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. 3, March 2026, pg.81 – 90

DT-EdgeGNN: Digital Twin–Driven Edge Intelligence with Graph Neural Networks for Predictive 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.v15i03.009

Abstract: An edge intelligence-based predictive and secure communication framework Vehicular Ad Hoc Networks (VANETs) is offered based on Digital Twin (DT)-compliant Edge Intelligence (EdgeGNN). In traditional VANET there is reactive intrusion detection and centralized processing that is not able to deal with high mobility, dynamic topology and latency. The proposed solution to such obstacles ensures that the digital twin layer of real-time traffic simulation and attack case, the spatio-temporal Graph Neural Network (GNN) of vehicle interaction, and the edge intelligence layer at Right Side Unit (RSUs) are integrated to make decisions on a low-latency basis. A small blockchain system that has dynamic trust scores is embedded to guarantee safe and trustworthy communication. The framework anticipates link failure, congestion, and malicious behavior of nodes, which are created to be able to facilitate proactive routing and mitigate attacks. The results of the experiments show that the accuracy is 93.4, the attack detecting rate (0.72) is better, false positive rate (0.13) is lower and the network is much better in terms of latency and throughput. The suggested DT-EdgeGNN model can efficiently transform VANET communication into proactive management and predictive instead of reactive monitoring, which is appropriate in the next-generation advanced transportation systems.

Keywords: Vehicular Ad Hoc Networks (VANETs), Digital Twin, Edge Intelligence, Graph Neural Networks (GNN), Spatio-Temporal Modeling, Predictive Routing, Blockchain Security, Intrusion Prevention, Adaptive Trust Management, Intelligent Transportation Systems (ITS).

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have become a cornerstone of Intelligent Transportation Systems (ITS), which provides vehicles and roadside infrastructure to support real-time communication between vehicles and roadside infrastructures in order to enhance road safety, traffic performance, and the user experience [1]. As connected vehicles and the future of smart cities rise to prominence, VANETs are currently confronted with more dynamic network states in terms of high mobility, topology, and heterogeneous data streams [2]. These features, however, come with great challenges concerning latency, scalability, reliability and most importantly, security.

Conventional VANET systems are largely based on centralized architecture and reactive intrusion detection system which has not been sufficient in countering the contemporary cyber attack of the Sybil attacks, Denial-of-Service (DoS), and false data injection [2]. Such strategies normally identify malicious acts after they have been executed and as such, responses are delayed leading to possible network degradation. Moreover, machine learning-based methods tend to be less predictive and fail to infer complex spatio-temporal relationships present in vehicular communication data because of the complexity of the latter [4].

The recent blockchain technology has provided solutions to the privacy and security of data exchange in VANETs through decentralization and tamper resistance [5]. Blockchain allows management of trust, authentication, and integrity of data without the involvement of centralized authorities. Nonetheless, the current blockchain-based VANET models have high computational complexity, scalability, and low integration with intelligent prediction models [6]. Equally, the advent of Agentic Artificial Intelligence has enhanced decision making attributes within distributed systems, but even the processes do not have a proven predictive insight and timely responsiveness when implemented in highly dynamic vehicular network [7].

Moreover, Edge computing has become a powerful facilitator to real-time processing of data by moving computation and data sources together, say, Road Side Units (RSUs), which makes latency shorter and reliance on centralized cloud infrastructures less significant. It is shown to be faster and more efficient due to integration of edge intelligence with predictive learning models which is crucial in safety-critical vehicular applications[8].

Due to these developments, this paper suggests a Digital Twin-powered Edge Intelligence model with Graph Neural Networks (DT-EdgeGNN) to predictive and safe VANET communication. The suggested framework combines the simulation of Digital Twin-based simulation, spatio-temporal GNN modelling, edge-based decision-making, and lightweight blockchain processes to support proactive intrusion prevention, adaptive routing, and secure data transmission. With prediction and security, the paradigm is transformed into active and proactive network management, and no longer reactive detection.

Provide the key contribution to the proposed work:

- Digital Twin-based VANET modeling that allows real-time simulation of traffic dynamics and attack scenarios, which facilitates the proactive analysis of the network.
- Graph Neural Network (GNN) framework spatial-temporal to indicate link failures, congestion, and malicious node actions in changing vehicular surroundings.
- Decision system by using edge intelligence at RSUs in low-latency, real-time routing and security measures without dependence on the cloud.
- Lightweight blockchain and adaptive trust scoring based on hybrid predictive security framework to achieve secure, scalable, and proactive VANET communication.

Section II is a review of the available VANET frameworks such as blockchain-based security models, machine learning, and recent breakthroughs in edge intelligence and graph-based techniques, the strengths and weaknesses of each. Section III provides the description of the proposed DT-EdgeGNN structure and explains how Digital Twin modeling is integrated with spatio-temporal Graph Neural Networks, edge intelligence at RSUs, predictive routing, and blockchain-based trust management. Section IV addresses the experimental findings, such as the performance analysis in the light of accuracy, latency, throughput, and security metrics, and also a comparison of the results to the existing VANET models. Lastly, Section V decides the work with an overview of the main findings and the perspectives of future research to the practical purpose of scalable, real-time and completely autonomous vehicular communication systems.

II. LITERATURE SURVEY

The proposal of Li et al. (2023) [9] was a blockchain-enabled digital twin vehicular edge network to offload tasks securely: digital twins track communication, computation, and caching resources in real time and blockchain secures offloading transactions, which is decentralized. It has a robust method of minimizing joint latency and energy consumption by cooperating with edges and smart contracts, yet it is concerned with the efficiency in offloading, not in proactive threat detection or graphical modeling in vehicular behavior.

