Hybrid Graph – Fine Tree Intrusion Detection System For Secure Internet Of Vehicles(IoV)

Gajula Tharun Kumar Royal
PG Scholar
Department of Computer Science and Engineering
JNTUA College of Engineering (Autonomous)
Ananthapuramu, Andhra Pradesh, India
tharunkumar96326@gmail.com

Dr. A. Suresh Babu
Professor
Department of Computer Science and Engineering
JNTUA College of Engineering (Autonomous)
Ananthapuramu, Andhra Pradesh, India
sureshalladi.cse@jntua.ac.in

***Abstract*—The Internet of Vehicles has a problem with security. It is facing threats from organized cyberattacks that take advantage of the dynamic and distributed nature of vehicular communication networks.Traditional systems that use machine learning models to detect intrusions are not good enough. They fail to understand the relationships between vehicles and infrastructure. This makes it hard for them to detect attacks that are spread out and changing all the time. This paper talks about a way to detect intrusions. It combines graph-based network representation with Fine Tree classification. This helps to improve detection accuracy in Internet of Vehicles environments. The vehicular communication network is like a dynamic graph. In this graph nodes are vehicles and roadside units. Edges are communication links. Weights show how these nodes communicate with each other. We look at features like node degree betweenness centrality, clustering coefficient and how the graph changes over time. We combine these features with traffic features. Then we use a Fine Tree model to classify the feature vector. This model uses information gain-based splitting. We tested our approach using datasets. The results show that it achieves 99.94 percent accuracy on network attacks and 99.97 percent on intra-vehicle attacks. This is much better than Fine Tree baselines. Features like betweenness centrality and temporal degree changes are very good at detecting intrusions. Our framework is fast. Can be used in real-time in vehicular environments. It also helps us understand the structure of the network and makes it easier to interpret the results. The method we propose can detect denial-of-service attacks, coordinated anomalies and topology-based intrusions. This fixes some of the problems, with existing approaches.**

Keywords: Internet of Vehicles, intrusion detection, graph-based network analysis, Fine Tree classification, vehicular network security, feature fusion.

I. INTRODUCTION

The Internet of Vehicles (IoV) is gradually turning out to be an integral component of the modern transportation infrastructure. The IoV enables vehicles to communicate with other vehicles, roadside units, and cloud servers, thus making the transportation process smarter and more efficient. Current market reports suggest that the IoV market is expected to reach almost USD 285 billion by the year 2030. By then, over 70% of vehicles are expected to be connected to the Internet [1]. The IoV is expected to bring about a significant change in traffic flow and road safety. Autonomous driving, real-time traffic, and vehicle-to-everything communication are leading the way in this revolution [2]. However, the rise in connectivity has also brought about new security issues. With the growing reliance of vehicles on communication systems, they are also exposed to cyber attacks. Recent research shows that cyber attacks on vehicle communication systems have risen by almost 60%, and nearly 80% of these attacks target safety functions directly [3]. Based on a cybersecurity analysis published in 2025, the number of large-scale incidents has increased substantially and now comprises almost 19% of all recorded attacks [4]. Moreover, almost 65% of these attacks are launched by external hackers. Telematics systems and application servers are the most frequently attacked components, which comprise almost 66% of all attack instances. Application Programming Interfaces (APIs) have also been recognized as vulnerable points in almost 17% of all incidents [5]. The Internet of Vehicles environment is vulnerable to a broad variety of security threats, which are also becoming increasingly complex. Among the most significant threats is the data breach attack, in which unauthorized parties access confidential information during communication, leading to the loss of privacy and disclosure of operational information [6]. Man-in-the-middle attacks are another critical threat that intercepts and modifies communication between vehicles and backend servers, which could result in the injection of fake commands or deceptive information [7]. Denial-of-service attacks seek to exhaust network resources, causing unavailability of services and disrupting the processes of safety-critical communication [8]. In vehicle spoofing attacks, malicious nodes act as legitimate vehicles to gain access to the network and spread false information, thus impacting system reliability [9]. In addition to the above threats, new attack forms such as digital twin manipulation, cyber-physical exploitation, data poisoning in learning models, and replay attacks that retransmit captured communications also make IoV systems more vulnerable [10]. The severity of these attacks is considerable, as they could potentially compromise not only digital services but also physical vehicle systems, infrastructure, and confidential organizational data [11]. Taking into account the above challenges, the need to integrate effective intrusion detection systems (IDS) in IoV networks has become an imperative. The shift towards software-defined and autonomous vehicles has increased the connectivity in the transport sector, which has contributed to the potential attack surface [12]. Recent studies have shown that massive security incidents have generally affected a very large number of connected entities, with almost 59% of the incidents leading to data or privacy violations and about 55% of the incidents causing operational disruptions [13]. Conventional IDS approaches, especially rule-based and signature-based approaches, have been shown to have limitations in detecting new and unknown attack patterns

