Minimax Theory and its Applications
Volume 11 (2026), No. 1, 91 - 109

Privacy-Preserving Integrity Assurance for Optimized Vehicular Network Performance in Edge Computing

Vijayalaxmi Saibaba Sadlapur[1], Nayana Hegde[2]

[1] REVA University, Bengaluru, Selection Grade Lecturer, Government Polytechnic Zalaki, Vijayapura, Karnataka, India
[2]Assistant Professor, REVA University, Bengaluru, India

Abstract

The rapid evolution of the Internet of Vehicles (IoV) and Vehicular Edge Computing (VEC) has led to increased data traffic and communication challenges, necessitating efficient and secure models for seamless connectivity. Traditional models struggle with maintaining high communication efficiency and reliability in dynamic vehicular environments. This study addresses these challenges by introducing the Privacy-Preserving Integrity Assurance (PPIA) State-Action Reinforcement Learning Game (SARLG) (PPIA-SARLG) model. The primary objective of PPIA-SARLG is to enhance communication efficiency, reduce failure rates, and improve throughput in urban and highway scenarios. The proposed model was implemented using the SIMITS simulator, integrated with NS3, and evaluated under realistic conditions using the CICIoV2024 dataset for cyberattack simulation. Experimental results demonstrated that PPIA-SARLG achieved an average improvement of 19.71% in communication efficiency, reduced communication failures by 18.36%, and enhanced throughput by 15.79% compared to Two-Factor Privacy-Preserving Protocol Authentication (TF-3PA). The novelty of PPIA-SARLG lies in its adaptive learning mechanism, which dynamically optimises packet transmission in high-mobility networks.

Keywords: IoV VEC, PPIA-SARLG, Cyberattack mitigation, Reinforcement Learning

1. Introduction

Vehicular Ad Hoc Networks (VANETs) are a crucial component of modern Intelligent Transportation Systems (ITS), enabling communication among vehicles, infrastructure, and pedestrians. These networks facilitate real-time data exchange to enhance road safety, traffic management, and overall driving efficiency. With the rise of the Internet of Vehicles (IoV), the integration of VANETs with broader internet-based services has become essential, requiring ultra-reliable and low-latency communication (URLLC) [1]. However, current wireless technologies such as 4G and 5G face limitations in handling massive connectivity, ultra-low latency, and high-speed data processing demands of IoV [2]. This is where 5G and 6G networks play a vital role, providing unprecedented network speed, enhanced reliability, and intelligent edge computing capabilities to ensure seamless VANET-IoV integration. Moreover, the incorporation of 5G supports real-time data analytics and ultra-fast communication, providing a highly efficient and secure intelligent transportation ecosystem. Also, the VANETs support a wide range of applications, including traffic management, emergency communication, and collision avoidance [3]. Real-time vehicle communication helps prevent accidents by alerting drivers to potential hazards such as sudden braking, lane changes, and roadblocks. Additionally, VANETs facilitate efficient traffic flow by dynamically adjusting traffic signals based on congestion levels and enable seamless internet access for passengers, location-based services, and automated toll payment systems. With autonomous driving on the rise, VANETs provide critical support for vehicle coordination, enhancing overall road safety.

An application of VANET, Advanced Driver Assistance Systems (ADAS), leverages an array of sensors, radars, and cameras to enhance driving safety and automation [4]. These systems assist drivers in tasks such as lane-keeping, adaptive cruise control, blind-spot detection, and emergency braking. The effectiveness of ADAS relies on accurate sensor data, which must be processed in real-time to make split-second decisions. LiDAR, radar, and high-resolution cameras provide a comprehensive environmental understanding, allowing ADAS to detect pedestrians, obstacles, and other vehicles [4]. However, the sheer volume of data generated by these sensors necessitates efficient data fusion and aggregation for high-accuracy decision-making. For ADAS to function

optimally, effective sensor fusion is crucial. Hence, combining data from multiple sensors minimises errors and enhances situational awareness. However, achieving high accuracy in data aggregation while maintaining low latency remains a challenge. In real-world driving scenarios, delays in processing can lead to catastrophic accidents. Therefore, an efficient data aggregation mechanism is required to ensure that ADAS receives accurate, real-time information for decision-making. The challenge lies in handling massive sensor data streams efficiently, especially in dynamic urban environments where rapid changes in traffic conditions demand instant responses. Despite the advantages of VANET, current VANET models face significant limitations in data processing, security, authentication, and aggregation [5], [6]. The decentralised nature of VANETs makes them vulnerable to various cyber threats, including spoofing attacks, Distributed Denial of Service (DDoS) attacks, and false data injection [7], [8]. Attackers can manipulate or inject fake data into the network, leading to incorrect traffic management decisions and safety hazards. Additionally, traditional VANET models struggle with secure data aggregation, making it difficult to filter out malicious or tampered data. The lack of efficient authentication mechanisms further exacerbates these security vulnerabilities.

Further, the Vehicular Edge-Cloud (VEC) plays a pivotal role in addressing the challenges faced by VANETs, particularly in terms of security, authentication, and efficient data processing [9], [10]. VEC extends cloud computing capabilities to the edge of the network, reducing latency and enabling real-time decision-making. By offloading computational tasks to edge servers, VEC alleviates the burden on individual vehicles while ensuring seamless and secure data processing. Additionally, VEC provides an extra layer of security by filtering and verifying incoming data before it reaches the central cloud. In ADAS, VEC plays a crucial role by handling high-computation tasks such as image processing, object detection, and path planning [11]. These sensors and cameras in ADAS systems continuously capture and mosaic images to detect road conditions, obstacles, and vehicle movements. However, due to the computational intensity of these tasks, offloading data to VEC is essential for ensuring real-time responses. While offloading enhances processing efficiency, it also introduces security risks, including data privacy breaches and integrity threats [12]. Ensuring secure transmission of data between vehicles and edge servers is crucial to maintaining system reliability. Moreover, one of the major concerns in VEC-assisted ADAS is data security during offloading and processing [13]. Privacy and integrity threats arise when malicious entities intercept or manipulate transmitted data. Traditional security mechanisms, such as blockchain-based reputation models [14], [15], have been proposed to counter these threats. However, these methods come with drawbacks such as high computational overhead, low throughput, communication failures, and reduced efficiency. Additionally, during a cyberattack, VECs consume excessive energy and processing time when handling large image workloads, further impacting system performance.

To address these security and efficiency challenges, this work proposes a novel Privacy-Preserving Integrity Assurance (PPIA) mechanism, designed to authenticate vehicles, mitigate attack impacts, and eliminate malicious entities from VANETs. PPIA enhances data reliability by ensuring that only verified data is used for decision-making, reducing the risk of compromised information influencing traffic management and ADAS functionalities. Furthermore, this work introduces the State-Action Reinforcement Learning Game (SARLG) model to enhance data authentication, privacy protection, and integrity assurance. SARLG leverages Reinforcement Learning (RL) to dynamically adjust authentication thresholds based on real-time traffic conditions and potential security threats. Unlike traditional security models, SARLG is designed for both trusted and untrusted edge servers, ensuring robust protection even in heterogeneous network environments. The contribution of the PPIA-SARLG model is as follows.

This work presents the PPIA model, which ensures secure data aggregation and authentication of vehicles, mitigating the impact of malicious attacks and removing compromised nodes from the VANET. This work also introduces an RL-based approach to dynamically adjust authentication thresholds, enhancing data security and privacy protection. This work reduces latency and computational overhead by securely offloading vehicle sensor data to VEC for real-time processing. This work reduces communication failures and improves throughput by optimising data exchange between vehicles and edge servers. This work also minimises energy consumption and processing delays when handling large image workload tasks, especially during cyberattacks. This work enhances vehicles' functionalities in VEC by ensuring accurate and trustworthy data fusion from multiple sensors and radars, leading to improved decision-making.

The manuscript is organised in the following way. In Section II, the literature survey is presented, which discusses different data transmission, aggregation, and RL-based approaches used in VANET and VEC for providing security and for offloading data from vehicles to the edge-layer of VEC.

Further, Section III presents the PPIA, SARLG, and reputation model used in this work for providing secure data aggregation, data authentication, data privacy, and data reliability. Section IV presents the results of the PPIA-SARLG model and compares it with the existing approach. Finally, Section V presents the conclusion and future work for PPIA-SARLG.