Jeremiah et al. (2024) [10] designed a digital twin-based resource allocation system of vehicular edge computing based on edge collaboration and RSU association. Their model can be successfully used to reduce the time taken to complete the tasks and enhance throughput by collectively optimizing offloading, channel

allocation and selection of the RSU. Nevertheless, network optimization is the focus of the study, and there is no direct modeling of cyberattacks, trust adaptation, and secure predictive routing.

Chai et al. (2024) [11] proposed a lightweight blockchain powered by a digital twin to work with dynamically operating Internet of Vehicles. The technique minimizes the cost of communication and operational time of blockchain in very mobile environments, which is useful in vehicles that need real-time interactions. The primary strength of it in efficient blockchain synchronization with dynamic topology, however, the framework does not pay much attention to smart attack prediction and lacks the use of spatio-temporal graph learning to make mobility-informed predictions.

In [12] Jamil et al. offered a lightweight zero-trust framework of the secure communication of 5G VANET. What is appealing about the model is that it enhances the authentication and access control and also fits the low-latency vehicular communication. It is largely policy-driven with its key contribution being better handling of trust in modern 5G-VANET environments, but it lacks the simulation of digital twins along with learning-based predicting of congestion and link-failures.

The article of Ahmed et al. (2024) [13] suggested a federated version of Q-learning to VANETs with EX-ECC, IPFS, and delegated Byzantine fault tolerance and applied blockchain. The framework is advantageous in terms of the fact that it integrates decentralized learning and safe coordination, which facilitates the process of making decisions at scale in vehicular settings. Nevertheless, control based on reinforcement might not be adequate to capture the structural relationships among vehicles and the approach does not directly construct graph representations to predict dynamic topologies.

In Zhang et al. (2024) [14], feature reduction and efficient learning are related to the creation of an intrusion detection model of the IoV based on GRIPCA and OWELM. The approach is efficient in terms of computations and classification accuracy than traditional baselines and is applicable to resource-limited vehicular systems. Nevertheless, it is based on tabular learning of features and thus it cannot fully made use of dynamic node-to-node interaction patterns on VANET graphs.

The article by Fu et al. (2025) [15] proposed the use of the IoV-BERT-IDS, a hybrid intrusion detection solution which uses a BERT-like large-model architecture to process IoV traffic. This model is beneficial since it has more traffic semantic and it is more general to heterogeneous intrusion patterns. It has a weakness in the fact that semantic sequence learning itself does not implicitly encode spatial relationships between vehicles and RSUs, which are key to link prediction and a routing decision in a VANET.

One of them is DT-LHBC, a safe lightweight digital twin hashing-blockchain cryptography framework of VANETs, proposed by Kishore et al. (2025) [16]. It is remarkable that the research integrates digital twins and lightweight cryptography in ensuring communication integrity against attacks like replay, jamming and Sybil-like behavior. Although the framework reinforces safe transmission, the framework is more cryptography-based than intelligence-based and lacks edge-based predictive learning and graph awareness mobility analysis.

A secure MEC model of VANETs is designed using hybrid networks by Goud et al. (2025) [17] through blockchain networks. The key advantage of this work is that it offers multi-layer security in supporting communication between vehicles and edge servers that enhance safeguarded information exchange in MEC-enabled vehicular systems. Simultaneously, the research focuses mainly on secure MEC work and fails to bring together digital twin-based what-if simulation and GNN-propagated attack or congestion forecasting.

Wang et al. (2025) [18] developed a BS-GAT, a graph attention network, which is applied in intrusion detection in edge computing where learning is supported by the similarity of behavior to construct a graph and the weighted edge relationship. This publication is particularly applicable as it demonstrates that graph-based modeling may be used to out-perform traditional intrusion detection, and results are high in terms of binary and multi-class classification. However, it does not focus on mobility-aware VANET digital twins but general edge-network intrusion detection, and routing control and blockchain-based trust adaptation is not fostered. Table I provides the summary of the recent VANET approaches and compares their methodologies, strengths, and limitations to determine the gap in the existing research and encourage the proposed DT-EdgeGNN framework.

TABLE I.
COMPARATIVE ANALYSIS OF RECENT DIGITAL TWIN, AI, AND BLOCKCHAIN-BASED VANET FRAMEWORKS

Sno.	Author et al. (Year)	Methodology	Main advantage	Main limitation
[1]	Li et al. (2023)	Blockchain-enabled digital twin vehicular edge network with improved cuckoo optimization for offloading	Reduces network cost, latency, and energy through edge cooperation	Focused on offloading, not predictive security or graph intelligence
[2]	Jeremiah et al. (2024)	DT-assisted edge collaboration for vehicular edge resource allocation	Improves throughput and task completion delay	Limited treatment of attacks and trust dynamics
[3]	Chai et al. (2024)	DT-empowered lightweight blockchain for dynamic IoV	Lowers blockchain latency and communication overhead	Lacks spatio-temporal attack prediction
[4]	Jamil et al. (2024)	Lightweight zero-trust framework for secure 5G VANET communication	Strong authentication and secure access for low-latency networks	No digital twin or GNN-driven prediction

[5]	Ahmed et al. (2024)	Blockchain-enabled federated Q-learning with EX-ECC and IPFS	Supports decentralized secure learning and coordination	Does not model vehicular topology as graphs
[6]	Zhang et al. (2024)	GRIPCA-based feature reduction with OWELM intrusion detection	Efficient and accurate attack classification	Limited relational modeling of vehicle interactions
[7]	Fu et al. (2025)	BERT-based hybrid IoV intrusion detection	Learns rich traffic semantics and improves generalization	Weak in explicit spatial/graph relationship learning
[8]	Kishore et al. (2025)	DT-LHBC secure lightweight hashing-blockchain cryptography	Enhances secure wireless communication with lightweight protection	More cryptographic than predictive
[9]	Goud et al. (2025)[19]	Blockchain-based secure MEC model for VANETs using hybrid networks	Strong secure communication between vehicles and edge servers	No unified DT + GNN + routing framework
[10]	Wang et al. (2025)[20]	BS-GAT graph attention–based intrusion detection	Strong graph-based detection performance	Built for edge intrusion detection, not full VANET predictive control