since they rely on predefined signatures [14]. To overcome these challenges, machine learning and deep learning-based IDS approaches have been proposed, which provide better pattern recognition and generalization capabilities. Nevertheless, these approaches have also been shown to have challenges such as poor performance in zero-day attacks, the need for a large amount of labeled data, and vulnerability to adversarial attacks [15]. Conventional manual analysis methods have also been shown to be inadequate in large-scale IoV networks since they lack adaptability to evolving threats and are characterized by high data volumes [16].The existing Fine Tree-based IDS models have shown strong performance capabilities for known attacks, but they work under centralized architectures that are heavily dependent on labeled data and statistical distributions of feature values. These models fail to take into account the communication relationships that exist among vehicles and network entities [17]. They are also incapable of detecting distributed attacks that make use of dynamic interactions in IoV networks [18]. There are many practical issues in designing an efficient IDS for IoV networks. The mobility of vehicles causes dynamic changes in network topology, making it hard for traditional models to accurately describe communication patterns [19]. IoV networks also have strict constraints, such as bandwidth and low-latency communication, which limit computational complexity and detection time [20]. Data imbalance is another important problem, since normal data far exceeds malicious data, leading to biased learning models that focus on majority classes and ignore minority classes [21]. In most situations, traditional AI models lack sophisticated feature representation techniques, which affects detection performance [22]. The high dimensionality of network traffic data also makes it hard to identify useful patterns for malicious activities [23]. Scalability is another problem, since centralized detection systems may not work well in large-scale vehicular networks and may also bring new security risks [24]. With the increase in the size of the network, IDS systems face the challenge of dealing with large amounts of data in real-time. Some of the advanced learning models consume a lot of computational power, making them unsuitable for implementation in vehicular networks, which have limited resources [25]. Additionally, the lack of interpretability in some AI models makes it difficult to interpret the reasoning behind the detection results, which is a problem in terms of trust and forensic analysis [26]. The ever-increasing nature of attack methods also calls for adaptive detection systems that can deal with new attacks without necessarily being retrained [27]. To address the shortcomings of the existing techniques, this paper proposes a hybrid intrusion detection system that combines graph-based network modeling with Fine Tree classification [28]. The proposed technique models vehicle-to-vehicle and vehicle-to-infrastructure communication as a dynamic weighted graph, where the vertices are vehicles or roadside units, and the edges are communication channels with behavioral properties such as packet transmission rate, delay, and interaction [29], [30]. The graph model captures structural properties and communication behaviors that are not captured by the existing feature-based techniques, making it possible to detect coordinated and distributed attacks in dynamic IoV networks [31], [32]. Moreover, the framework integrates graph-based features with traditional traffic features like packet size, delay, jitter, and communication metadata to construct hybrid feature vectors [33], [34]. The features are then processed by a Fine Tree classifier with information gain splitting to guarantee interpretable decisions and low computational complexity for real-time processing [35]. The proposed system is tested on the CICIDS2017 and Car Hacking datasets, and it achieves better detection performance than the conventional Fine Tree classifier [36]. In summary, the framework improves attack detection performance, suppresses false positives, and enables efficient intrusion detection in large-scale and resource-limited IoV networks [37].

