International Journal of Technology

http://ijtech.eng.ui.ac.id

Research Article

Privacy-Preserving Data Uploading SchemeBased on Threshold Secret Sharing Algorithm for Internet of Vehicles

Zheng Jiang [1], Fang-Fang Chua [1,*], Amy Hui-Lan Lim [1]

[1]*Faculty of Computing and Informatics, Multimedia University, Cyberjaya 63100, Malaysia*
[*]*Corresponding author: ffchua@mmu.edu.my; Tel.: +603-83125406; Fax: +603-83125264*

Abstract: Vehicle is needed to upload sensitive data such as the locations and traffic information in Internet of Vehicles (IoV). However, this process has significant privacy risks, specifically in scenarios where vehicles are constantly moving. Therefore, this study proposed a scheme called Privacy-Preserving Data Uploading Scheme (PriDUS), which relied on Threshold Secret Sharing Algorithm (TSSA). The scheme worked by grouping vehicle dynamically, calculating sub-IDs to replace real vehicle IDs during data uploads. These sub-IDs were distributed among vehicle in a group, ensuring that the original vehicle ID stayed hidden during transmission. Major variables considered in the process included group size, time allowed for reporting, and position or speed of vehicle were major considerations. Through simulations, the results showed that PriDUS could lower the risk of privacy breaches by up to 2.5% while keeping data transmission duration at 100 to 150 milliseconds. The method proved to be both practical and efficient, allowing it to be suitable for dynamic as well as complex IoV environments.

Keywords: Dynamic grouping; Internet of vehicles; Privacy protection; Threshold secret sharing algorithm

1. Introduction

Internet of Vehicles (IoV) is a part of Internet of Things (IoT) landscape. IoV has a range of applications, from automated transport vehicle in settings such as mines and ports, to incorporating features in new energy vehicle that improve user satisfaction (Whulanza, 2023). Furthermore, advancements in this area can lead to self-driving technologies that surpass drivers in terms of safety and dependability. Figure 1 shows the applications of IoV in four areas (Zhou et al., 2020), namely Vehicle to Network (V2N), Vehicle to Pedestrian (V2P), Vehicle to Infrastructure (V2I), and Vehicle to Vehicle (V2V), respectively (Pan et al., 2022). Following the discussion, each area presents its hurdles and important considerations. This study focuses on examining the security challenges related to protecting privacy data shared in the V2I sector (Hasan et al., 2024).

As the number of vehicle continues to rise (Sitinjak et al., 2023), the amount of data exchanged between automobiles and IoV systems grows significantly. This increasing movement of information has heightened concerns privacy protection. The risk of data interception or leakage during collection and uploading processes has made data security a crucial issue in IoV ecosystem. Relating to the discussion, studies are actively working on tackling these challenges. A recent method introduced by Hu et al. (2023) focused on ensuring privacy and maintaining data integrity in IoV through methods such as data sharing, homomorphic encryption, as well as symmetric encryption. Similarly, Rathore et al. (2022) introduced EAST model, which integrated encryption

This work was supported by Multimedia University

https://doi.org/10.14716/ijtech.v16i3.7260
Received August 2024; Revised November 2024; Accepted March 2025

with steganography to improve security during data transmission in IoV systems. Vulnerabilities remain despite these advancements specifically concerning network attacks that can compromise model parameters or encryption keys, threatening data confidentiality and security. Consequently, there is a growing interest in implementing Threshold Secret Sharing Algorithm (TSSA) to mitigate these risks (Babkin et al., 2021).

TSSA divides a secret S into segments distributed among connected vehicle in IoV system (Zhang et al., 2021). The secret S is reconstructed only when a required number of segments are collected, ensuring security even when some are lost or intercepted. However, applying TSSA in IoV presents challenges, and it struggles in IoV due to vehicle mobility originally designed for networks assuming segments that can be retrieved anytime (Huang and Chang, 2006). Vehicles exchanging data such as location and traffic status may not always locate the necessary segments, making reconstruction impractical. To address this, PriDUS adapts TSSA to IoV dynamic during the process. The system forms dynamic groups based on vehicle IDs and generates sub-IDs from the main ID using TSSA, ensuring data can be uploaded even as vehicle frequently enter or leave a region.