Current VANET architectures are characterized by ineffective and disconnected solutions in which security, prediction, and network optimization are not coordinated and results in slow intrusion response, failure to capture dynamic vehicle interactions, high latency through cloud dependency, and an inability to take proactive decisions in highly mobile situations. Also, the traditional models do not model spatio-temporal relationships and cannot predict effectively link failures, congestion and propagation of attacks. To solve these shortcomings, the proposed DT-EdgeGNN architecture comprises the Digital Twin-based simulation of real-time scenarios, the use of spatio-temporal Graph Neural Networks to predict network responses, edge intelligence at RSUs to make decisions with low-latency, and a lightweight blockchain with variable trust scoring to establish secure communication. The resulting combined solution can be used to help transition to proactive prediction and optimization rather than reactive detection to enhance reliability, scalability, and security in next-generation VANET systems.

III. PROPOSED WORK

The suggested DT-EdgeGNN architecture will be able to deliver predictive, secure, and low-latency communication in Vehicular Ad Hoc Networks (VANETs) by incorporating Digital Twin modeling, spatio-temporal Graph Neural Networks, edge-based intelligence, predictive routing, and lightweight blockchain-managed trust. The proposed framework anticipates the occurrence of such events ahead of time, unlike the traditional VANET systems that respond once any of the given factors (congestion, link degradation, or attacks) happen and implement a preventive measure only at the Road Side Unit (RSU) edge layer. The overall procedure includes the data collection, pre-processing, simulation of a digital twin, the dynamic graph development, spatio-temporal forecasting, adjudgment of edges, routing based on the trust, blockchain-based communication that is securable. Figure 1 shows the overall workflow of the DT-EdgeGNN architecture, which involves simulation of digital twins, graphical prediction, edge intelligence, and blockchain security in proactive VANET management.

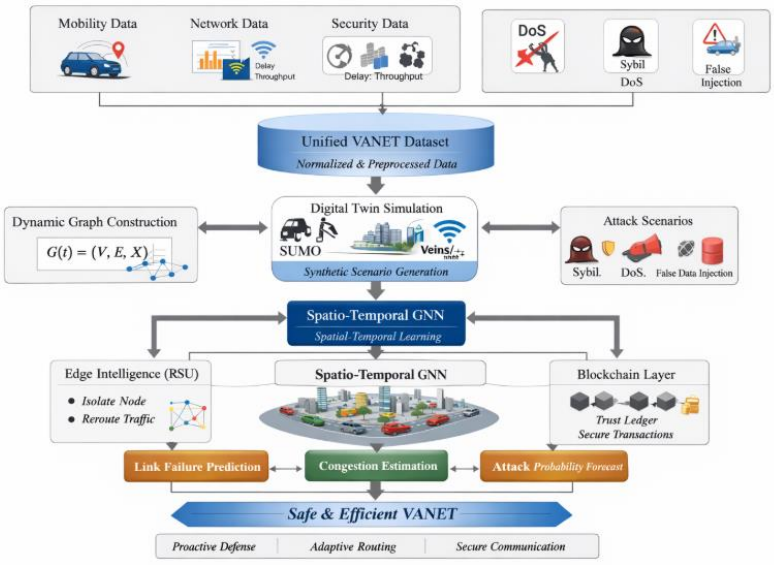

Fig. 1. Architecture of the Proposed DT-EdgeGNN Framework for Predictive and Secure VANET Communication

The input VANET dataset at time t is represented as

$$D(t) = \{n_i(t)\}_{i=1}^{N} \quad (1)$$

where N is the number of vehicles and each node record is defined as

$$n_i(t) = [x_i(t), y_i(t), v_i(t), \theta_i(t), p_i(t), d_i(t), th_i(t), ss_i(t), tr_i(t), a_i(t)] \quad (2)$$

Here, $x_i(t)$ and $y_i(t)$ denote the spatial coordinates of vehicle iii, $v_i(t)$ denotes speed, $\theta_i(t)$ denotes direction, $p_i(t)$ represents packet delivery ratio, $d_i(t)$ denotes communication delay, $th_i(t)$ denotes throughput, $ss_i(t)$ represents signal strength, $tr_i(t)$ is the trust value, and $a_i(t)$ is the attack label.

To eliminate scale imbalance among heterogeneous vehicular features, Z-score normalization is first applied. For a feature fff, the normalized value is

$$z_i^{(f)} = \frac{x_i^{(f)} - \mu_f}{\sigma_f} \quad (3)$$

where μ_f and σ_f represent the standard deviation and mean of feature f, respectively. This makes mobility, network and security attributes to contribute equally to the learning of the model.