2. Literature Survey

The literature survey presents various data transmission, aggregation, and RL-based approaches used in VANET and VEC to enhance security and facilitate efficient data offloading from vehicles to the edge layer of VEC. Z. Zeng et al. [16] presented an approach called Blockchain-Collaborative Service-based Conditional Privacy-Preserving (BCS-CPP) for providing data privacy in VANET-based IoV. The BCS-CPP approach utilised contract-based Condition-based Privacy-Preserving Authentication (CPPA) for solving the issue of key-escrow and public-key certification supervision, providing better privacy-based secured location-based service. The evaluations on providing security showed that the BCS-CPP approach reduced communication overhead and computation. Moreover, the BCS-CPP provided a constant communication overhead as the number of users increased in the network. T. Nandy et al. [17] discussed different kinds of security services, security threats, characteristics, and architectures of VANET. Also, this work discussed the different Intrusion Detection System (IDS) architectures for VANETs. Further, this work also discusses the different approaches, datasets, and tools used for simulation. Further, this work also discussed the need for resource-efficient and adaptive IDS approaches for handling security threats in VANETs. M. A. Al Sibahee et al. [18] presented an effective authentication approach, which was built on a cryptography approach, called Two-Factor Privacy-Preserving Protocol Authentication (TF-3PA) in IoV. In their approach, they used Physical Unclonable Function (PUF) for providing two-factor authentication. The PUFs generated random passwords and identities, which provided better authentication for the vehicles in VANET. The evaluations were conducted considering the Real-or-Random (RoR) approach, which provided real-time simulation. Findings showed that the approach reduced energy consumption and computation and provided better security in comparison with existing methods.
Z. Ma et al. [19] presented an authentication approach for solving issues related to connection with roadside units, called Blockchain-based Secured Distributed Authentication (BSDA) for IoVs. In BSDA, first, the process of processing data and storing data is decentralised in the edge layer, which reduces computation time, response time, and communication delay, considering a trusted authority. Further, for authentication, smart contracts were used, and for achieving an automated trigger for authentication, a Practical-Byzantine Fault-Tolerant Consensus (PBFT) approach was presented, which added authentication data to the blockchain ledger, such that the outcome of authentication could be reused. Further, for evaluation, the RoR approach and the Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool were used. Findings from the evaluation show that the BSDA approach reduced computation cost, delay, and overhead and showed better communication. C. Xu et al. [20] presented an Intelligent Secured Task-Offloading and Caching (ISTOC) approach for Vehicle Edge-Computing (VEC), where a digital twin-assisted VEC was established, which migrated the blockchain security model from physical space to cyberspace, providing dynamic vehicle handovers. Also, this work proposed a Diffused-Delegated Byzantine Fault-Tolerance (D2BFT) approach. The main aim of this approach was to reduce task computation latency and provide better throughput. To achieve this objective, an optimisation problem was developed that included caching, computation, and communication, which addresses issues of blockchain stability, task deadline, cache storage, computation, bandwidth, and task splitting. Because of the nonconvexity of the objective, the problem was transformed into a Markov-Decision-Process (MDP). To solve the MDP, a Multi-Agent Double Actor-Critic (MADAC) approach is presented. Evaluations of the security approach showed that the MADAC-ISTOC approach provided better outcomes in comparison with existing approaches in terms of convergence, latency, and throughput.
J. Akram et al. [21] presented an approach called Unmanned Aerial Vehicle Guard (UAVGuard) for providing security for the UAVs deployed in the VEC environment. In this work, they utilised the advantages of Graph-Neural-Network (GNN) for identifying gradient-based attacks. From the analysis of GNN, found that GNN sometimes overfits training data, providing inaccurate results. Hence, this work aimed to provide a framework that utilised Community-Preserving Self-Supervised Tasks as a regularisation approach. Evaluations were conducted on three datasets, where the approach showed better outcomes. X. Lu et al. [22] presented a reputation-based approach for VEC, which incorporated a secure offloading approach for VEC and provided security against selfish and

eavesdropping attacks. The approach consisted of a 3-level structured framework for every vehicle and utilised the reputation achieved using blockchain for optimising edge-node selection, power allocation, and offloading ratio. This, in turn, reduced latency, attack rate, and energy consumption. Moreover, this work utilised a punishment function that avoided data leakage and task failures. Also, a multi-agent deep RL-based secured offloading approach was presented for improving secured offloading performance. Findings show that the approach achieved better outcomes when compared with existing approaches. Z. Li et al. [23], for providing a solution for security, offloading, and data transmission, employed Physical-Layer-Security (PLS) and designed a workflow for addressing the issue of Joint-Secure-Offloading and Resource-Allocation (JSORA) in VEC. The workflow approach modelled authentication of various vehicles using resource clusters on edge-servers and accurately reflected release and occupancy of every resource unit. To solve the problem of JSORA due to its complexity, a Filtered-Deep RL-based Secured Offloading and Allocation (FDRL-SOA) was developed, which controlled resource allocation and offloading in clusters. The findings from simulations showed that the FDRL-SOA approach reduced cost, latency, and energy consumption. Y. Chen et al. [24] presented an approach that used idle vehicles in VEC for connecting to the edge layer and for coordination and authentication presented a Multi-Stage Multi-Leader Multi-Follower Stackelberg Game (MSMLMFS) approach, which provided better authentication. For addressing the problem of data asymmetry among vehicles and vehicle operators, introduced incentive-compatibility and individual rationality constraints using contract theory for analysing and ensuring the effectiveness of contracts. Further, employed backward induction for simplifying the game model to convex optimisation and for proving Nash equilibrium points. Findings show that the MSMLMFS approach achieved better results. Table 1 shows the summary of existing work designed to provide security during the offloading process in IoV-VEC.

Table 1: Comparative Summary of Existing IoV–VEC Security and Offloading Approaches

Ref	Method	Privacy Level	Authentication Scheme	Computational Overhead	Data Reliability	RL Integration
[16]	BCS-CPP	High (conditional privacy)	CPPA + Blockchain	Medium	No	No
[18]	TF-3PA	High (PUF-based)	Two-factor PUF authentication	Low	No	No
[19]	BSDA	Medium	Blockchain + PBFT	Medium	No	No
[20]	ISTOC	Medium	Blockchain + D2BFT	High	Partial	MADAC
[22]	Reputation-MARL	Medium	Blockchain reputation	High	Partial	Multi-agent DRL
[23]	FDRL-SOA	Low	Physical-layer security	High	No	DRL
[24]	MSMLMFS	Low	Stackelberg game	Medium	No	No

In the literature survey, most existing works in VANET and IoV security have primarily focused on either privacy preservation or authentication. For instance, Zeng et al. [16] proposed the BCS-CPP approach to enhance privacy in IoV, while Al Sibahee et al. [18] introduced TF-3PA for secure authentication using PUF. Similarly, Ma et al. [19] developed BSDA, utilising blockchain and PBFT for authentication, and Xu et al. [20] introduced ISTOC to improve task offloading security. Other works, such as Akram et al. [21] and Lu et al. [22], leveraged UAV-based security and reputation-based methods, respectively. Also, Z. Li et al. [23] and Y. Chen et al. [24] mainly focused on offloading, but failed to address security issues. However, despite their advancements, most approaches have not adequately addressed data reliability, fusion, and aggregation challenges in dynamic vehicular environments [25], [26]. Security threats such as spoofing and DDoS attacks still impact data integrity and decision-making in ADAS and VEC environments [27], [28].

The overall research gap identified is that most of the existing approaches focus on either privacy preservation or authentication or task offloading, but they fail to jointly address: Secure data

aggregation, reliable data validation, dynamic malicious behaviour, incentive-based privacy compensation, and Lightweight RL-based threshold optimisation. Hence, this work proposes the PPIA-SARLG model to jointly ensure: privacy-preserving aggregation, reliable authentication, robust attack mitigation, RL-based threshold optimisation, and Reputation-driven incentive control while maintaining efficiency in trusted and untrusted edge-cloud environments. In the next section, the PPIA-SARLG model is discussed in detail.

3. Methodology

This section first discusses the PPIA model, which provides secure aggregation and reliable authentication. Further, this section presents the SARLG model for data reliability. Finally, this section presents the reputation model.

3.1. Architecture

Consider a VANET environment in which all vehicles are interconnected, as illustrated in Figure 1. Furthermore, the vehicles in the VANET are connected to roadside units (RSUs) or the edge layer, where simple and delay-sensitive tasks are offloaded to the edge, while computationally intensive tasks are forwarded to the cloud layer for Advanced Driver Assistance Systems (ADAS). Since the communication links between vehicles, the edge layer, and the cloud layer are established over wireless channels, they are vulnerable to security threats such as DoS and spoofing attacks. To address these vulnerabilities, this work first introduces a secure aggregation mechanism that authenticates participating vehicles and identifies and removes malicious nodes from the VANET before data aggregation and offloading. Table 2 shows the notation used in the Proposed Model.

Figure 1. VEC Architecture

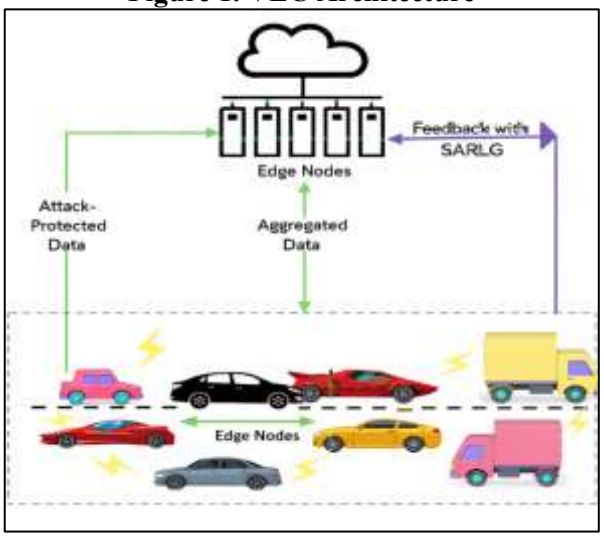

Table 2. Notation Used in the Proposed Model

Symbol	Description
x_k	k-th vehicle
z_k	Sensor data from the vehicle
$\tilde{z}_k$	Perturbed data
δ_k	Gaussian noise
P	Total vehicles
P'	Reliable vehicles
y_k^m	Weight
t_k^m	Reputation
ϵ_k	Privacy parameter
r_c^k	Compensation
θ	Detection threshold
u_m	SARSA state
$Q(u,\theta)$	Q-value
τ	Learning rate
τ	Discount factor