Based on the above description, this study makes several key contributions. First, the analysis introduces a novel method of privacy protection in IoV by treating vehicle ID as a secret S and dividing it into multiple sub-IDs, which are then distributed to automobiles. The original vehicle ID can only be reconstructed when a sufficient number of sub-IDs are collected, ensuring that even when some sub-IDs are lost or intercepted, data security and privacy are preserved. Second, the study proposes Privacy-Preserving Data Uploading Scheme (PriDUS), which is based on TSSA. By dynamically grouping vehicle using position and speed information, PriDUS assigns temporary sub-IDs that replace vehicle IDs during data uploads. This guarantees that even when an attacker intercepts data, the information cannot be traced back to a specific vehicle, improving privacy protection while preserving efficiency of the system.

2. Literature review

The growth of IoV raises has raised significant concerns regarding data privacy and security (Chen et al., 2022). Building on trust among users is crucial for enabling secure vehicle interactions. However, implementing measures such as two-factor authentication may introduce operational delays. IoV systems generates vast amount of sensitive data, including location and driving routes (Teoh et al., 2023), which further complicates efforts to protect user privacy. Additionally, cyber threats such as DoS/DDoS attacks, impersonation, replay attacks, and eavesdropping can disrupt system operations as well as pose a risk to safety of users (Garg et al., 2020). Data collection raises issues concerning misuse and security risks. Privacy issues develop when users unintentionally disclose information about others or breach system boundaries. Many hesitate to use IoV services due to data misuse concerns, potentially affecting system efficiency.

The assurance privacy and security in IoV system represents a central focus of this analysis. According to a study by Wang et al. (2023), efforts have been made to develop technologies in IoV framework to protect vehicle data and addressing privacy issues. Despite these initiatives, IoV systems encounter obstacles such as cybersecurity threats, scalability concerns, and authentication challenges that impact data security. The intricate nature of IoV systems renders the systems susceptible to cyber risks due to the number of vehicles and frequent data exchanges, which heighten the risk of privacy breaches during interactions. Despite past studies investigating privacy issues in IoV, devising a universal solution remains challenging due to the complexities in the system.

Rathore et al. (2022) developed EAST framework to improve security in IoV system. This method combines encryption and steganography procedures to secure data transfers. In EAST model, encryption keys are used to convert text into cipher text, which is then hidden in files using steganography for secure sharing. This strategy has proven effective in protecting IoV privacy information and has shown improvements in both data transmission efficiency as well as security. However, certain limitations remain when using the method despite its advantages. When a malicious actor has access to and decrypt file containing data, both encrypted information and encryption key can be compromised, increasing the risk of data exposure as well as security breaches. This situation presents a significant threat to IoV systems, as the exposure of the encryption key

allows hackers to decode all communications protected by that key. As EAST model provides a layer of protection, its effectiveness relies heavily on securing the file and ensuring that steganography remains undetectable.