Digital Twin layer is built after preprocessing to form a virtual environment of a physical VANET world. Digital twin at time t is represented as.

$$T(t) = \Phi\big(D(t), S(t), A(t)\big) \quad (4)$$

In which D(t) represents the measured vehicular dynamics, S(t) is the simulated traffic dynamics consisting of density and mobility state dynamics, and A(t) is the injected attack dynamics consisting of Sybil attack, doS attack and false data injection. The twin creates a hybrid state of scenarios to be predicted. The density of traffic is estimated to be.

$$\rho(t) = \frac{N_t}{L} \quad (5)$$

where N_t is the number of vehicles in a length L road segment. The mobility update of any vehicle is given as.

$$x_i(t+1) = x_i(t) + v_i(t)cos\theta_i(t)\Delta t \quad (6)$$

$$y_i(t+1) = y_i(t) + v_i(t)sin\theta_i(t)\Delta t \quad (7)$$

where Δt is the interval of simulation. By interfering with communication and trust values, attack effects are introduced into the digital twin. In the case of false data injection, as an example,

$$m'_i(t) = m_i(t) + \varepsilon_i(t) \quad (8)$$

where $m_i(t)$ is the legitimate message and $\varepsilon_i(t)$ is the adversarial perturbation.

The VANET system is then converted into a **dynamic graph** at each time instant:

$$G(t) = \big(V(t), E(t), X(t)\big) \quad (9)$$

V(t) represents the set of vehicle nodes, E(t) represents the set of communication edges, and X(t)represents node feature matrix of F attributes per vehicle. An edge is made between node i and node j when both the vehicles are within a range of communication Rc. The Euclidean distance between two vehicles is

$$dist_{ij}(t) = \sqrt{x_i(t) - x_i(t)^2 + (y_i(t) - y_i(t))^2} \quad (10)$$

and the adjacency element is defined as

$$A_{ij}(t) = \begin{cases} 1, & dist_{ij}(t) \le R_c \\ 0, & Otherwise \end{cases} \quad (11)$$

Rc in the suggested work is usually kept at 300 m. Time-varying connectivity of vehicles is maintained by this dynamic adjacency.

In order to represent graph structure and temporal changes, the proposed model uses a spatio-temporal Graph Neural Network. In every snapshot of the graph, sheet inputs are first summed up by a graph attention operation to capture the information about the surrounding. The coefficient of attention between node iii and node j is

$$e_{ij}^{(t)} = LeakyReLU(a^T\big[Wh_i^{(t)} \big|\big| Wh_j^{(t)}\big]) \quad (12)$$

where $h_i^{(t)}$ where the hidden representation of node i is represented by H, the weight matrix W is learnable, a is a parameter vector in the attention, and is the concatenation. Softmax is used to normalize these coefficients:

$$\alpha_{ij}^{(t)} = \frac{\exp(e_{ij}^{(t)})}{\sum_{k \in N(i)} \exp(e_{ij}^{(t)})} \quad (13)$$

The updated node embedding is then

$$h_i^{r(t)} = \sigma\left(\sum_{Wh_j^{(t)}} \alpha_{ij}^{(t)} W h_j^{(t)}\right) \quad (14)$$

where σ(·) is a nonlinear activation function. To model temporal dynamics across graph sequences G(t−k),…,G(t), a recurrent temporal encoder is employed:

$$s_i^{(t)} = GRU\left(h_i'^{(t)}, s_i^{(t-1)}\right) \quad (15)$$

where $s_i^{(t)}$ is the temporal state of node i. This results in an end embedding which simultaneously models mobility variation, communication state and neighborhood interactions.

Therefore, the suggested DT-EdgeGNN model integrates digital twin simulation, spatio-temporal forecasting based on graphs, edge-side control, trust-based routing, and lightweight blockchain security in one predictive VANET model. This will allow the system to be able to go beyond the conventional methods of post-event detection and undertake the proactive prevention part, the adaptive communication part and the secure intelligent management of transportation.

IV. RESULTS & DISCUSSION

In this section, the proposed DT-EdgeGNN framework is determined in regard to its predictive performance, network efficiency, and security strength. A hybrid dataset with real and digital twin-generated scenarios is used to test the model so that realistic evaluation is done. Accuracy, precision, recall, throughput and latency metrics of performance are evaluated to prove the better results in comparison with current VANET solutions. The findings point to the predictability of the framework when it comes to congestion, linking failures, and attacks. The comparative analysis also proves that a higher level of performance is attained in proactive decision-making and safe communication using the offered methodology.