3.2. Privacy Preserving Integrity Assurance (PPIA) Model

For secure aggregation, this work first considers that all vehicles present in VANET are in VEC, and lets the vehicles present in VANET be represented as $X = \{x_1, x_2, \dots, x_P\}$, where P Denotes the total number of vehicles present in VANET, which are generating a large set of workload tasks data collected using sensors, represented as $Z = \{z_1, z_2, \dots, z_P\}$, which is then transmitted towards the edge layer in VEC. Also, consider the data collected by the sensors as $z_k \in T$, which defines large and complicated data. Further, this work determines the state of the vehicle, i.e., whether it is in a normal state or malicious. For determining if a vehicle x_k Is malicious; this work utilises a normalised security-reputation-based result, denoted as t_k, which ranges between 0 and 1 Representing non-malicious and malicious, respectively. Further, for aggregating sensitive data collected by vehicle sensors in VEC, this work utilises Eq. (1).

$$a = \frac{1}{P}\sum_{k=1}^{P} \quad z_k \tag{1}$$

Using Eq. (1), an average aggregation of sensitive data generated by vehicles is done. Nevertheless, this approach introduces privacy concerns, as the VANET consists of both normal and malicious vehicles. Also, there is a chance that a compromised VANET may receive tampered data from malicious vehicles or can extract sensitive data, making it susceptible to spoofing attacks. Hence, for addressing privacy issues, the secure aggregation model incorporates an approach that preserves vehicle data privacy. In the proposed PPIA approach, consider the data collected as z_k, to ensure security, a Gaussian noise is added, denoted as δ_k, which follows a normal distribution having a mean of zero and a variance σ^2, thereby ensuring randomness in the noise generation approach, i.e., $\delta_k \sim P(0, \sigma^2)$. Further, the overall data, which consists of sensor-collected data and noise, is then transmitted to other vehicles or towards the edge layer, which is represented as $\tilde{z}_k = z_k + \delta_k$. By adding noise in Eq. (1) and by applying an approximation to make the process simple, Eq. (1) can be represented as Eq. (2).

$$\hat{a}^m = \sum_{k=1}^{P'} \quad y_k^m \tilde{z}_k^m \tag{2}$$

In Eq. (3), P' denotes the correct data of collected data, and y_k^m is a dynamic weighted approximated variable. Consider that the δ_k generates unique noise, which can be represented $\delta_k \sim P(0, (\sigma_k)^2)$, where $(\sigma_k)^2$ is represented as Eq. (3). In Eq. (3), α^2 denotes adjacent sensors and is true only when $k = k_0$ and ϵ_k denotes the KL-privacy preserving parameter for. Also, when the collected data goes through a noise generation approach, the identification of the original data raises issues. Also, generating unique noise every time for the collected data creates privacy issues. Hence, to solve the following issues, an incentive variable ζ is presented in this work, which is evaluated using Eq. (4).

$$(\sigma_k)^2 = \frac{\alpha^2}{2\epsilon_k} \tag{3}$$

$$\zeta = \left[\underline{a} - \hat{a}\right] \tag{4}$$

In Eq. (4), $\underline{a}$ denotes the true average for the computation of $\tilde{z}_k$ and $\hat{a}$ denotes aggregation accuracy for the computation of $\tilde{z}_k$. Hence, utilizing ζ Variable, data is aggregated, having better security outcomes, ensuring integrity and privacy. The ζ Variable is always kept less in this work for achieving better data integrity and for preserving the data privacy of the vehicle. x_k. The complete process of achieving less value for ζ The variable is discussed in detail in the Hypothesis.

Hypothesis: Consider that the evaluated outcome $\hat{a}$ converges to the average $\underline{a}$ having the closest variance of ζ variable, considering different values of r in range $(0,1)$, as presented in Eq. (5), hence, using this, the weighted variable y_k and ϵ_k for x_k These are achieved using the following hypothesis. Further, considering the following hypothesis, the original data for x_k Without noise is achieved using Eq. (6). Also, added noise in the original data is achieved using Eq. (7). By considering. $Variance(\delta_k) = 2\sigma_k^2$ In Eq. (7), Eq. (8) is obtained. Further, by applying probabilistic approximation on Eq. (8), which ensures a lower deviating factor for every ζ Variable, Eq. (9) is obtained.

$$\zeta = \frac{\alpha}{\sqrt{1-r}}\sqrt{\sum_{k=1}^{P'} \quad (y_k^m)^2 \frac{1}{\epsilon_k}} \tag{5}$$

$$a = \sum_{k=1}^{P'} y_k z_k \tag{6}$$

$$= \sum_{k=1}^{P'} y_k^m (z_k + \delta_k) = a + \sum_{k=1}^{P'} y_k \delta_k \tag{7}$$

$$Variance\left(\sum_{k=1}^{P'} y_k \delta_k\right) = 2\sum_{k=1}^{P'} (y_k^m)^2 \sigma_k^2 \tag{8}$$

$$Pr[|\hat{a} - a| \geq \zeta] \leq \frac{2}{\zeta^2}\sum_{k=1}^{P'} (y_k^m)^2 \sigma_k^2 \tag{9}$$

Consider $Pr[|\hat{a} - a| < \zeta] = r$, substitute in Eq. (9) and from this, Eq. (10) is obtained. By finding ζ In Eq. (10), Eq. (11) is achieved. Further, by substituting Eq. (3) in Eq. (11), Eq. (5) is achieved. For the following hypothesis, the computational cost to ensure the privacy of x_k is attained using Eq. (12). In Eq. (12), μ_k It is a non-negative variable representing vehicles' privacy. To ensure integrity assurance accuracy, denoted as rc_k And privacy-preservation using Eq. (14), it has to ensure the conditions presented in Eq. (13).

$$\frac{2}{\zeta^2}\sum_{k=1}^{P'} (y_k^m)^2 \sigma_k^2 = 1 - r \tag{10}$$

$$CapZeta\zeta = \frac{\sqrt{2}}{1-r}\sqrt{\sum_{k=1}^{P'} (y_k^m)^2 \sigma_k^2} \tag{11}$$

$$e_k = \mu_k (\epsilon_k)^2 \tag{12}$$

$$rc_k - \mu_k (\epsilon_k)^2 \geq 0, \ \ \forall k \in [1, P] \tag{13}$$

When best tradeoff using rc_k is achieved, then only x_k transmits the original and added noise data using ϵ_k parameter to other vehicles or towards the edge layer. As seen from the hypothesis, for achieving the least ζ, $\sum_{k=1}^{P} \frac{(y_k^m)^2}{\epsilon_k}$ Has to be ensured. Also, the VANET has to penalise if any privacy breach occurs using a variable. D. To ensure the best tradeoff among data-integrity accuracy and privacy-preserving data, this work presents an incentive method for finding the best. rc_k and ϵ_k Using Eq. (14).$such\ that\ rc_k - \mu_k(\epsilon_k)^2 \geq 0, \sum_{k=1}^{P'} rc_k \leq D, rc_k \geq 0, \epsilon_k > 0, k \in [1, P']$ Using Eq. (14), the best rc_k and ϵ_k Are achieved using Eq. (15) and Eq. (16), respectively.

$$\sum_{k=1}^{P'} \frac{(y_k^m)^2}{\epsilon_k} \tag{14}$$

$$rc_k^* = \sqrt{\frac{(y_k^m)^2 (\mu_k)^{-\frac{2}{3}}}{\sum_{l=1}^{P'} (y_l^{m-1})^2 (\mu_l)^{-\frac{1}{2}}} D} \tag{15}$$

$$Script\epsilon_k^* = \sqrt{\frac{(y_k^m)^2 (\mu_k)^{-\frac{2}{3}}}{\sum_{l=1}^{P'} (y_l^{m-1})^2 (\mu_l)^{-\frac{1}{3}}} D} \tag{16}$$

Using Eq. (15), the PPIA model ensures enhanced privacy preservation. Further, by using position evaluation, if any attack occurs, the exact location where the attack took place can be identified. However, if an attack manipulates transmitted data, the PPIA model addresses the following issue using a reliable authentication model, which utilises a state-changing approach. For the reliable authentication model, consider two scenarios, J_0, where transmitted data maintains strong security, and J_1, where security is provided, yet there is a possibility of an attack. In J_1 In a scenario, the attack can be identified by monitoring transmitted data, as it continuously changes with varying reputation values. In the normal state, transmitted data follows a relationship. $R_h = R(J_1|J_0)$, while in attack state, it follows $R_0 = R(J_0|J_1)$. Using state-changes, a variance N is determined using $N = \| z_k^m - \hat{z}_k^m \|^2$, where z_k^m is a previous state-changing variable and $\hat{z}_k^m$ Is the next state-changing variable, which establishes whether data is in normal or in attack state, i.e., if data transmitted changes its state, the following vehicle is swapped as a malicious vehicle, as $\hat{z}_k^m \leftarrow z_k^{m-1}$, else is kept as a normal vehicle as $\hat{z}_k^m \leftarrow z_k^m$. Using NThe attack is identified as presented in Eq. (17). It is important to note that malicious data introduces computational overhead, which leads to high delay and loss in data as malicious data compromises other data. Hence, consider I_0, which represents overhead because of malicious data and I_1 represents overhead because of non-malicious data, such that $I_0 > I_1 > 0$. From this consideration, attack probability $T(\vartheta, R)$ can be identified using Eq. (18). Using Eq. (18), the impact of malicious packets on overhead and the evaluation of attack probability in data is determined. Further, for providing better security, this work presents the SARLG model, which provides an approach for validating data reliability, ensuring a more secure and reliable data aggregation system. The complete process of PPIA, which forwards reliable data to SARLG, is provided in Algorithm 1.