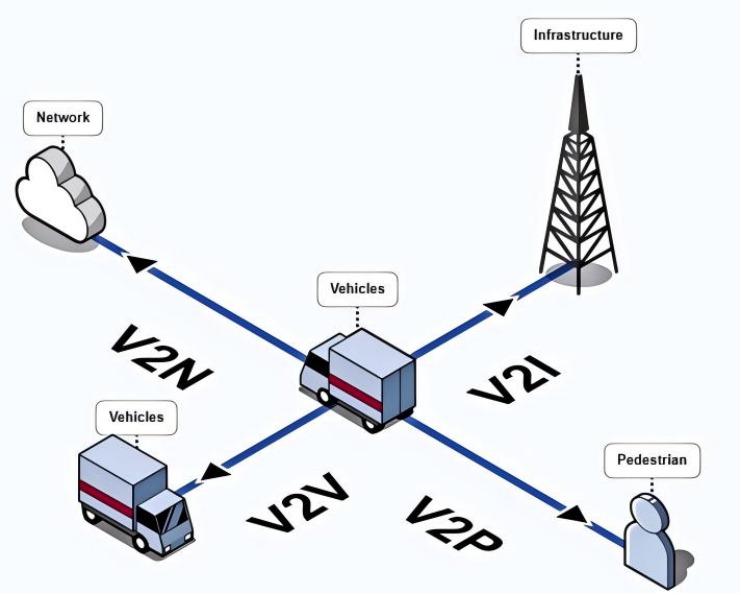

Figure 1 Main directions of IoV

Figure 2 shows that IoV ecosystem comprises servers, roadside units (RSUs), and vehicle. Core services depend on server clusters to manage vehicle, perform firmware upgrades, and process uploaded data such as location, speed, and traffic conditions. This data is then cleaned and used to train AI models. A primary challenge is ensuring timely and accurate data transmission between core servers and vehicle. To address this challenge, RSUs establish local networks with vehicle in the coverage area (Guerna et al., 2022). RSUs are also equipped with storage and computing capabilities to support efficient data exchange. Due to the constant movement of vehicle, RSU-vehicle network is highly dynamic, making real-time communication essential. These networks support both Vehicle-to-RSU (V2R) and Vehicle-to-Vehicle (V2V) interactions, which enable effective information sharing, especially in high-traffic scenarios. The transient nature of these connections demands high adaptability to maintain low-latency and reliable data transmission, even as the network composition changes frequently.

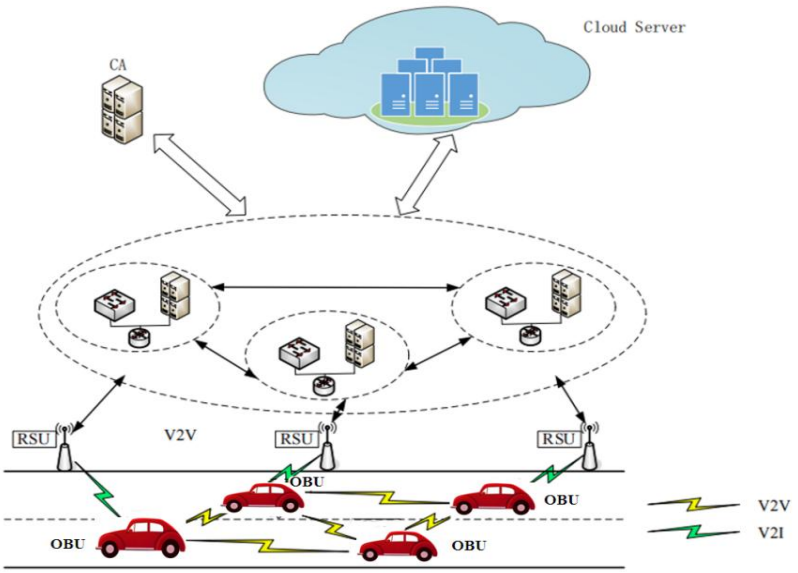

Figure 2 The architecture of Cloud-RSU-Vehicle layers

Cloud-RSU-Vehicle is a network formed by RSUs and vehicles covered architecture features. After vehicle enters the coverage area of RSU, it connects with other vehicles to establish a network (Tuyisenge et al., 2018). In this network, vehicle can exchange updates, such as traffic information and accident notifications, eventually improving the driving experience (Gao et al., 2023). However, these data exchanges come with privacy risks, such as vehicle identities, locations, speeds, and surrounding traffic conditions are shared (Hu et al., 2023). The major characteristics of networks formed by RSUs and vehicles include:

1. Member Changes: Vehicles frequently move in and out of RSUs coverage area necessitating management of these constant changes.
2. Privacy and Security Concerns: Ensuring data exchange among vehicles in RSU range is crucial to improve driving experiences, but safeguarding this interaction poses a challenge due to the nature of IoV.

TSSA has become a solution to address privacy and security challenges in IoV systems. The system works by generating sub-IDs from the ID, enabling the vehicle to transmit data using these sub-IDs. When a malicious attacker gains access to the sub-IDs, identifying the true identity of the vehicle becomes highly challenging, thereby preserving privacy and improving security. Several privacy-preserving schemes have been developed based on TSSA, including threshold key management, T-N threshold sharing mechanism, and secret sharing schemes.