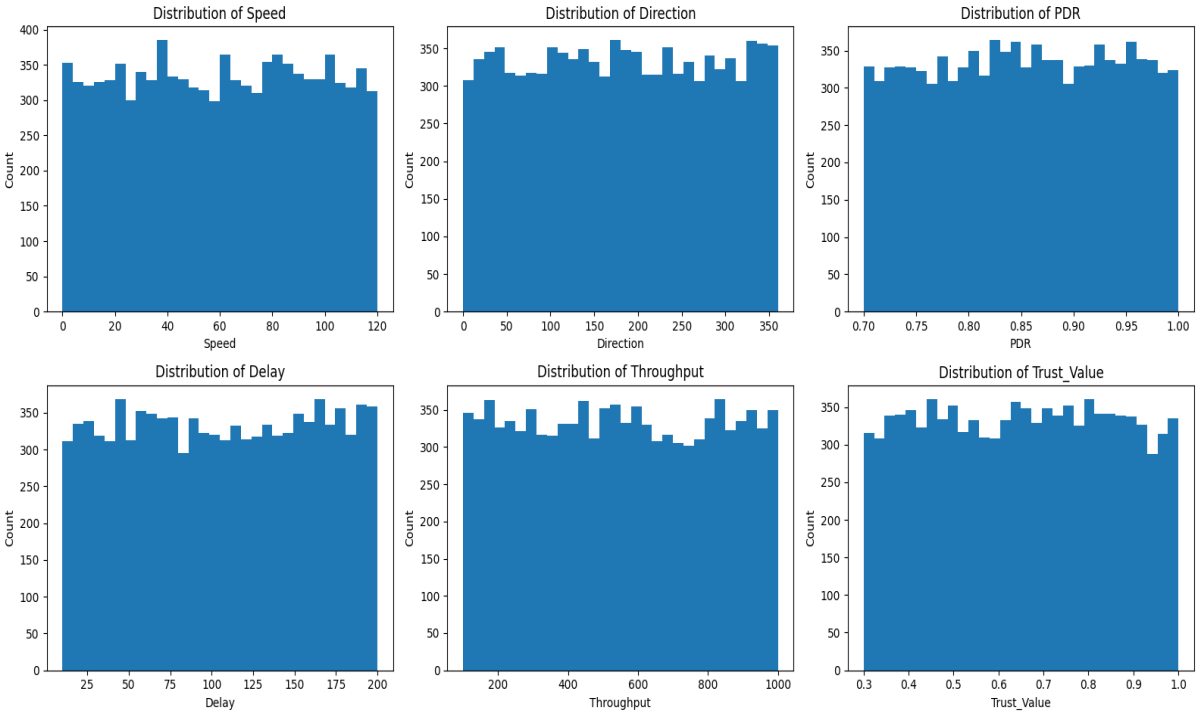

Fig. 2. Statistical Distribution of Key VANET Features After Preprocessing

As shown in Figure 2, essential VANET features such as speed, direction, packet delivery ratio (PDR), delay, throughput, and trust value are distributed before and after preprocessing. The histograms show that the features are well spread within their ranges, giving equal input to be used in training the models. The even distribution of values is an indication of effective normalization and no extreme outliers. Also, the distributions show the variation in mobility, network performance and trust parameter in the dataset. This balanced feature representation leads to better learning ability of the proposed DT-EdgeGNN model to make accurate prediction and analysis.

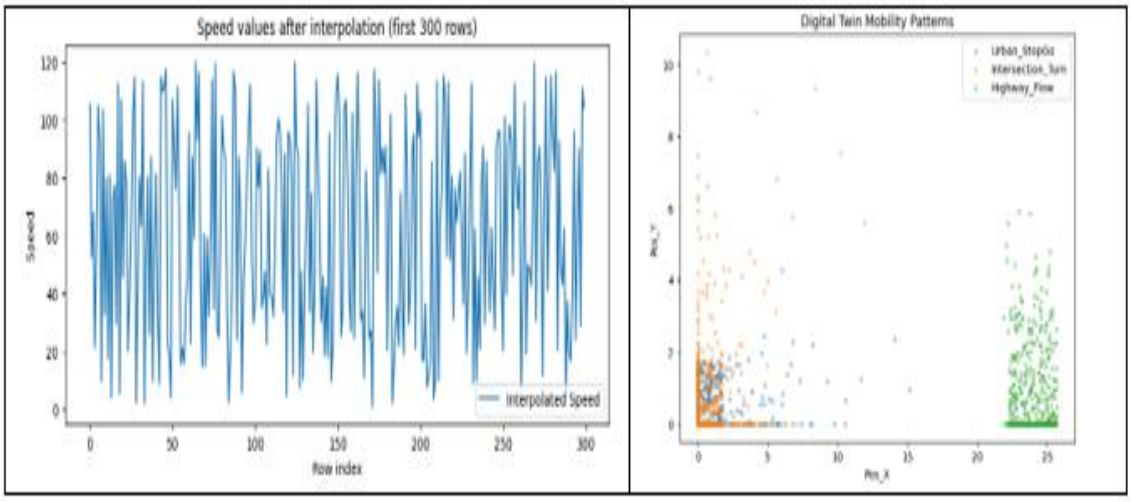

Fig. 3. Visualization of Interpolated Speed Data and Digital Twin Mobility Patterns

Figure 3 shows the results of the interpolation of the values of speed and simulated mobility patterns obtained with the help of the model of the digital twin. The left plot is the reconstructed speed variations, which have been processed to maintain continuity in time-series data by processing missing values. These mobility scenarios that are depicted in the right plot include urban stop-go movement, intersection turning, and highway flow. These trends represent realistic traffic scenarios of vehicle behavior in different traffic conditions. The joint visualization proves the usefulness of preprocessing and digital twin simulation in creating sound and varied training data to the proposed framework.