$$N \lessgtr_{J_1}^{J_0} (\vartheta) \tag{17}$$

$$CapT(\vartheta, R) = \Big(I_1\big(1 - R_h(\vartheta)\big) - ER_h(\vartheta)\Big)\left(1 - \sum_{k=1}^{P_o} rcs_k\right) + (I_0\big(1 - R_o(\vartheta)\big) - ER_o(\vartheta)) \sum_{k=1}^{P_o} rc_k \tag{18}$$

Algorithm 1: PPIA Aggregation and Incentive Mechanism

1. Initialise vehicles x_k, reputation $t_k = 0.5$
2. Add Gaussian noise δ_k to data
3. Compute weighted aggregation
4. Estimate the accuracy deviation ζ
5. Optimise r_c^k and ϵ_k using Eq. (15) and (16)
6. Penalise low-reputation vehicles
7. Forward reliable data to SARLG

3.3State-Action Reinforcement Learning Game (SARLG) Model

In recent years, RL has proven effective in the identification of best outcomes. Since attack frequency in VANET and VEC environments is often unknown, determining the best test threshold is important for the validation of reliable data. Hence, this work employs SARSA (State-Action-Reward-State-Action) in SARLG because of its better stability when compared with Q-Learning. Alongside, on-policy learning is stable under dynamic attacks, has a lower energy cost than DQN, faster convergence in continuous threshold control, and avoids Q-learning overestimation. Table 3 shows comparative reasons and benefits of choosing SARSA over Q-learning and DQN-based methods.

Table 3: SARSA instead of Q-learning or DQN

Algorithm	Convergence	Energy	Stability
Q-Learning	Medium	Low	Low
DQN	High	High	Medium
SARSA	High	Low	High

SARSA evaluates one-step expected reward, providing faster convergence and reduced energy usage. For validating data reliability, the SARLG model initially considers Eq. (17) for assessing every data point from P For a time slot. Hence, from this, the false attack-rate and missed attack-rate from the reliable authentication model in the $m-1^{\text{The}}$ slot from the state u_m is denoted as presented in Eq. (19).

$$u_m = \tag{19}$$

Further, this work models threshold estimation as a continuous-space MDP, for reducing complexity, for which the state-space α_m and action-space β_m In SARSA are quantised to multiple levels. Specifically, the error rates are split into $Z+1$ levels, whilst the test threshold ϑ is selected from $A+1$ Levels. More levels (i.e., larger from Z orA) enhances validation accuracy, but increase computation complexity because of a greater number of actions for every state. Moreover, the validation accuracy is evaluated considering simulation by evaluating the failure and success attack detection rate. Further, the VEC selects action. ϑ_m based on the state u_m for maximising utility W_m, as presented in Eq. (20).

$$W_m = w_t^m(\vartheta, R) \tag{20}$$

As malicious vehicles in VANET can negatively impact reliable data validation, this reduces VEC's utility. Moreover, because of the increasing number of malicious vehicles in VANET, the PPIA model performance degrades; hence, the data reliability is verified using the SARLG model to evaluate the effectiveness of the validation method and allocate rewards and punishments for vehicles. Nevertheless, the PPIA optimises the test threshold for achieving higher VEC utility in comparison with existing methods. Further, for every time slot m, after the selection of action ϑ_m, next-state u_{m+1} Is observed. Also, the next state outcome is dependent on Eq. (17), ϑ_m and the authenticity of input data. For data reliability validation, in SARLG, the SARSA incorporates a learning rate. $\tau \in (0,1)$, which adjusts the weights of the Q-value function, represented as $Q(u_m, \vartheta_m)$, where the Q-value gets updated in VEC using Eq. (21). Further, in this work, the SARSA discount factor accounts for the uncertainty of future rewards. Hence, SARLG defines the state-value function as $X(u)$ which is updated using Eq. (22). In Eq. (22), $\pi(u_m)$ represents threshold selection probability ϑ for state u_m. In this SARLG model, ϵ-A greedy approach is adopted, which allows VEC for choosing sub-optimal action with a probability ϵ and the best action having probability $\epsilon - 1$. Hence, from this the best threshold ϑ^* is achieved using Eq. (23).

$$Q(u_m, \vartheta_m) \leftarrow (1-\tau) of\ Q(u_m, \vartheta_m) + \tau\big(W_m + \delta X(u_{m+1})\big) \tag{21}$$

$$X(u_m) \leftarrow \sum_{\vartheta \in \left\{\frac{1}{A}\right\} 0 \le n \le A} \pi(u_m) Q(u_m, \vartheta) \tag{22}$$

$$\vartheta^* = arg Q(u_m, \vartheta) \tag{23}$$

Further, for differentiation among malicious vehicles (which uploads tampered data) and normal vehicles (which submit perturbed data that maintains privacy-preserving properties), reputation-based metrics are used. Consider the reputation for k^{th} vehicle for time m as t_k^m, which is updated based on respective weights denoted as y_k^m. Also, consider absolute deviation for every data point from reference value as f_k and the maximum deviation across all data points as $f_\uparrow = \{f_k\}$. In a similar vein, the deviation for every data point from reference values for reliable data is denoted as f' and the maximum deviation across all data points for reliable data is denoted as $f'_\uparrow = \{f'_k\}$. Hence, from this, the reputation updates follow the following rules.

Rule 1: If $f_k \le f_\uparrow$, then the reputation value increases when f_k decreases, i.e., vehicles providing reliable data gain a higher reputation. Rule 2: If $f_k \ge f_\uparrow$, then the reputation value decreases when $f_k - f_\uparrow$ increases, i.e., vehicles providing unreliable data gain a lower reputation or their reputation value goes to 0. From the following rules, the reputation update function t_k^m is evaluated using Eq. (24).

$$t_k^m \leftarrow t_k^{m-1} + \frac{\varphi(f_k - f_\uparrow') + 1}{2} \cdot \left(1 - t_k^{m-1}\right) \cdot exp(-\psi|f_k) + \frac{\varphi(f_k - f_\uparrow') - 1}{2} \cdot t_k^{m-1} \cdot (1 - exp\{-\eta(f_k - f_\uparrow)\}) \quad (24)$$

In Eq. (24), ψ and η represent a negative real number, which scales t_k^m and $\varphi(z) = \{-1, z > 0 \; -1, z \leq 0$. The changes in ψ and η are analysed by monitoring changes in reputation for both malicious and normal vehicles, considering initial reputation values as 0.5. When ψ is kept small, it leads to faster reputation growth, while a higher η leads to a significant decline in reputation. Hence, in SARLG, only the reliable data is used for computing the weighted average. For weight evaluation y_k^m, consider reliable data verified using data-reliability validation represented as $z' = \{z_1, z_2, \ldots, z_{P'}\}$, hence, from this, the y_k^m is evaluated using Eq. (25).

$$y_k^m = \frac{\xi_k^m}{\sum_{k=1}^{P'} \xi_k^m} \quad (25)$$

In Eq. (25), $\xi_k^m = \frac{t_k^{m-1}}{\sum_{k=1}^{P'} t_k^{m-1}} + \frac{f'}{f_\uparrow'}$. The Eq. (15) and (25) ensure that only reliable data is utilised for improving aggregation accuracy. Also, using this rule-based approach, malicious vehicle receives lower values in comparison with normal vehicles because of their poor reputation, even if they later contribute reliable data. Conversely, normal vehicles receive reduced values and reputation penalties if they begin submitting unreliable data. However, if malicious vehicles consistently provide reliable data, their reputations improve, increasing their value over time. Similarly, normal vehicles can become malicious if they repeatedly submit unreliable data, causing their values to decline. Overall, the combined effect of the incentive mechanism and reputation update strategy effectively penalises malicious vehicles, ensuring a more secure and reliable data aggregation system using PPIA-SARLG with lesser computational complexity as shown in Table 4.

Table 4. Complexity Analysis

Component	**Time Complexity**
Noise addition	$O(P)$
Reputation update	$O(P')$
SARSA update	$O(\|S\|\|A\|)$
Aggregation	$O(P')$
Total per iteration	$O(P + \|S\|\|A\|)$
Space complexity	$O(P + \|S\|\|A\|)$

4. Result And Discussion

This section evaluates the performance of the PPIA-SARLG model and compares it with the TF-3PA model [18] in an IoV-VEC environment [19], [20]. The evaluation was conducted based on key performance metrics, including overall throughput, communication efficiency, communication failure rate, energy consumption, and workload execution time. Both PPIA-SARLG and TF-3PA were implemented using the SIMITS simulator [29], [30] combined with Cloudsim [28] for designing VEC, which provides a realistic propagation model. The IEEE 802.11 6G standard gateway was utilised within SIMITS to model the IoV-VEC environment. The simulator was developed using the C# programming language and integrated with the NS3 network simulator. To simulate IoV-based cyberattacks, the CICIoV2024 dataset was used, which contains records of Denial-of-Service (DoS) and spoofing attacks [31], [32]. The detailed simulation parameter used for simulating the experiment is shown in Table 5.