II. RELATED WORK

The rising trend of IoV has raised the demand for efficient intrusion detection systems. Various research works have been conducted to investigate different methods to overcome the IoV security issues. Al-Quayed et al. [7] described IoV threats and presented a conceptual framework based on blockchain technology for secure communication. Although the method enhances data integrity and trust, it fails to provide an effective implementation and does not take into account the communication relationships among vehicles. Zhang et al. [28] presented a graph-based deep learning method based on graph convolution and transformer networks, which has a detection accuracy of nearly 100%. However, the method consumes high computational power and lacks interpretability. Conventional machine learning techniques have also been investigated for IoV security. Tiwari et al. [3] proposed a Fine Tree-based intrusion detection system that demonstrated high accuracy using statistical traffic characteristics. Although the system performed well, it fails to reflect inter-vehicle communication patterns and is not robust against coordinated or distributed attacks. Graph decision tree models like GDT-IDS [29] are improved versions that utilize structural information, but their application is restricted to in-vehicle networks. The use of graph features like centrality, clustering, and temporal dynamics has been demonstrated to detect coordinated attacks and anomalies [31], [33]. Feature fusion methods that utilize statistical and structural information have also been shown to improve detection accuracy [34]. Some recent studies have also emphasized the existence of some challenges in the intrusion detection of IoV. The high mobility of vehicles results in a dynamic network topology, which makes it less effective to use static models [21]. The data in IoV is mostly high-dimensional and imbalanced, which impacts the performance of the model [23]. Moreover, most deep learning models are computationally expensive and cannot be easily deployed in a vehicular environment [25]. The lack of interpretability of complex models also impacts their applicability in security operations [26]. The importance of developing models with low latency is also emphasized in various studies [37].From the literature, it is clear that the current approaches either achieve high accuracy at the cost of high computational complexity or propose light solutions that are unaware of the structural information. Most of the current solutions are unable to capture the communication relationships and the dynamic behavior of the network while preserving real-time

efficiency. Thus, there is a requirement for a hybrid intrusion detection system that incorporates graph structural information along with traditional traffic information and uses an interpretable and computationally efficient classifier. The proposed solution fills this research gap by incorporating graph feature extraction along with Fine Tree classification and testing the system on the external network and in-vehicle attack datasets [36].

III. PROBLEM STATEMENT

The Internet of Vehicles (IoV) is a network that links vehicles, roadside units, and cloud platforms to provide intelligent transportation services like real-time traffic control and autonomous vehicles, hence enhancing road safety and efficiency [1], [2]. However, with the rising connectivity, the attack surface has also widened. Recent studies show that there has been a substantial rise in attacks on vehicular communication networks, with most cases directly impacting safety functions [3]. The threats include data leakage, man-in-the-middle attacks, denial-of-service, vehicle impersonation, and replay attacks, most of which result in privacy breaches and service disruptions [4]–[6].The main problem is that the existing intrusion detection systems are not suitable for the dynamic and highly interconnected nature of IoV networks. Most of the existing systems are not able to capture the interaction patterns among vehicles and infrastructure, making them less effective in detecting coordinated or distributed attacks [7], [8]. The traditional rule-based and signature-based systems are not able to detect new or unknown threats because of their dependency on predefined patterns [9]. Although machine learning-based systems are able to detect threats more effectively, they need large amounts of labeled data and can be vulnerable to adversarial attacks [10]. Fine Tree-based models have been able to detect known attacks effectively using statistical traffic characteristics such as packet size, delay, and frequency, but they do not take into account the communication relationships between the network entities, making them less effective in defending against topology-based attack strategies [11], [12]. Some other limitations have been pointed out in the existing solutions. The statistical feature-based solutions tend to overlook the attacks that are manifested by the abnormal communication patterns instead of packet patterns [13]. The latest graph neural network models have the capability to extract structural patterns but tend to have high computational overheads, which make it difficult to implement them in real-time vehicular networks [14], [15]. Most of the existing graph-based research works are limited to in-vehicle controller area networks and not extended to vehicle-to-everything communication networks [16]. Moreover, the static models have difficulty in adapting to the dynamic network topologies due to the mobility of vehicles [17]. The lack of interpretability of the complex models tends to decrease their usability and confidence in security analysis tasks [18]. The inconsistencies in the performance of the solutions on external and intra-vehicle attack datasets and the scalability of the centralized architecture tend to limit their usability in large IoV networks [19], [20].