A study by Lin (2023) proposed a multi-level blockchain framework to secure information in IoV. The framework incorporates threshold key management, elliptic curve cryptography, and group signatures. By dividing the system key into multiple shares and reconstructing it from a subset of the shares, threshold key management mechanism improves fault tolerance and reduces the risks associated with single-point failures. This scalable and resilient framework offers several benefits, including secure data transmission, strong protection against tampering as well as unauthorized access, and lower communication costs. The framework is particularly suited for the dynamic and complex environment of IoV. Similarly, a study by Zuo et al. (2024) introduced Secure Enhanced Privacy-Preserving Data Aggregation (SEPDA) scheme, which used a T-N threshold-based sharing mechanism. This method divides a value into shares distributed among users, allowing any group of T users to reconstruct the original value. By distributing the decryption process across multiple servers, the system improves security and reduces vulnerability to single-point attacks. During system initialization, Key Management Center (KMC) distributes encryption keys, with vehicle encrypting data using these shared keys before transmission. RSUs perform decryption after verification, while multiple servers at the Traffic Management Center (TMC) handle decryption and data consolidation. This strategy ensures privacy protection and improves resilience against various attacks. Despite the benefits in safeguarding privacy and security, threshold algorithms face challenges in managing member changes as well as addressing performance issues. Frequent changes in group membership can complicate the management and reorganization of the system, impacting its real-time performance. Each membership alteration requires recalculating group parameters, which adds to the workload. Furthermore, encryption and threshold sharing methods are computationally complex, particularly in scenarios with large datasets and frequent updates. This complexity can hinder performance, making it challenging to meet efficiency requirements for certain applications. Despite the system offering privacy protection and adaptability, it is crucial to consider the computational load as well as performance challenges before implementation.

A multi-party computation protocol was introduced in a related study by Liang et al. (2023) through a sharing scheme to protect user data privacy. The protocol divides user data into shares distributed among servers for storage and processing. During truth discovery, servers use these shares to update truth values and user weights without showing data points. A significant aspect of this protocol is the ability to reconstruct data when a minimum number of shares (threshold) are combined, preventing any server from accessing complete information. In case a server is compromised, threshold algorithm effectively minimizes the chances of privacy violations. Additionally, this algorithm improves system security and resilience by using distributed computing, offering defense against attacks. As shown in Table 1, although there has been considerable analysis of the application of TSSA in IoV, most of these studies focus on how TSSA is

used in a static environment for data encryption. In scenarios where vehicles communicate directly with a central server, drivers always upload data to a fixed set of central servers regardless of the movement of vehicle, creating a relatively static environment. However, in the three-tier architecture of cloud-edge-vehicle IoV, vehicles typically interact with RSUs. TSSA may struggle to acquire sufficient sub-secrets to reconstruct the original secret S due to the limited coverage of RSUs and the frequent changes in vehicle members in the same coverage area of RSU, such as vehicle entering or leaving this area, rendering the recovery process unsuccessful.

IoV vehicle collects and transmits data such as location, speed, and traffic conditions, raising privacy concerns despite encryption measures designed to protect this information (Liu and Pan, 2023). A previous section discusses TSSA in IoV system on how the model improves security by dividing a secret into sub-secrets, allowing reconstruction only when specific threshold is met. Building on the discussion, many studies assume a two-tier model where vehicle sends data to a central server, but modern IoV uses a three-tier cloud-edge-vehicle architecture (Zhou et al., 2023). Vehicle mobility may render sub-secrets inaccessible, leading to key reconstruction failures. Static participant assumption of TSSA limits its adaptability in dynamic IoV environments. To address this, PriDUS which is a method based on TSSA is proposed.

Table 1 Problems of TSSA in the IoV

Source	Description	Methods	Limitations
(Lin, 2023)	To propose threshold key management protocol to ensure the recovery and security of system keys.	threshold key management	
(Zuo et al., 2024)	To propose a Secure Enhanced Privacy-preserving Data Aggregation (SEPDA) scheme to improve system security by distributing the decryption process across multiple servers, preventing single-point attacks.	T-N threshold sharing mechanism	While these strategies effectively protect data privacy and security, schemes are designed primarily for scenarios where vehicle membership remains relatively stable, allowing the systems to be more suitable for static groups.
(Liang et al., 2023)	To propose a secure multi-party computation protocol to improve system security and fault tolerance through distributed computing, strengthening the defense against single-point attacks.	secret sharing scheme	
Proposed Work: 1. To accommodate the frequent joining and leaving of vechicle with RSUs, dynamic processing capabilities were added to threshold secret-sharing scheme.			