Table 5. Simulation Parameters

Parameter	**Value**
Learning rate (τ)	0.1
Discount factor (γ)	0.9
ε-greedy	0.1
Vehicles	50, 100

Attack rate	10–40%
Dataset	CICIoV2024
Simulator	NS3-based SIMITS
Edge-cloud layer	Cloudsim

4.1. Communication Efficiency

Communication efficiency plays a crucial role in evaluating the performance of vehicular networks, particularly in scenarios involving high mobility and varying traffic densities. Figures 2 to 5 show the communication efficiency of the PPIA-SARLG model in comparison to TF-3PA in different vehicular environments, namely urban and highway settings, with varying vehicle densities of 50 and 100. In an urban environment with 50 vehicles, as presented in Figure 2, the PPIA-SARLG model consistently outperforms TF-3PA across all instances. Initially, at lower vehicle densities, the difference between the two models is minimal. However, as vehicle density increases, PPIA-SARLG exhibits a more significant improvement. On average, the PPIA-SARLG achieves 23.62% better communication efficiency compared to TF-32PA. The performance of PPIA-SARLG is even better in an urban environment with 100 vehicles, as presented in Figure 3. At initial instances, both models exhibit similar communication efficiency; however, as the vehicle density increases, PPIA-SARLG demonstrates superior efficiency. On average, the PPIA-SARLG achieves 21.97% better communication efficiency compared to TF-32PA.

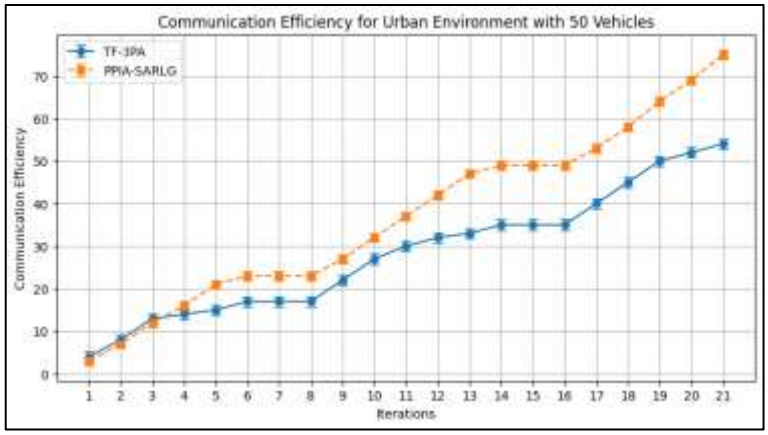

Figure 2. Communication efficiency performance for an urban environment considering 50 vehicles.

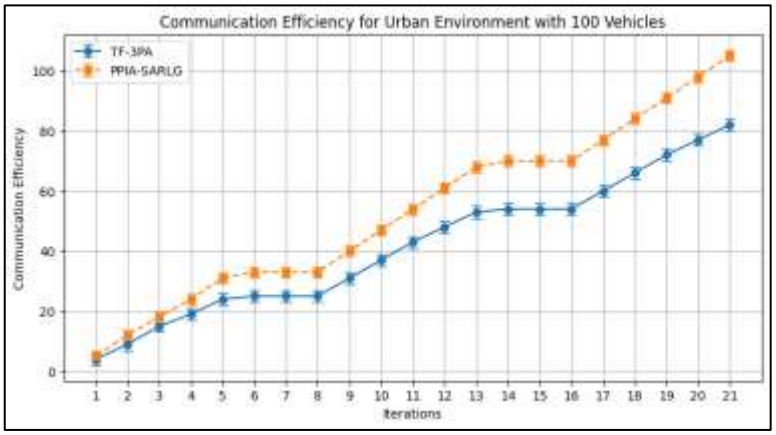

Figure 3. Communication efficiency performance for an urban environment considering 100 vehicles.

In the highway environment with 50 vehicles, as presented in Figure 4, the PPIA-SARLG model shows notable improvements over TF-3PA. Due to higher mobility and rapid vehicle movement on highways, efficient communication is essential for maintaining seamless connectivity. On average, the PPIA-SARLG achieves 25.40% better communication efficiency compared to TF-32PA. The impact of PPIA-SARLG is further evident in the highway environment with 100 vehicles, as presented in Figure 5. The model maintains a steady increase in communication efficiency as vehicle density rises. On average, the PPIA-SARLG achieves 7.83% better communication efficiency

compared to TF-32PA. On average, PPIA-SARLG achieves 19.71% better communication efficiency compared to TF-3PA across urban and highway environments. These results show that PPIA-SARLG enhances communication efficiency by reducing delays, improving data exchange reliability, and ensuring seamless connectivity, particularly in high-mobility vehicular networks.

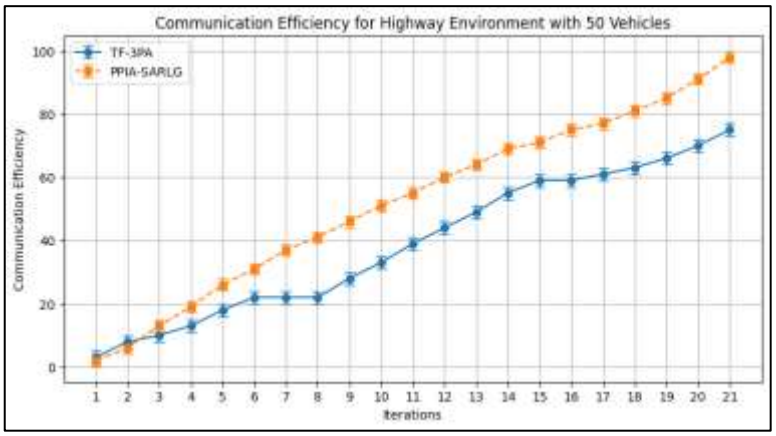

Figure 4. Communication efficiency performance for a highway environment considering 50 vehicles.

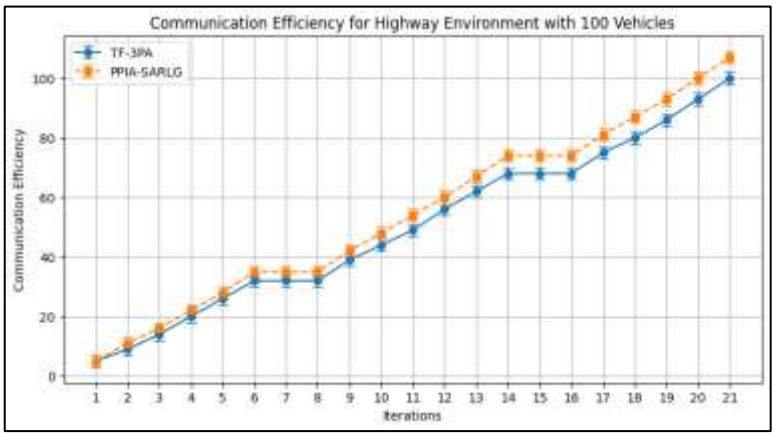

Figure 5. Communication efficiency performance for a highway environment considering 100 vehicles.

4.2. Communication Failure

Communication failure is a critical metric in evaluating the reliability of vehicular communication models. A lower communication failure rate indicates a more robust and efficient system, reducing data loss and enhancing real-time decision-making. The performance of PPIA-SARLG and TF-3PA is compared across different vehicular environments in terms of communication failure. The results show that PPIA-SARLG consistently reduces communication failures compared to TF-3PA across all scenarios. In an urban setting with 50 vehicles, as presented in Figure 6, PPIA-SARLG significantly reduces communication failure compared to TF-3PA, especially as vehicle density increases. Initially, both models exhibit similar performance, but as the number of vehicles increases, the communication failure rate of TF-3PA increases sharply, while PPIA-SARLG maintains a lower failure rate. On average, the PPIA-SARLG reduces communication failure by 26.35% in comparison with TF-3PA. For 100 vehicles in an urban environment, as presented in Figure 7, PPIA-SARLG shows better performance by significantly reducing communication failure rates. On average, the PPIA-SARLG reduces communication failure by 10.16% in comparison with TF-3PA.

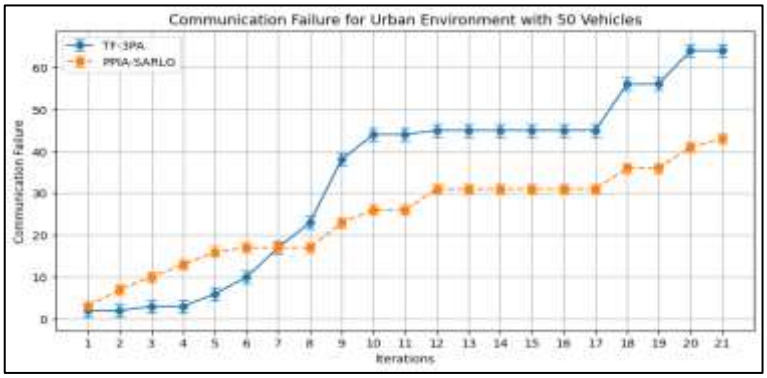

Figure 6. Communication failure performance for an urban environment considering 50 vehicles.