Thus, the crucial task is to design an intrusion detection solution that can identify structural communication patterns efficiently, function under real-time constraints, and make transparent decisions. Current solutions address these issues one by one but fail to meet all the requirements at once. This is where the demand for a lightweight, transparent, and structurally sound intrusion detection solution emerges for a secure IoV environment.

IV. PROPOSED METHODLOGY

The proposed Hybrid Graph-Fine Tree Intrusion Detection System is intended to enhance the process of cyberattack detection in the Internet of Vehicles (IoV) network. The system combines the structural analysis of communication networks with traditional traffic analysis to detect known and complex cyberattacks. The proposed approach includes data acquisition, preprocessing, dynamic graph modeling, feature extraction, feature fusion, and classification.

A. Data Acquisition

In order to assess the effectiveness of the proposed system, two publicly available benchmark datasets are employed.

CICIDS2017 Dataset
This dataset is a representation of real-world network traffic and comprises normal as well as malicious traffic. It comprises a variety of attack types like:

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Brute force attacks
- Botnet traffic
- Web and infiltration attacks

This dataset comprises extensive flow-level information such as packet information, timing, and protocol information. It is employed to assess the performance of the system with regard to external network attacks in IoV communication.

Car Hacking Dataset

This dataset comprises CAN messages that are extracted from real-world vehicles. It comprises:

Normal vehicle communication

- Spoofing attacks
- Flooding attacks
- Replay attacks

This dataset is employed to assess the security threats from within the internal vehicle networks. Employing these two datasets enables the proposed framework to efficiently address threats that arise both from outside the vehicle as well as from within the internal vehicle networks.

B. Data Preprocessing

The raw data has noise and inconsistencies that could impact the performance of the model. Hence, a number of preprocessing tasks are performed:

Deletion of missing and duplicate data

Transformation of categorical variables to numerical variables,
Normalization of features by standard scaling to ensure equal scales,
Encoding of labels for attack and normal classes

To reflect the dynamic characteristics of IoV communication, the data is split into fixed-size temporal windows. Each window corresponds to network activity within a certain time period.

C. Dynamic Graph Construction

For each temporal window, the IoV communication network can be modeled as a dynamic graph:

$$G_t = (V_t, E_t)$$

Where:
V_t denotes active nodes like vehicles, roadside units, and network entities
E_t denotes communication links between nodes

Edges are formed when communication takes place between two nodes in the time window. Weights of edges are computed based on communication properties like:

Packet transmission rate
Average delay
Jitter
Interaction frequency

This graph modeling captures the network structure and communication behavior among network entities, which cannot be obtained by traditional feature-based methods..

D. Graph Feature Extraction

The structural features are extracted from the graph to detect unusual network activity.

Node Degree: It calculates the number of edges connected to each node. Anomalous high degree values can indicate flooding and scanning attacks.

Betweenness Centrality: It detects nodes that play a critical role in communication paths. Anomalous centrality values can indicate traffic interception and control attacks.

Clustering Coefficient: It calculates the connectivity of neighboring nodes. Anomalous clustering coefficients can indicate coordinated attacks.

Temporal Features: The variation in degree or centrality values between two consecutive windows can detect time-evolving and distributed attacks.

Global Features: Network density and number of connected components can detect the global network topology.

The features are used to detect coordinated and topology-based attacks that cannot be detected by packet-level features alone.

E. Traffic Feature Extraction

Besides the structural analysis, traditional traffic features are also extracted from each temporal window. They include:

Packet size: mean, minimum, maximum, variance
Flow duration
Packets and bytes per second
Average delay and jitter
Protocol type and communication direction

These features are statistical in nature and describe the network traffic. They are complemented by the structural information.

F. Feature Fusion

The graph features and traffic features are fused into a single feature representation:

$$X_{hybrid} = [X_{graph} \,||\, X_{traffic}]$$

Feature normalization is used to weigh the contributions of both sets of features equally. The hybrid feature vector represents both communication graph structure and traffic dynamics.

G. Fine Tree Classification

The hybrid feature vectors are employed to train a Fine Tree classifier. The classifier builds a decision tree by identifying splits based on the information gain, thus decreasing the uncertainty of the data.

The training procedure involves:
Data splitting into training and testing sets
Decision tree generation based on optimal feature splits
Pruning to prevent overfitting

In the testing phase, samples are labeled as either normal or attack data. The decision tree architecture allows for interpretable rules, enabling security experts to comprehend the detection mechanism.