3. Methodology

PriDUS was designed to protect vehicle identity during data uploads in IoV. Since vehicle was constantly moving, a static privacy-preserving method was not enough. Therefore, PriDUS introduced dynamic grouping mechanism and applied TSSA to ensure secure and efficient data transmission.

3.1. Threat Model

In IoV environments, privacy threats primarily arose from attackers attempting to track vehicle movements, intercept sensitive data, or manipulate system behavior (Jeong et al., 2021). A common risk was tracking attacks, where an adversary related consecutive data uploads to identify and monitor a specific vehicle over time. When direct vehicle IDs were not transmitted, static pseudonyms or recurring patterns in anonymized data could still reveal the vehicle's identity.

Eavesdropping was another significant concern, as wireless communication in IoV systems was vulnerable to interception. When vehicle IDs or location data were transmitted without sufficient protection, attackers could analyze the data to uncover movement patterns, potentially leading to serious privacy breaches.

PriDUS prevented the direct exposure of vehicle identities by dynamically generating sub-IDs using TSSA to mitigate these risks. Each vehicle ID was split into multiple sub-IDs, which were distributed among automobiles in a temporary group. The original ID could only be reconstructed when a sufficient number of sub-IDs were collected, making collusion attacks difficult. When some sub-IDs were intercepted, the individual components remained meaningless. Furthermore, PriDUS assigned sub-IDs dynamically for each reporting session, preventing long-term tracking or replay attacks. As sub-IDs changed with each data upload, attackers were unable to link past and future transmissions to the same vehicle, ensuring strong privacy protection in dynamic IoV environments.

3.2. Key Steps of PriDUS

PriDUS addressed the limitations of traditional methods in dynamic environments by incorporating dynamic grouping with TSSA. During data uploads, vehicles transmitted sub-IDs along with privacy-sensitive data, including speed and location. This method ensured that even when attackers intercepted the data, the use of sub-IDs prevented any direct connection between the uploaded information and the originating vehicle, thereby safeguarding vehicle privacy. In the design of PriDUS, a combination of RSUs and Edge computing was selected to improve the computational capabilities of RSUs (Jeremiah et al., 2024). Since RSUs and Edge units were typically deployed together to cooperate on computations and task processing (Fan et al., 2024; Wang et al., 2020), the term "RSU-Edge" was used to describe this combined unit throughout the discussion. Figure 3 showed that data uploading in PriDUS includes four primary steps, namely Vehicle Grouping, Calculating and Distributing Sub-IDs, Data Collection and Reporting, and Vehicle ID Verification, as each step was explained as follows.

Step 1: Vehicle Grouping: The process included RSU-Edge continuously monitoring vehicles in its coverage area. When Vehicle U needed to upload data, such as location and speed, RSU-Edge dynamically grouped the machines, including Vehicle U. This grouping process considered the speed and position of vehicle surrounding Vehicle U, selecting those with similar speeds and proximity for inclusion in the group. The method ensured more stable communication when Vehicle U needed to collect sub-IDs. Additionally, the sub-IDs generated through dynamic grouping were collected in a short time frame and uploaded by Vehicle U. This method helped prevent situations where vehicle holding sub-IDs moved out of RSU-Edge coverage, ensuring the timely collection of sufficient sub-IDs. This step corresponded to the generation of sub-secrets in TSSA and the recovery of the original secret from these sub-secrets.

Step 2: Computation and Distribution of sub-IDs. This step included the computation of the sub-IDs using TSSA based on the ID of vehicle U reporting data and then distributed these sub-IDs after RSU-Edge successfully grouped the machines.

Step 3: Data Collection and Reporting. This step used standard V2V communication to gather sub-IDs (He et al., 2023). When Vehicle U needed to upload data such as location and speed, it collected the sub-IDs stored by other machines in the group, along with various types of data such as vehicle speed, location, and other relevant metrics. Vehicle U then uploaded this data to RSU-Edge during the process.