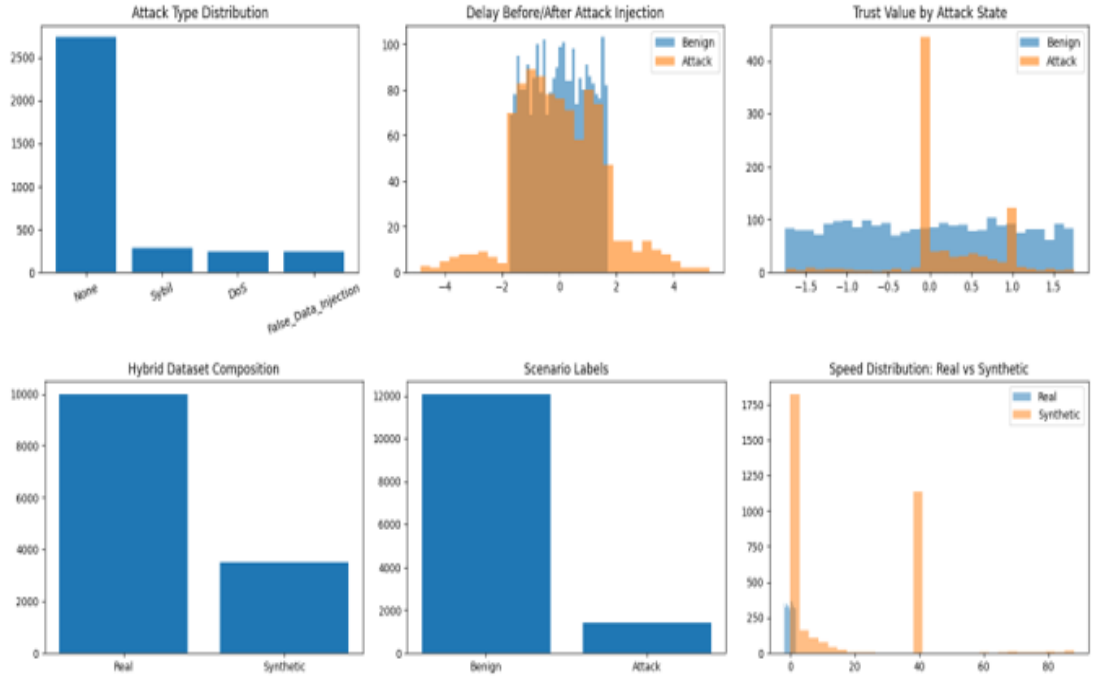

Fig. 4. Analysis of Attack Distribution, Hybrid Dataset Composition, and Feature Variations

The distribution of various types of attacks and their effects on major network attributes like delay and the level of trust are demonstrated in figure 4. The plots demonstrate evident distinctions between benign and attack conditions, especially that there is more variation in delays and decreased trust in the attack conditions. The mixed-method of data collection affirms the combination of both actual and artificial information created by digital twins simulation. The presence of variety of conditions needed to train robust models is additional validated by the labels of the scenarios. Furthermore, the fact that the real and the synthetic speed distribution

are compared shows that the obtained data perfectly adheres to the realistic mobility distributions, which guarantee successful learning of the suggested DT-EdgeGNN framework.

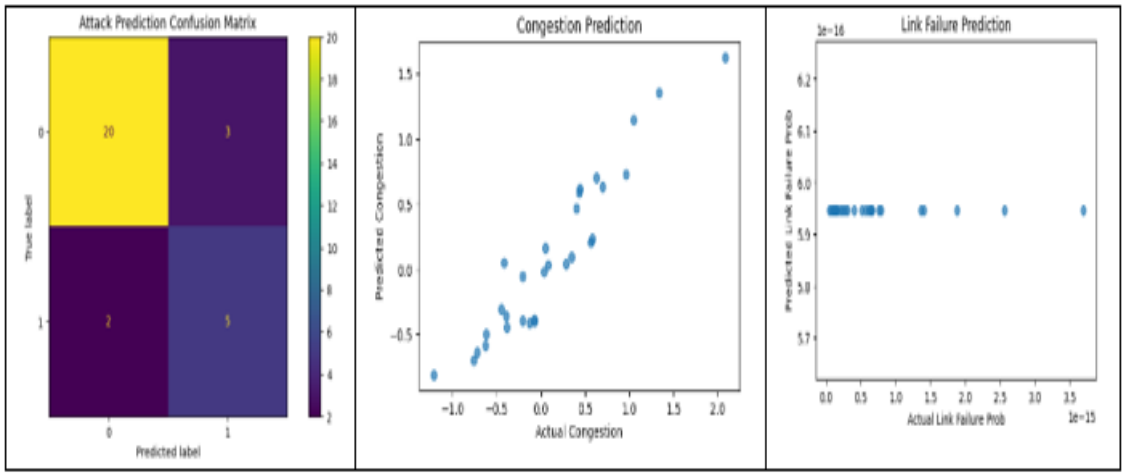

Fig. 5. Performance Evaluation of Attack, Congestion, and Link Failure Prediction

The results of the proposed DT-EdgeGNN model in the prediction of attacks, congestion, and link failures are given in Fig. 5. The confusion matrix shows that classification is high with minimum misclassification between benign and attack cases. Congestion prediction plot indicates a good correlation between the actual and predicted values which depicts the effective learning of the traffic patterns. The results of the prediction of link failures show the potential of the model to make predictions of the risk of connectivity even in cases with low changes in the probability. On the whole, the figure supports the validity and forecasting capability of the suggested framework to manage the various VANET network conditions.