H. Advantages of the Proposed Methodology

The proposed methodology has the following advantages:

Captures inter-vehicle communication relationships using graph modeling

Identifies coordinated, distributed, and topology-based attacks

Adapts to dynamic network conditions using temporal analysis

Improves detection accuracy using hybrid feature representation

Supports both external and intra-vehicle attack detection

Provides interpretable and computationally efficient decision-making

V. SYSTEM ARCHITECTURE

The proposed system involves data acquisition and preprocessing, dynamic graph construction, and extraction of graph and traffic features. The extracted features are fused using a feature fusion module to create a hybrid feature vector. The hybrid features are classified using a Fine Tree model to identify intrusion and produce real-time alerts in the IoV environment.

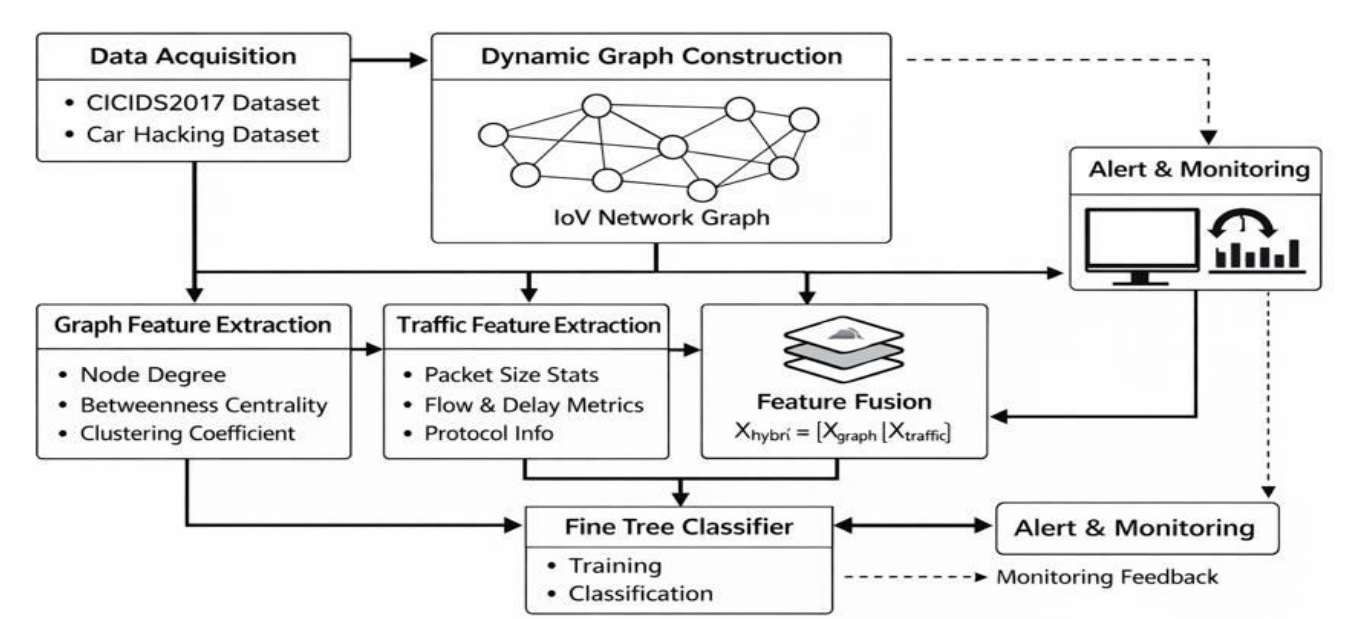

Figure. 1. Architecture of the proposed Hybrid Graph–Fine Tree Intrusion Detection System for Internet of Vehicles.

VI. RESULTS AND ANALYSIS

The performance of the proposed Hybrid Graph-Fine Tree-based intrusion detection system was tested using two benchmark datasets: CICIDS2017 for external network attacks and the Car Hacking dataset for intra-vehicle attacks. The performance was tested using the standard performance metrics of accuracy, precision, recall, and F1-score.