Step 4: Vehicle ID Verification. During this step, RSU-Edge used TSSA to reconstruct the vehicle ID from the uploaded data and verify the authenticity, ensuring both the integrity and accuracy of the collected data. When verification failed, the vehicle was deemed an unknown entity, and the data would be rejected.

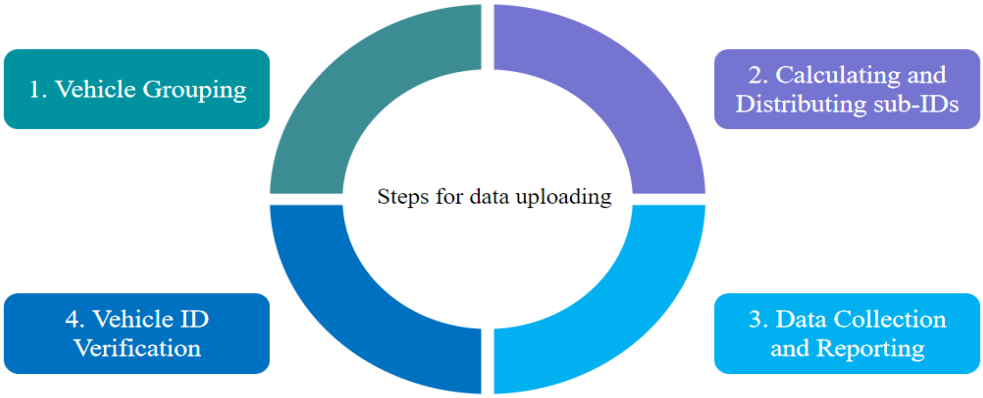

Figure 3 Steps for data uploading in PriDUS

Throughout this analysis, PriDUS was validated both theoretically and experimentally. Theoretical models were used to assess the ability of the model to protect vehicle data and prevent privacy attacks. In the experimental phase, the HighD dataset (Li et al., 2023), which contained real-world vehicle trajectories, was used. Simulations were conducted to analyze privacy leakage probability and transmission latency, allowing the evaluation of PriDUS in dynamic IoV scenarios.

4. Proposed scheme

4.1. Introduction of PriDUS

PriDUS improved the ability of TSSA to handle dynamic IoV membership changes. The model protected sensitive data such as location, speed, and traffic conditions designed for the three-tier cloud-edge-vehicle architecture. Moreover, PriDUS treated vehicle ID as a secret (S), dividing it into sub-IDs using TSSA. The system extended TSSA by adding dynamic grouping, forming a group around Vehicle U when uploading data. Vehicle U collected sub-IDs from nearby vehicles and submitted the information with its data to RSU, which reconstructed the ID using Lagrange interpolation. Even when intercepted, data remained secure, ensuring vehicle privacy during the process.

4.2. Overview of TSSA

The TSSA, or (t,n) threshold encryption algorithm, required at least t participants out of n to reconstruct a secret (Iwamura, 2023). For example, when the ID of Vehicle U served as the secret S, and five automobiles participated, with three sub-secrets required (t = 3, n = 5), TSSA generated five sub-secrets, including (1, f(1)), (2, f(2)), (3, f(3)), (4, f(4)), and (5, f(5)). Following this process, Vehicle U could reconstruct S by collecting any three of these sub-secrets. The process included calculating as well as distributing the sub-secrets, and reconstructing S after at least t sub-secrets were obtained. TSSA used a polynomial with randomly generated coefficients to prevent exposure of the secret. When fewer than t sub-secrets were available, it became impossible to recover the original secret.

For each participant i, a sub-secret was generated by substituting x = i into the polynomial. Each sub-secret took the form (xi, f(xi)), where xi was the unique identifier of the participant (e.g., 1, 2, 3, 4, or 5), and f(xi) was the result of substituting xi into the polynomial. Importantly, i could not be 0, as shown in Equation 2. When i = 0, the output would have been the original secret S, which would defeat the purpose of TSSA in generating sub-secrets. Furthermore, the fact that i = 0 produced the original secret S was a crucial aspect of how Lagrange interpolation was used to recover the original secret. To ensure the randomness of the sub-secrets, random coefficients a_1, a_2,…, a_i were introduced in Equation 1. This addition made the value significantly more difficult to infer the secret using only a small number of sub-secrets.

