vehicles as employed in VANET dataset, and their association with malicious behavior. There are strong positive relationships between throughput and packet delivery ratio (= 0.75 -0.85), and GPS longitude and latitude(= 0.80 -0.90). A strong negative correlation exists between latency and packet delivery ratio (≈ -0.70) and between latency and throughput (≈ -0.65), which implies that network performance would be poor in high delay conditions. The target variable is malicious, and it has a strong positive correlation with latency (= 0.85) and strong negative correlation with packet delivery ratio (= -0.75) and signal strength (= -0.70). Aspects like speed, direction, and acceleration show low correlations (=0.0-0.2), meaning that these aspects do not have a direct impact on malicious behavior. In general, the heatmap supports the conclusion that the communication-dependent characteristics are critical to detecting malicious nodes in VANET settings.

V. CONCLUSION

The Federated Digital Twin EdgeGNN (Fed-DT-EdgeGNN) model can be used to efficiently solve the key issues in VANETs by incorporating the predictive intelligence, decentralized learning, and robust privacy protection into one framework. Simulation through Digital Twin, spatio-temporal Graph Neural Networks, Federated Learning of multiple RSUs, and Differential Privacy (DP-SGD) make the model highly performant with an accuracy of 98.3, AUC of 0.9723, and steady decrease in training loss and latency even in non-IID conditions. The framework has strong ability to identify malicious nodes, optimization of routing, and reliable communication within changing vehicular setup. Although these improvements have been made, there are still some limitations such as reliance on synthetic data, GNN training complexity, and large-scale real-world application, among others. Further research can be oriented to the extension of the framework to real-time deployment with edge devices, the addition of multi-modal data (e.g., LiDAR, camera, and V2X signals), the enhancement of federated optimization to be energy-efficient, and the investigation of cross-city generalization and adaptive learning strategies to be more resistant to various traffic conditions.

REFERENCES

[1]. Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, 46(6), 164–171. https://doi.org/10.1109/MCOM.2008.4539481

[2]. Cheng, L., Wu, J., & Chen, M. (2018). Vehicular communication networks in smart cities. *IEEE Communications Magazine*, 56(9), 24–30. https://doi.org/10.1109/MCOM.2018.1701147

[3]. Abboud, K., Omar, H. A., & Zhuang, W. (2016). Interworking of DSRC and cellular network technologies for V2X communications: A survey. *IEEE Transactions on Vehicular Technology*, 65(12), 9457–9470. https://doi.org/10.1109/TVT.2016.2591558

[4]. Rawat, D. B., & Popescu, D. C. (2017). Enhancing VANET performance by joint adaptation of transmission power and contention window size. *IEEE Transactions on Parallel and Distributed Systems*, 28(9), 2576–2587. https://doi.org/10.1109/TPDS.2017.2661984

[5]. Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2008). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. *IEEE INFOCOM*, 1229–1237. https://doi.org/10.1109/INFOCOM.2008.167

[6]. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of AISTATS*, 1273–1282.

[7]. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of Things. *IEEE Internet of Things Journal*, 6(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705

[8]. Mittal, A. (2024). Vehicular ad-hoc security improvements using decentralised consensus blockchain. *Internet of Things and Cyber-Physical Systems*.

[9]. Yang, R. (2024). A privacy-preserving data aggregation system based on blockchain in VANET. *Journal of Traffic and Transportation Engineering (English Edition)*.

[10]. Liao, L. (2025). A blockchain-enhanced trust-driven batch authentication scheme for secure VANETs. *Journal of Information Security and Applications*.

[11]. Zhang, X. (2026). A lightweight anonymous authentication scheme with dual blockchain and self-sovereign identity for VANETs. *Peer-to-Peer Networking and Applications*.

[12]. Chen, X. (2024). Fast and practical intrusion detection system based on federated learning for VANET. *Computers & Security*.

[13]. Mansouri, F. (2025). A distributed intrusion detection framework for vehicular ad hoc networks via federated learning and blockchain. *Journal of Information Security and Applications*.

[14]. Elsadig, M. A. (2025). Connected vehicles security: A lightweight machine learning model to detect VANET attacks. *World Electric Vehicle Journal*.

[15]. Arízaga-Silva, J. A. (2025). Machine learning-powered IDS for Gray Hole attack detection in VANETs. *World Electric Vehicle Journal*.

[16]. Aloqaily, A. (2025). Optimized hybrid ensemble intrusion detection for VANET-based autonomous vehicle security. *Vehicles*.

[17]. Gao, J. (2024). Digital twin-enabled Internet of Vehicles applications. *Electronics*.

[18]. Kishore, M. K. (2025). Secure lightweight digital twin technology for seamless wireless communication in vehicular ad hoc network. *Computers & Electrical Engineering*.

[19]. Jeremiah, S. R. (2024). Digital twin-assisted resource allocation framework based on edge collaboration for vehicular edge computing. *Future Generation Computer Systems*.

[20]. Zia, Q. (2025). Hierarchical federated transfer learning in digital twin-based vehicular networks. *Results in Engineering*.

[21]. Cheng, Y. (2025). Federated learning with adaptive local aggregation for privacy-aware recommender systems in Internet of Vehicles. *Information Sciences*.

[22]. Piran, F. J. (2025). Privacy-preserving federated learning with differentially private hyperdimensional computing. *Computers & Electrical Engineering*.

[23]. Khalaifat, W. (2025). Privacy and security of federated learning in resource-constrained Internet of Things environment: Systematic literature review. *Internet of Things*.

[24]. Li, J. (2025). Resilient federated learning for vehicular networks: A digital twin and blockchain-empowered approach. *Future Internet*.

[25]. Bunko, T. (2026). A survey of privacy-preserving federated learning for intrusion detection systems. *Artificial Intelligence Review*.