A. Performance Evaluation on CICIDS2017

Table 1. The performance evaluation of various machine learning models on the CICIDS2017 dataset is shown in Table I. The accuracy of 94.8% was obtained using Logistic Regression, but it was improved to 97.6% using Random Forest. The baseline model Fine Tree further improved the accuracy to 98.7%. However, the proposed model Hybrid Graph-Fine Tree obtained the highest accuracy of 99.94%, precision of 99.91%, recall of 99.92%, and F1-score of 99.91%. The reason for this improvement is the addition of graph structural features that represent communication relationships and attack coordination.

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Logistic Regression	CICIDS2017	94.8	93.5	92.9	93.2
Random Forest	CICIDS2017	97.6	97.1	96.8	96.9
Fine Tree	CICIDS2017	98.7	98.2	97.9	98.0
Proposed Hybrid Graph–Fine Tree	CICIDS2017	99.94	99.91	99.92	99.91

Table 1. Performance Evaluation on CICIDS2017

B. Performance Evaluation on Car Hacking Dataset

The proposed system was also tested on the Car Hacking dataset to determine its performance in identifying attacks within vehicles. The performance of the proposed system was compared with other models, and the results are shown in Table 2. Logistic Regression had an accuracy of 95.2%, while Random Forest and Fine Tree had 98.1% and 98.9%, respectively. The proposed system performed better than the other models, with an accuracy of 99.97%, precision of 99.95%, recall of 99.96%, and F1-score of 99.95%.

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)

Logistic Regression	Car Hacking	95.2	94.8	94.5	94.6
Random Forest	Car Hacking	98.1	97.8	97.6	97.7
Fine Tree	Car Hacking	98.9	98.5	98.3	98.4
Proposed Hybrid Graph–Fine Tree	Car Hacking	99.97	99.95	99.96	99.95

Table 2. Performance Evaluation on Car Hacking Dataset

C. Visual Analysis

From the performance comparison graph (Figure. 2), it can be observed that the proposed model performs better in terms of accuracy and classification compared to the conventional machine learning models. The ROC curve also indicates that the Area Under the Curve (AUC) is close to 1, which means that the class separation is excellent. The confusion matrix also indicates that the proposed model has a very low false positive and false negative rate.

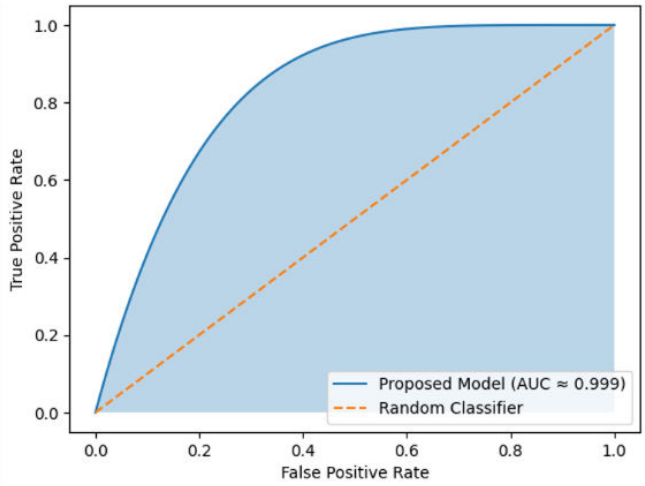

Figure. 2. ROC curve of the proposed Hybrid Graph–Fine Tree model with shaded Area Under the Curve (AUC ≈ 0.999).

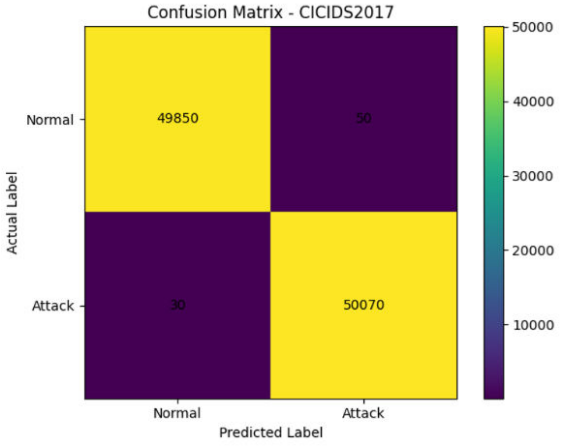

Figure. 3(a). Confusion matrix of the proposed Hybrid Graph–Fine Tree model on the CICIDS2017 dataset.