In a highway environment with 50 vehicles, communication reliability is more critical due to high-speed mobility and frequent topology changes. In this Figure 8 scenario, on average, the PPIA-SARLG reduces communication failure by 31.36% in comparison with TF-3PA. In Figure 9, scenario 100 vehicles in a highway environment, PPIA-SARLG continues to outperform TF-3PA by maintaining lower communication failure rates. In this scenario, on average, the PPIA-SARLG reduces communication failure by 5.58% in comparison with TF-3PA. The PPIA-SARLG model achieves an average improvement of 18.36% in reducing communication failures across all scenarios. These findings show that PPIA-SARLG enhances communication reliability by reducing data loss, improving network resilience, and ensuring more efficient data transmission in vehicular networks.

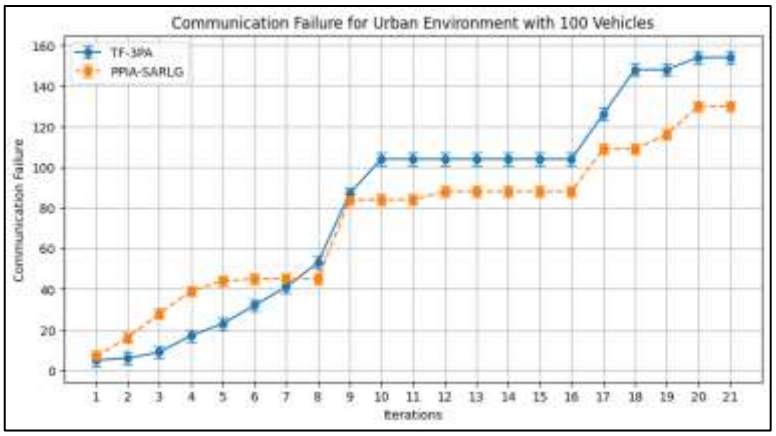

Figure 7. Communication failure performance for an urban environment considering 100 vehicles.

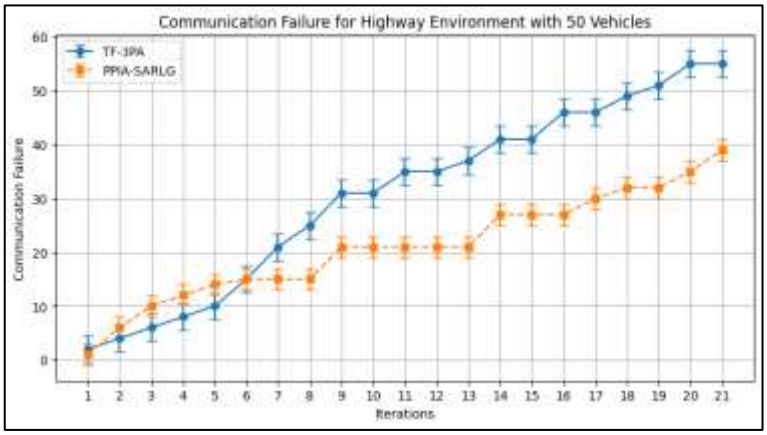

Figure 8. Communication failure performance for a highway environment considering 50 vehicles.

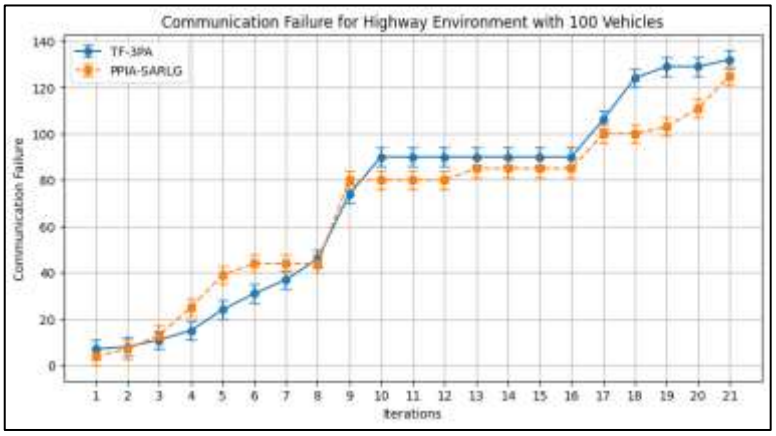

Figure 9. Communication failure performance for a highway environment considering 100 vehicles.

4.3. Throughput

Throughput is a key performance metric that measures the efficiency of data transmission in vehicular networks. Higher throughput indicates better network utilisation, leading to improved communication reliability. The PPIA-SARLG model consistently outperforms TF-3PA across all scenarios, demonstrating its effectiveness in handling vehicular network traffic efficiently. For 50 vehicles in an urban environment, PPIA-SARLG provides a notable improvement over TF-3PA in terms of throughput, as presented in Figure 10. On average, PPIA-SARLG achieved 18.01% better throughput in comparison with TF-3PA. With 100 vehicles, PPIA-SARLG continues to outperform TF-3PA, especially at higher densities, as presented in Figure 11. On average, PPIA-SARLG achieved 21.97% better throughput in comparison with TF-3PA.

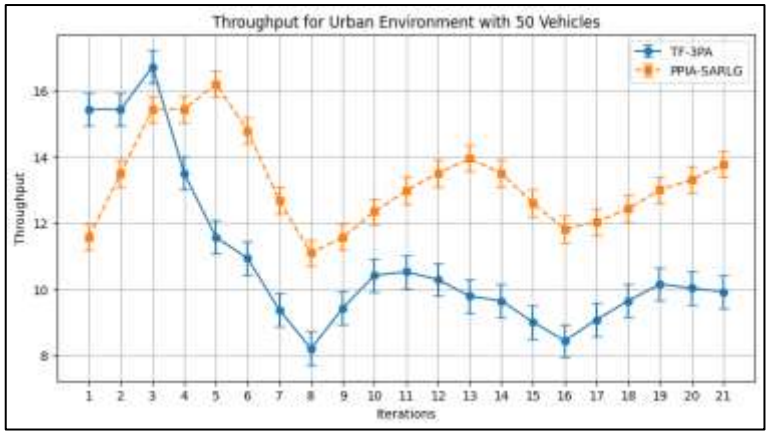

Figure 10. Throughput performance for an urban environment considering 50 vehicles.

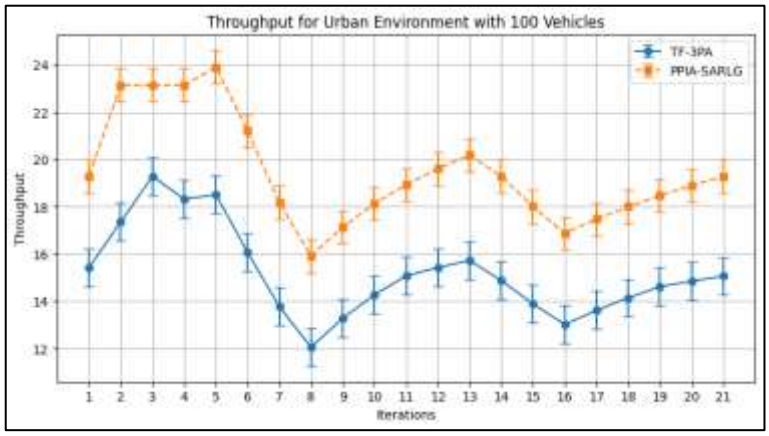

Figure 11. Throughput performance for an urban environment considering 100 vehicles.

In a highway setting with 50 vehicles, PPIA-SARLG consistently achieves higher throughput than TF-3PA, as presented in Figure 12. On average, PPIA-SARLG achieved 14.94% better throughput

in comparison with TF-3PA. In the Figure 13 scenario, 100 vehicles in a highway scenario, PPIA-SARLG maintains superior throughput performance over TF-3PA. On average, PPIA-SARLG achieved 8.26% better throughput in comparison with TF-3PA. The PPIA-SARLG model consistently achieved better throughput performance than TF-3PA, with average improvements ranging from 15.79%, depending on the scenario. These results confirm that PPIA-SARLG enhances data transmission efficiency, reduces delays, and optimises network performance in both urban and highway vehicular environments.

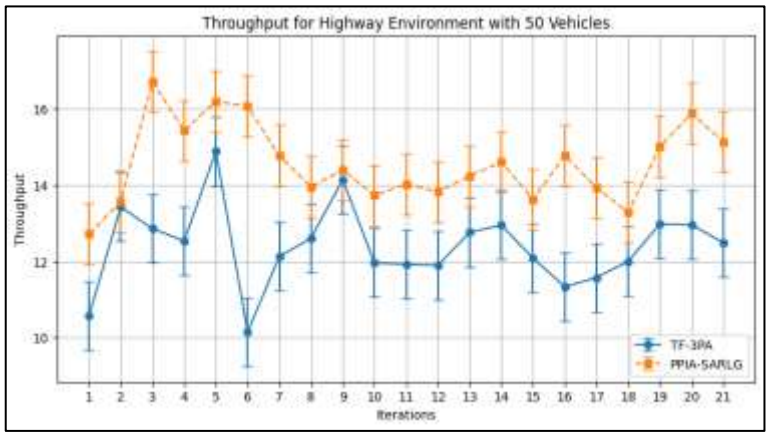

Figure 12. Throughput performance for a highway environment considering 50 vehicles.