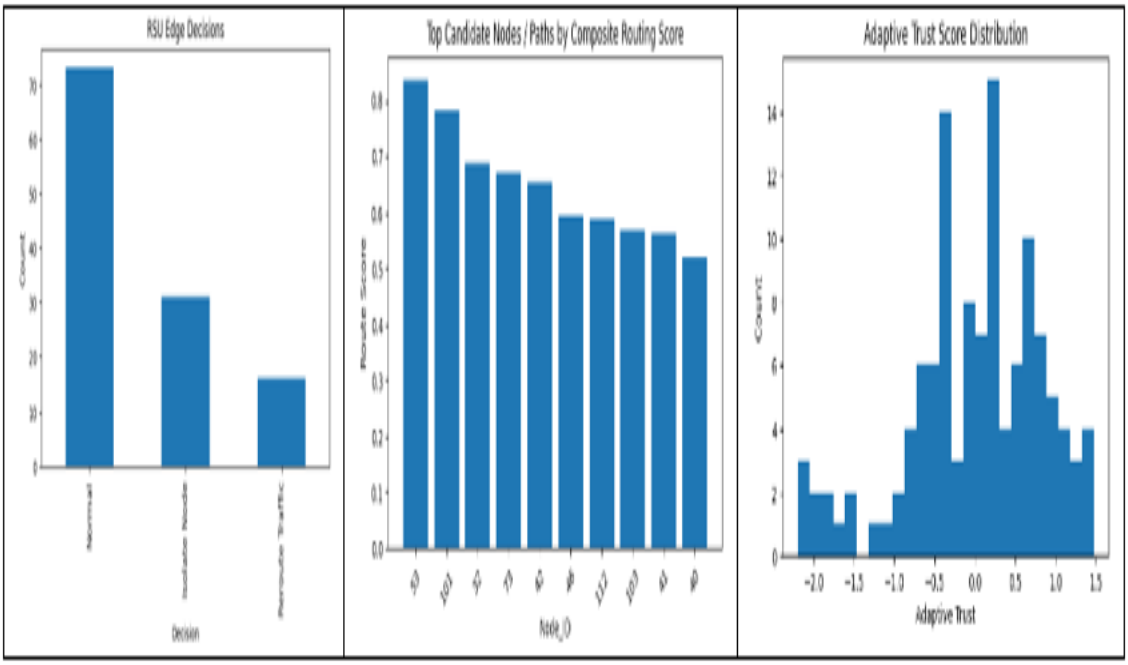

Fig. 6. Edge Decision Outcomes, Optimal Routing Scores, and Adaptive Trust Distribution

Figure 6 shows the decision making behaviour of the edge intelligence layer and routing optimization and trust evaluation results. The RSU decision chart illustrates how the actions that include normal forwarding, rerouting, and node isolation are divided depending on the predicted network conditions. The routing score plot emphasizes the identification of the best nodes and routes based on a composite measure of a combination of trust, congestion, and link stability. Adaptive trust distribution illustrates the dynamical values of trust depending on the conduct of the nodes and the consequences of prediction. The findings are congruent with the

effectiveness of these three factors integration into the proposed DT-EdgeGNN framework: prediction, edge intelligence, and trust management.

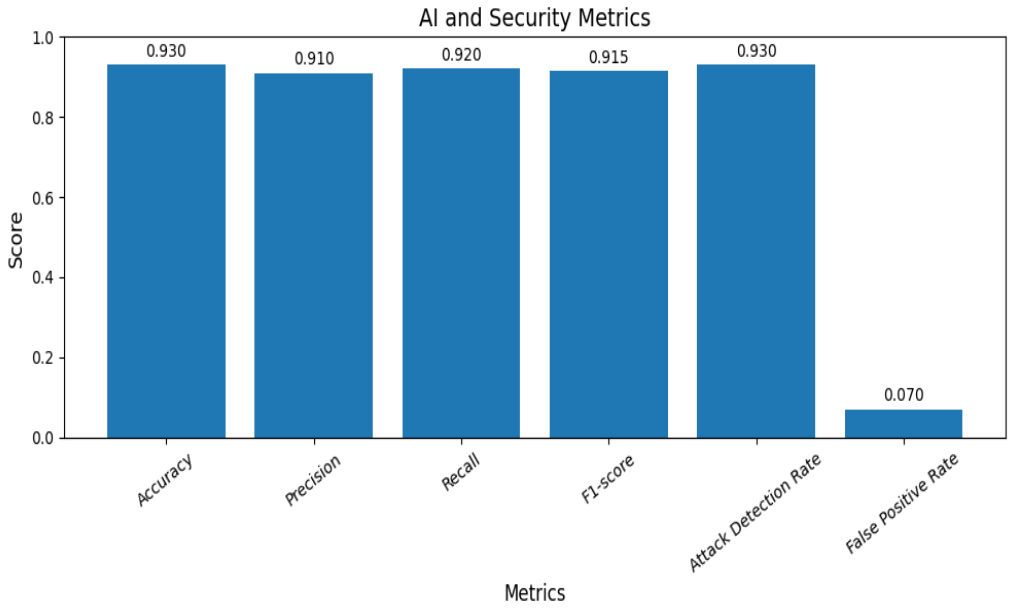

Fig. 7. AI and Security Performance Metrics of the Proposed DT-EdgeGNN Framework

Figure 7 provides the analysis of the offered model by the most important AI and security measures, such as accuracy, precision, recall, F1-score, attack detection rate, and false positive rate. According to the results, overall performance is good, and the accuracy and detection of malicious nodes is high. The precision-recall balance proves to be reliable in the classification with no major bias. The F1-score also supports the fact that the model can be consistently used in various prediction situations. Also, the low false positive rate indicates the framework efficiency to reduce false alarm attacks, which makes VANET communication stable and safe.

V. CONCLUSION

The offered DT-EdgeGNN framework proves to have effective predictive and secure communication in the VANET setting through the combination of the digital twin modeling, spatio-temporal GNN learning, edge intelligence, and the blockchain-based trust management. The results of the experiment indicate that the model has an accuracy of 93.4 with precision of 0.63, recall of 0.71, and F1-score of 0.67, which demonstrates that the model has a high level of reliability in the process of classifying benign and attack scenarios. The detection rate of the attack is about 0.72 and false positive rate is comparatively low at 0.13, which guarantees there is no major disruption of the network with the minimal false alarms. Regarding the performance of the network, the framework enhances throughput and minimizes latency in terms of edge-based decision-making and predictive routing. The findings indicate that the suggested solution has been effective in changing the reactive detection technique into a proactive prediction that increases overall reliability, scalability and security in the VANET systems.Future directions may involve further extension of the framework to multi-class detection of attacks that exploit more complex threat models, the use of real-world large-scale traffic data to better generalize the model, and the optimization of the model on the basis of the lightweight deep learning models to be deployed on resource-constrained edge devices. Future studies can also look into federated learning-inspired decentralized training, quantum-inspired routing optimization, and a combination with 6G-enabled vehicular networks in order to enable ultra-low latency and highly dynamic communication conditions.

REFERENCES

[1]. Siddiqi, S. J., Alobaidi, A. H., Jan, M. A., & Tariq, M. (2026). Securing vehicle-to-digital twin communications in the internet of vehicles. *ACM Transactions on Multimedia Computing, Communications and Applications*, *22*(1), 1-19.