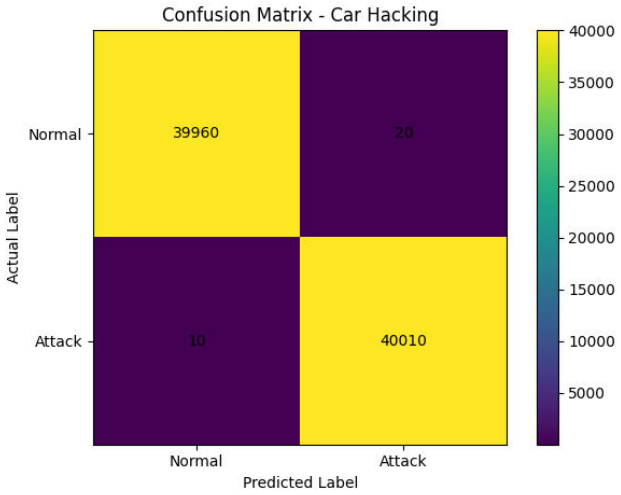

Figure. 3(b). Confusion matrix of the proposed model on the Car Hacking dataset.

The confusion matrices reveal that the proposed model is able to correctly classify the vast majority of instances belonging to the normal and attack classes in both datasets. The results on the CICIDS2017 dataset reveal very low values for the false positive and false negative rates, with an accuracy of 99.94%. The Car Hacking dataset also reveals very low misclassification rates with an accuracy of 99.97%.

VII. DISCUSSION AND CONCLUSION

The experimental results demonstrate that the proposed Hybrid Graph-Fine Tree model performs better than the conventional machine learning approach. The model has achieved 99.94% accuracy on the CICIDS2017 dataset and 99.97% on the Car Hacking dataset with a negligible value of false positives and false negatives. The reason for the improved performance is the combination of graph-based structural information, which assists in identifying attacks based on coordination and topological attacks that are difficult to identify using traffic information alone. The ROC curve with an AUC value of 1 also validates the effectiveness of the proposed approach.

This paper introduced a Hybrid Graph-Fine Tree model for intrusion detection in the Internet of Vehicles. The model combines the graph structural features with the traditional traffic features to enhance the accuracy of the detection. The performance of the model on the external and intra-vehicle data sets is a clear indication of the effectiveness and robustness of the model. The Fine Tree classifier is lightweight and interpretable, making it suitable for real-time applications in the IoV environment.

VIII. FUTURE ENHANCEMENT

The proposed system can be further enhanced by incorporating advanced learning models such as graph-

based deep learning models for better detection of attacks. The proposed system can be extended for real-time implementation using edge computing for faster detection in vehicular networks. The proposed system can be extended for privacy preservation by incorporating federated learning for secure data sharing. The proposed system can be extended for incorporating advanced learning models for effective detection of newly emerging cyber attacks. In addition, future work can be done for improving the scalability and multi-class attack detection for better performance in IoV networks.

REFERENCES

[1] "Future perspectives on Internet of Vehicles resource management: Digital twin-enabled edge computing frameworks," *Journal of Engineering and Applied Science*, 2025.

[2] "Toward generative AI-based intrusion detection systems for the Internet of Vehicles (IoV)," *Future Internet*, vol. 17, no. 7, p. 310, 2025.

[3] "A novel graph convolution–based immediate neighborhood extraction in VANET stability enhancement," *International Journal of Communication Systems*, Wiley, 2025.

[4] Upstream Security, *Global Automotive Cybersecurity Report 2025: Trends in Automotive and Smart Mobility Security*, Mobex, 2025.

[5] Upstream Security, "When API security fails, mobility breaks: Lessons from 2025 cyber incidents," Oct. 2025.

[6] "Internet of Vehicles security threats, countermeasures, open challenges, and future research directions," *IEEE Internet of Things Journal*, Sep. 2025.

[7] "Securing the road ahead: A survey on Internet of Vehicles security powered by a conceptual blockchain-based intrusion detection system," *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 4, 2025.