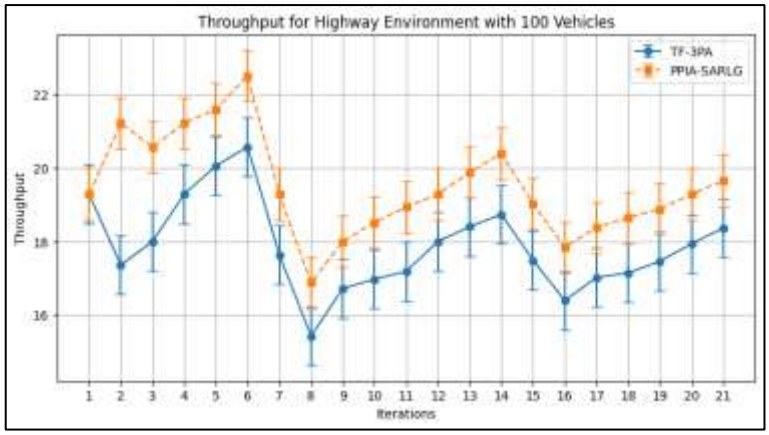

Figure 13. Throughput performance for a highway environment considering 100 vehicles.

4.4. Confusion Matrix

Based on the confusion matrices shown in Figure 14 and Figure 15, the qualitative performance of the proposed PPIA-SARLG scheme demonstrates reliable and robust attack detection capability when compared with the existing TF-3PA method. PPIA-SARLG records a high number of true positives and a very small number of false positives, indicating that most malicious packets are correctly identified while legitimate traffic is rarely misclassified as attacks. In contrast, TF-3PA exhibits comparatively higher false positive and false negative values, which suggests weaker discrimination between normal and malicious traffic. This imbalance may lead to unnecessary alarms and missed attack instances in dynamic vehicular environments. Furthermore, the lower false negative count achieved by PPIA-SARLG ensures that only a limited number of attacks escape detection. The overall distribution of predictions confirms that the proposed approach offers more accurate, stable, and mobility-resilient attack detection than the existing TF-3PA scheme.

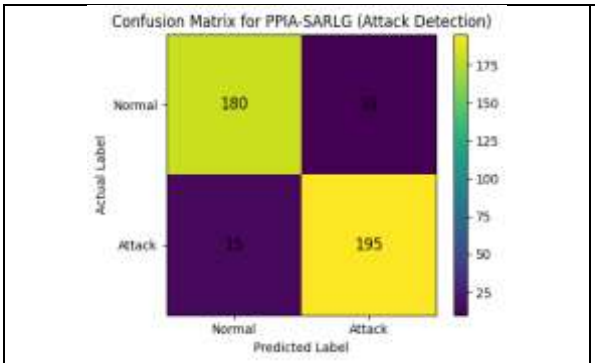

Figure 14. Confusion Matrix for PPIA-SARLG.

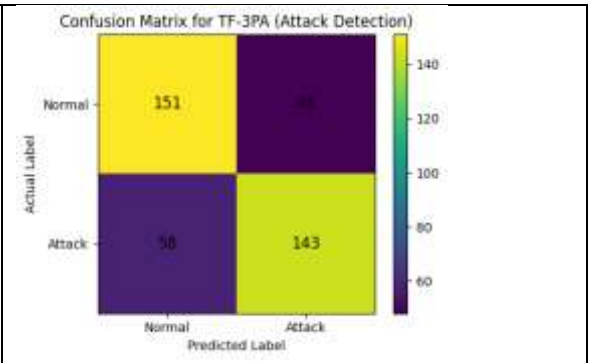

Figure 15. Confusion Matrix for PPIA-SARLG.

4.5. Energy Consumption and Latency Analysis

Table 6 compares the energy consumption and latency of the proposed PPIA-SARLG method with the TF-3PA scheme under different vehicle densities. It is observed that PPIA-SARLG consistently outperforms TF-3PA in both metrics. For 50 vehicles, PPIA-SARLG requires only 0.82 J of energy and achieves a latency of 45 ms, whereas TF-3PA consumes 1.12 J with a latency of 64 ms. As the number of vehicles increases to 100, the performance gap becomes more noticeable. PPIA-SARLG maintains lower energy usage (1.43 J) and reduced latency (71 ms) compared to TF-3PA, which records 1.75 J and 108 ms. These results demonstrate that the proposed approach scales efficiently with network size and provides better energy efficiency and faster response time under higher traffic conditions.

Table 6. Energy and Latency vs Vehicles

Vehicles	PPIA-SARLG Energy (J)	TF-3PA Energy (J)	PPIA-SARLG Latency (ms)	TF-3PA Latency (ms)
50	0.82	1.12	45	64
100	1.43	1.75	71	108

4.6. Runtime Analysis

The runtime performance of different models is presented in Table 6 to evaluate their computational efficiency. Among the compared methods, TF-3PA achieves the lowest execution time of 2.91 seconds, indicating faster processing under the given experimental setup. The proposed PPIA-SARLG model records a runtime of 3.02 seconds, which is very close to TF-3PA and remains competitive despite incorporating additional learning and security mechanisms. In contrast, BSDA and ISTOC require longer execution times of 3.44 seconds and 4.18 seconds, respectively, reflecting higher computational overhead. Although PPIA-SARLG does not yield the absolute minimum runtime, it offers a favourable balance between efficiency and advanced functionality. These findings suggest that the proposed approach can be deployed in practical environments without introducing significant delays while still achieving improved decision-making performance.

Table 6. Runtime Complexity

Model	Runtime (s)
TF-3PA	2.91
BSDA	3.44
ISTOC	4.18
PPIA-SARLG	3.02

4.7. Discussion

The incorporation of privacy-preserving noise inevitably influences the detection and decision accuracy of the proposed framework. While noise injection enhances data confidentiality and mitigates inference attacks, excessive perturbation may slightly degrade the reliability of aggregated vehicular data and affect learning stability. This highlights a critical tradeoff between communication overhead and data protection, as stronger privacy mechanisms require additional signalling and processing, increasing bandwidth usage and latency. Moreover, although the SARLG-based reinforcement learning model adapts effectively to dynamic network conditions, its generalisation

capability is constrained when exposed to unseen mobility patterns or highly irregular traffic scenarios. These limitations indicate that adaptive privacy tuning and more robust learning strategies are necessary to balance security, efficiency, and scalability in real-world vehicular edge-cloud environments.

5. Conclusion

This study proposed the PPIA-SARLG model to enhance communication efficiency, reliability, and throughput in IoV-VEC environments. The increasing complexity of vehicular networks, coupled with dynamic traffic conditions and cyber threats, necessitates robust communication models to ensure seamless data transmission. Traditional models, such as TF-3PA, face challenges in maintaining high performance under varying vehicular densities and mobility conditions. Addressing these challenges, this work introduced PPIA-SARLG. The methodology involved implementing PPIA-SARLG in the SIMITS simulator, integrated with NS3, and utilising the IEEE 802.11 6G gateway for realistic vehicular communication. The CICIoV2024 dataset was employed to simulate cyberattacks, ensuring the model's resilience under adversarial conditions. The key performance metrics, including communication efficiency, communication failure, throughput, and attack detection accuracy, were evaluated in both urban and highway scenarios with different vehicle densities. The results demonstrated that PPIA-SARLG consistently outperformed TF-3PA across all metrics. Specifically, PPIA-SARLG achieved an average improvement of 19.71% in communication efficiency, reducing delays and ensuring seamless data exchange. In terms of reliability, it reduced communication failures by 18.36%, enhancing network resilience and minimising data loss. Additionally, PPIA-SARLG improved throughput by an average of 15.79%, ensuring optimal utilisation of network resources. A qualitative analysis using confusion matrices further confirmed the robustness of the proposed model. PPIA-SARLG achieved a higher true positive rate and a lower false positive rate compared to TF-3PA, indicating more accurate attack detection and fewer misclassifications of legitimate packets. The incorporation of privacy-preserving noise was observed to slightly affect detection accuracy; however, this impact remained marginal and acceptable when compared with the gains in data protection. This highlights an inherent tradeoff between communication overhead and privacy preservation, where stronger privacy guarantees introduce minor computational and signalling costs. Moreover, while the reinforcement learning-based strategy demonstrated stable performance under varying mobility patterns, its generalisation capability may be constrained when exposed to unseen traffic conditions or attack behaviours, indicating a limitation of model adaptability in highly dynamic environments. These findings show that PPIA-SARLG is a robust and efficient model for vehicular communication, particularly in high-mobility environments. The proposed model significantly enhanced communication performance and security, making it suitable for next-generation IoV systems. For future work, the model can be extended by integrating blockchain-based trust management to strengthen distributed authentication and data integrity. Further evaluation using real-world vehicular traces generated from platforms such as Veins and SUMO will be conducted to validate its practical applicability. In addition, future research will explore multi-agent reinforcement learning and federated learning frameworks to improve scalability, cooperation among vehicles, and privacy preservation for complex IoV workflows and advanced ADAS system design.

ACKNOWLEDGMENTS

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for their unwavering guidance, invaluable insights, and encouragement throughout the research process.

FUNDING INFORMATION: No funding is raised for this research

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Vijayalaxmi Saibaba Sadlapur	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Nayana Hegde	✓	✓			✓	✓		✓	✓	✓	✓	✓		

C: **Conceptualisation**	I: **I**nvestigation	Vi: **Visualisation**
M: **M**ethodology	R: **R**esources	Su: **Su**pervision
So: **So**ftware	D: **D**ata Curation	P: **P**roject administration
Va: **Va**lidation	O: Writing - **O**riginal Draft	Fu: **Fu**nding acquisition
Fo: **Fo**rmal analysis	E: Writing - Review & **E**diting	

CONFLICT OF INTEREST STATEMENT: The Author declares no conflict of interest.