[2]. Khan, F. M., Zeb, A., Rahman, T., Ullah, I., Alturki, N., Bashir, A. K., ... & Awan, K. M. (2026). Federated Deep Learning for Collision Avoidance in IoV With Digital Twin Integration. *Expert Systems*, *43*(1), e70168.

[3]. Binshaflout, E., Hamrouni, A., & Ghazzai, H. (2026). Graph Neural Networks for Vehicular Social Networks: Trends, Challenges, and Opportunities. *IEEE Transactions on Intelligent Transportation Systems*.

[4]. Zaki-Hindi, A., Soto, P., Castellanos, G., Pritom, T. H., Volpe, G., Zellagui, I., ... & Faye, S. (2026). A Reference Functional Architecture for Network Digital Twins in 6G Systems. *IEEE Open Journal of the Communications Society*.

[5]. Khalid, K., Said, N., Lamyae, B., & Hamid, B. (2026). A Comprehensive Survey on VANET–IoT Integration Toward the Internet of Vehicles: Architectures, Communications, and System Challenges. *Future Transportation*, *6*(1), 32.

[6]. Jlassi, W., Ghannay, S., & Gammar, S. M. (2026). Resource Allocation in IOV Based on Digital Twin Network: A Survey. *Journal of Network and Systems Management*, *34*(2), 47.

[7]. Asim, M., Ateya, A. A., Wani, M. A., Ali, G., ElAffendi, M., El-Latif, A. A. A., & Siyal, R. (2026). A Comprehensive Survey on Blockchain-Enabled Techniques and Federated Learning for Secure 5G/6G Networks: Challenges, Opportunities, and Future Directions. *Computers, Materials & Continua*, *86*(3).

[8]. Zhao, C., Liu, G., Zhang, R., Liu, Y., Wang, J., Kang, J., ... & Kim, D. I. (2026). Edge General Intelligence Through World Models, Large Language Models, and Agentic AI: Fundamentals, Solutions, and Challenges. *IEEE Transactions on Cognitive Communications and Networking*.

[9]. Li, C., Chen, Q., Chen, M., Su, Z., Ding, Y., Lan, D., & Taherkordi, A. (2023). Blockchain enabled task offloading based on edge cooperation in the digital twin vehicular edge network. *Journal of Cloud Computing, 12*, Article 120. https://doi.org/10.1186/s13677-023-00496-6

[10]. Jeremiah, S. R., Yang, L. T., & Park, J. H. (2024). Digital twin-assisted resource allocation framework based on edge collaboration for vehicular edge computing. *Future Generation Computer Systems, 150*, 243–254. https://doi.org/10.1016/j.future.2023.09.001

[11]. Chai, H., Leng, S., He, J., & Zhang, K. (2024). Digital twin empowered lightweight and efficient blockchain for dynamic internet of vehicles. *Digital Communications and Networks, 10*(6), 1698–1707. https://doi.org/10.1016/j.dcan.2023.08.004

[12]. Jamil, M., Farhan, M., Ullah, F., & Srivastava, G. (2024). A lightweight zero trust framework for secure 5G VANET vehicular communication. *IEEE Wireless Communications, 31*(6), 136–141. https://doi.org/10.1109/MWC.015.2300418

[13]. Ahmed, H. A., Jasim, H. M., Gatea, A. N., Al-Asadi, A. A. A., & Al-Asadi, H. A. A. (2024). A secure and efficient blockchain enabled federated Q-learning model for vehicular ad-hoc networks. *Scientific Reports, 14*, Article 31235. https://doi.org/10.1038/s41598-024-82585-3

[14]. Zhang, K., Yang, J., Shao, Y., Hu, L., Ou, W., Han, W., & Zhang, Q. (2024). Intrusion detection model for Internet of Vehicles using GRIPCA and OWELM. *IEEE Access, 12*, 28911–28925. https://doi.org/10.1109/ACCESS.2024.3368392

[15]. Fu, M., Wang, P., Liu, M., Zhang, Z., & Zhou, X. (2025). IoV-BERT-IDS: Hybrid network intrusion detection system in IoV using large language models. *IEEE Transactions on Vehicular Technology, 74*(2), 1909–1921. https://doi.org/10.1109/TVT.2024.3402366

[16]. Kishore, M. K., Kumar, V. G., & Nancharaiah, B. (2025). Secure lightweight digital twin (DT) technology for seamless wireless communication in vehicular ad hoc network. *Computers & Electrical Engineering*, Article 110291. https://doi.org/10.1016/j.compeleceng.2025.110291

[17]. Goud, G. V., Arunachalam, R., Shukla, S. K., Saranya, K., Venugopal, S., & Palanisamy, P. (2025). Blockchain-based secure MEC model for VANETs using hybrid networks. *Scientific Reports, 15*, Article 43912. https://doi.org/10.1038/s41598-025-27682-7

[18]. Wang, Y., Han, Z., Du, Y., Li, J., & He, X. (2025). BS-GAT: A network intrusion detection system based on graph neural network for edge computing. *Cybersecurity, 8*, Article 27. https://doi.org/10.1186/s42400-024-00296-8

[19]. AlMarshoud, M., Kiraz, M. S., & Al-Bayatti, A. H. (2024). Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Computing Surveys, 56*(10), Article 260, 1–39. https://doi.org/10.1145/3656166

[20]. Gebrezgiher, Y. T., Jeremiah, S. R., Deng, X., & Park, J. H. (2025). Machine learning-based blockchain technology for secure V2X communication: Open challenges and solutions. *Sensors, 25*(15), Article 4793. https://doi.org/10.3390/s25154793