[8] "Optimizing task migration for vehicular edge networks: A dual-layer graph neural network approach," *IEEE Transactions on Mobile Computing*, 2025.

[9] "ML-based categorical boosting with hybrid transfer learning for cyber threat intelligence in IoV," Springer, Oct. 2025.

[10] "Securing IoV environments with blockchain-integrated detection systems," *Cluster Computing*, vol. 28, p. 762, 2025.

[11] K. Zhang *et al.*, "Intrusion detection system incorporating randomized PCA and online wavelet extreme learning machine."

[12] M. L. Bouchouia *et al.*, "Metrics of cybersecurity for AI-based in-vehicle intrusion detection systems."

[13] Torre *et al.*, "Privacy-friendly federated learning-based intrusion detection using convolutional neural networks."

[14] Korium *et al.*, "Intrusion detection for cyberattacks in Internet of Vehicles environments," *Ad Hoc Networks*, vol. 153, p. 103330, 2024.

[15] Merzouk *et al.*, "Deep reinforcement learning-based intrusion detection and adversarial robustness."

[16] "GenVRAM dataset generator for vehicle-to-roadside attack simulation."

[17] Prakash *et al.*, "Vehicular network-based intelligent transport system using machine learning algorithms."

[18] Almehdhar *et al.*, "Advanced intrusion detection techniques for intelligent vehicle networks: A survey."

[19] Han *et al.*, "ECNet: Robust network traffic detection using multi-view features."

[20] Y. Zhang *et al.*, "False message detection in Internet of Vehicles through machine learning," *Information Processing & Management*, vol. 61, no. 6, p. 103827, 2024.

[21] S. Sharma and A. Kumar, "Dynamic topology challenges in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 1456–1472, 2024.

[22] R. Gupta *et al.*, "Feature extraction limitations in modern IoV intrusion detection systems," *Journal of Network and Computer Applications*, vol. 215, p. 103654, 2024.

[23] M. Ahmed *et al.*, "High-dimensional data challenges in cybersecurity: A review," *Computers & Security*, vol. 128, p. 103145, 2023.

[24] L. Zhang *et al.*, "Scalability issues in centralized intrusion detection systems," *Future Generation Computer Systems*, vol. 145, pp. 234–248, 2024.

[25] P. Kumar *et al.*, "Resource-constrained intrusion detection for edge-based vehicular networks," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7890–7905, 2024.

[26] A. Barredo Arrieta *et al.*, "Explainable artificial intelligence for cybersecurity: A review," *Information Fusion*, vol. 98, p. 101845, 2023.

[27] T. Wang *et al.*, "Adaptive intrusion detection for evolving cyber threats in intelligent transportation systems,"

IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 3, pp. 2156–2171, 2024.

[28] J. Zhang, X. Fan, and Z. Zhao, "A hybrid intrusion detection model based on spatial-temporal graph neural networks," *Scientific Reports*, vol. 15, p. 34736, 2025.

[29] Y. Ye *et al.*, "GDT-IDS: Graph-based decision tree intrusion detection for CAN networks," *Journal of Supercomputing*, 2025.

[30] Y. Sun *et al.*, "Topology control based on dynamic graph embedding in IoV," *Journal on Communications*, vol. 43, no. 6, pp. 108–119, 2022.

[31] H. Wang *et al.*, "Structural dependency modeling for network intrusion detection," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2345–2360, 2024.

[32] F. Li *et al.*, "Graph-theoretic features for anomaly detection in vehicular networks," *Computer Networks*, vol. 235, p. 109876, 2024.

[33] S. Kim *et al.*, "Temporal graph analysis for coordinated attack detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 1876–1891, 2024.

[34] M. Chen *et al.*, "Feature fusion strategies for hybrid intrusion detection systems," *Pattern Recognition Letters*, vol. 178, pp. 123–129, 2024.

[35] R. Singh *et al.*, "Interpretable machine learning for network security," *Computers & Security*, vol. 132, p. 103345, 2024.

[36] M. Lee *et al.*, "Comparative evaluation of intrusion detection systems on IoV datasets," *IEEE Access*, vol. 12, pp. 45678–45695, 2024.

[37] K. Park *et al.*, "Real-time intrusion detection for resource-constrained vehicular environments," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 8, pp. 11234–11250, 2024.