DATA AVAILABILITY: The Dataset is utilised in this research, as mentioned in references [31, 32].

REFERENCES

1. S. A. Ali Shah, X. Fernando, and R. Kashef, “A Survey on Artificial-Intelligence-Based Internet of Vehicles Utilising Unmanned Aerial Vehicles,” Drones, vol. 8, no. 8, p. 353, Jul. 2024, doi: 10.3390/drones8080353.
2. N. M. Elfatih et al., “Internet of vehicles’ resource management in 5G networks using AI technologies: Current status and trends,” IET Communications, Dec. 2021, doi: 10.1049/cmu2.12315.
3. Z. Ghaleb Al-Mekhlafi et al., "Integrating Safety in VANETs: A Taxonomy and Systematic Review of VEINS Models," in IEEE Access, vol. 12, pp. 148935-148960, 2024, doi: 10.1109/ACCESS.2024.3476512.

A. A. Mehta et al., "Securing the Future: A Comprehensive Review of Security Challenges and Solutions in Advanced Driver Assistance Systems," in IEEE Access, vol. 12, pp. 643-678, 2024, doi: 10.1109/ACCESS.2023.3347200.

4. S. Mazhar et al., “State-of-the-art authentication and verification schemes in VANETs: A survey,” Vehicular Communications, vol. 49, p. 100804, Jun. 2024, doi: 10.1016/j.vehcom.2024.100804.
5. M. J. Patil and K. P. Adhiya, “Secured VANET: an improved COOT-algorithm-based optimal routing protocol with multiple authentication and fake message detection for secure data transmission,” Wireless Networks, Mar. 2025, doi: 10.1007/s11276-025-03941-3.
6. U. Tariq, “Optimised feature selection for DDOS attack recognition and mitigation in SD-VANETs,” World Electric Vehicle Journal, vol. 15, no. 9, p. 395, Aug. 2024, doi: 10.3390/wevj15090395.
7. U. Tariq and T. A. Ahanger, “Enhancing intelligent transport systems through decentralised security frameworks in Vehicle-to-Everything networks,” World Electric Vehicle Journal, vol. 16, no. 1, p. 24, Jan. 2025, doi: 10.3390/wevj16010024.
8. [9] M. Ahmed et al., “A survey on vehicular task offloading: Classification, issues, and challenges,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 7, pp. 4135–4162, May 2022, doi: 10.1016/j.jksuci.2022.05.016.
9. J. Lai, X. Zhang, S. Liu, S. Zhong, and A. J. Moshayedi, “Blockchain-based VANET edge computing-assisted cross-vehicle enterprise authentication scheme,” Computer Communications, p. 108040, Dec. 2024, doi: 10.1016/j.comcom.2024.108040.
10. M. J. Khan, M. A. Khan, S. Turaev, S. Malik, H. El-Sayed, and F. Ullah, “A Vehicle-Edge-Cloud framework for computational analysis of a Fine-Tuned deep Learning model,” Sensors, vol. 24, no. 7, p. 2080, Mar. 2024, doi: 10.3390/s24072080.
11. H. A. Ahmed, H. M. Jasim, A. N. Gatea, A. A. A. Al-Asadi, and H. A. A. Al-Asadi, “A secure and efficient blockchain-enabled federated Q-learning model for vehicular Ad-hoc networks,” Scientific Reports, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-82585-3.

A. Rattan, A. Rudra Pal, and M. Gurusamy, "Quantum Computing for Advanced Driver Assistance Systems and Autonomous Vehicles: A Review," in IEEE Access, vol. 13, pp. 17554-17582, 2025, doi: 10.1109/ACCESS.2025.3532958.

12. X. Han, D. Tian, J. Zhou, X. Duan, Z. Sheng, and V. C. M. Leung, "Privacy-Preserving Proxy Re-Encryption With Decentralised Trust Management for MEC-Empowered VANETs," in IEEE Transactions on Intelligent Vehicles, vol. 8, no. 8, pp. 4105-4119, Aug. 2023, doi: 10.1109/TIV.2023.3289069.
13. M. Fardad, G. -M. Muntean and I. Tal, "A Blockchain-Enabled Vehicular Edge Computing Framework for Secure Performance-Oriented V2X Service Delivery," in IEEE Transactions on Vehicular Technology, vol. 73, no. 9, pp. 13853-13867, Sept. 2024, doi:

10.1109/TVT.2024.3394150.
14.Z. Zeng, Q. Zhou, K. Wei, N. Yang, and C. Tang, "BCS-CPP: A Blockchain and Collaborative Service-Based Conditional Privacy-Preserving Scheme for Internet of Vehicles," IEEE Transactions on Intelligent Vehicles, vol. 9, no. 2, pp. 4130-4144, Feb. 2024, doi: 10.1109/TIV.2023.3327364. T. Nandy, Rafidah Md Noor, Raenu Kolandaisamy, Mohd, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," Journal of King Saud University - Computer and Information Sciences, pp. 101945–101945, Feb. 2024, doi: 10.1016/j.jksuci.2024.101945.
15.M. A. Al Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang, and J. Ma, "Two-Factor Privacy-Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks," IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14253-14266, 15 April 15 2024, doi: 10.1109/JIOT.2023.3340259.
16.Z. Ma et al., "A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles," IEEE Access, vol. 12, pp. 81471-81482, 2024, doi: 10.1109/ACCESS.2024.3409361.
17.C. Xu, P. Zhang, X. Xia, L. Kong, P. Zeng, and H. Yu, "Digital Twin-Assisted Intelligent Secure Task Offloading and Caching in Blockchain-Based Vehicular Edge Computing Networks," IEEE Internet of Things Journal, 2025. doi: 10.1109/JIOT.2024.3482870.
18.J. Akram, A. Anaissi, A. Akram, R. S. Rathore, and R. H. Jhaveri, "Adversarial Label-Flipping Attack and Defence for Anomaly Detection in Spatial Crowdsourcing UAV Services," IEEE Transactions on Consumer Electronics, 2025. doi: 10.1109/TCE.2024.3448541.
19.X. Lu et al., "Blockchain-Enabled Secure Offloading for VEC: a Multi-Agent Reinforcement Learning Approach," IEEE Transactions on Dependable and Secure Computing, 2025. doi: 10.1109/TDSC.2024.3523561.
20.Z. Li, J. Gong, X. Xiong, and D. Wang, "Multi-slot Secure Offloading and Resource Management in VEC Networks: A Deep Reinforcement Learning-Based Method," IEEE Access, 2025. doi: 10.1109/ACCESS.2024.3524636.
21.Y. Chen, J. Wu, S. Ye, W. Li, and Z. Xu, "Budget-Constrained Resource Allocation and Pricing in VEC: A MSMLMF Stackelberg Game With Contract Incentive Mechanism," IEEE Internet of Things Journal, 2025. doi: 10.1109/JIOT.2024.3486378.
22.Ling Xiong, Qiang Li, LeLe Tang, Fagen Li, Xingchun Yang, Blockchain-based conditional privacy-preserving authentication scheme using PUF for vehicular ad hoc networks, Future Generation Computer Systems, Volume 163, 2025, 107530, https://doi.org/10.1016/j.future.2024.107530.
23.P. Liu, Q. He, Y. Chen, S. Jiang, B. Zhao, and X. Wang, "A Lightweight Authentication and Privacy-Preserving Aggregation for Blockchain-Enabled Federated Learning in VANETs," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2024.3512545.
24.Seyedi, Z., Rahmati, F., Ali, M. et al. Verifiable and privacy-preserving fine-grained data management in vehicular fog computing: A game theory-based approach. Peer-to-Peer Netw. Appl. 17, 410–431 (2024). https://doi.org/10.1007/s12083-023-01601-x.
25.Z. Wei, B. Li, R. Zhang, X. Cheng, and L. Yang, "Many-to-Many Task Offloading in Vehicular Fog Computing: A Multi-Agent Deep Reinforcement Learning Approach" in IEEE Transactions on Mobile Computing, vol. 23, no. 03, pp. 2107-2122, March 2024, doi: 10.1109/TMC.2023.3250495.
26.M. A. Al-Absi et al., "Secure and Efficient High Throughput Medium Access Control for Vehicular Ad-Hoc Network," Sensors, vol. 21, no. 14, p. 4935, Jul. 2021, doi: 10.3390/s21144935.
27.N. Gadde, B. Jakkali, R. B. Halasinanagenahalli Siddamallaih, and G. Gowrishankar, "Quality of experience aware network selection model for service provisioning in heterogeneous network," International Journal of Electrical and Computer Engineering (IJECE), vol. 12, no. 2, p. 1839, Apr. 2022, doi: 10.11591/ijece.v12i2.pp1839-1848.
28."Datasets | Research | Canadian Institute for Cybersecurity | UNB," www.unb.ca. https://www.unb.ca/cic/datasets/iov-dataset-2024.html, DOI: 10.1016/j.iot.2024.100943
29.C. Pinto et al., "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," Internet of Things, pp. 101209–101209, May 2024, doi: 10.1016/j.iot.2024.101209.