$$f(x) = S + a_1 x + a_2 x^2 + \cdots + a_i x^i \quad (0 < i \leq t-1) \tag{1}$$

$$f(0) = S \tag{2}$$

In TSSA, after t and n were set, and Equation 1 was used to calculate the secret, n sub-secrets were generated. These shares could then be distributed to n different participants as needed. For example, in an IoV system, TSSA could be used to calculate n sub-IDs from the vehicle ID, which were then distributed among n vehicle in the same network. When t vehicle participated, the original vehicle ID could be reconstructed in the network. Equations 3 and 4 represented the core computational formulas of Lagrange interpolation method (Zayed and Butzer, 2001), which was essential in TSSA for reconstructing the original secret S using at least t sub-secrets. This formula expressed the polynomial f(x) as a linear combination of several basis functions $l_j(x)$. Each $l_j(x)$ was multiplied by its corresponding y_j value, and the results were then summed to form the function f(x). In equation 3, y_j referred to the sub-secret at the point x_j. Following this, $l_j(x)$, known as the Lagrange basis function, ensured that all other basis functions $l_i(x)$ equaled 0 when $x=x_j$.

$$f(x) = \sum_{j=1}^{t} y_j \cdot l_j(x) \tag{3}$$

As shown in equation 4, in each basis function $l_j(x)$, all indices m ($m \neq j$) were iterated over. This ensured $l_j(x) = 1$ when $x=x_j$, while at all other points $x=x_m$ ($m \neq j$), the basis function $l_j(x) = 0$. Consequently, in the function f(x), only $y_j \times l_j(x)$ influenced the value of f(x) ($x=x_j$), while the other terms had no effect due to $l_j(x)=0$ ($i \neq j$).

$$l_j(x) = \prod_{m \neq j}^{1 \leq m < t} \frac{x - x_m}{x_j - x_m} \tag{4}$$

Lagrange interpolation method was used in Equation 5 to find secret S, where Equation 2 signified that S=f(0). Therefore, finding f(0) uncovered the secret S, as the expression f(0) signified the value of the interpolating polynomial, at x=0. Where y_j represented the y coordinate of the given point (x_j, y_j) and $l_j(0)$ was the value of the Lagrange basis function $l_j(x)$ at x=0. Additionally, $l_j(x)$ was the Lagrange basis function, ensuring $l_j(x) = 0$ at all points x_m ($m \neq j$), and equalled 1 at x_j. Using this formula, the analysis reconstructed the polynomial from a given set of points $(x_1,y_1),(x_2,y_2),\ldots,(x_t,y_t)$ and determined the value of the polynomial at x=0, recovering the secret S. The process was crucial in TSSA because it ensured that the original secret could only be reconstructed when at least t participants cooperated.

$$s = f(0) = \sum_{j=1}^{t} y_j \cdot l_j(0) \tag{5}$$

4.3. Algorithmic Design of PriDUS

Figure 4 showed the typical IoV architecture comprising three layers, namely Cloud Servers, RSU-Edge, and Vehicles (Karim et al., 2022). This study primarily focused on the efficient vehicle grouping mechanism in RSU-Edge layer. During the initialization or operation of RSU-Edge system, it was crucial to set the minimum participant number t and the total participant number n for TSSA, as well as to define a time tolerance T. After vehicle collected privacy data, the mobile could not immediately report it. As an alternative, vehicle first needed to collect at least t sub-IDs, which were then submitted along with privacy data to RSU-Edge for ID reconstruction. During the process, the time tolerance T represented the maximum allowable time interval from when vehicle was ready to report its privacy data to the actual submission. When the reporting process was not completed in this interval, the request had to be discarded to ensure maximum privacy protection for vehicle. Given the high speed and unpredictable movement of vehicle (Wang et al., 2022), grouping had to be dynamic. Figure 5 showed that when vehicle U needed to report data in PriDUS design, RSU-Edge created an initial vehicle group G centered around the location of vehicle U with a radius determined

by the product of the average speed v and the time tolerance T. This ensured that vehicle U remained in this range throughout the time tolerance period T.

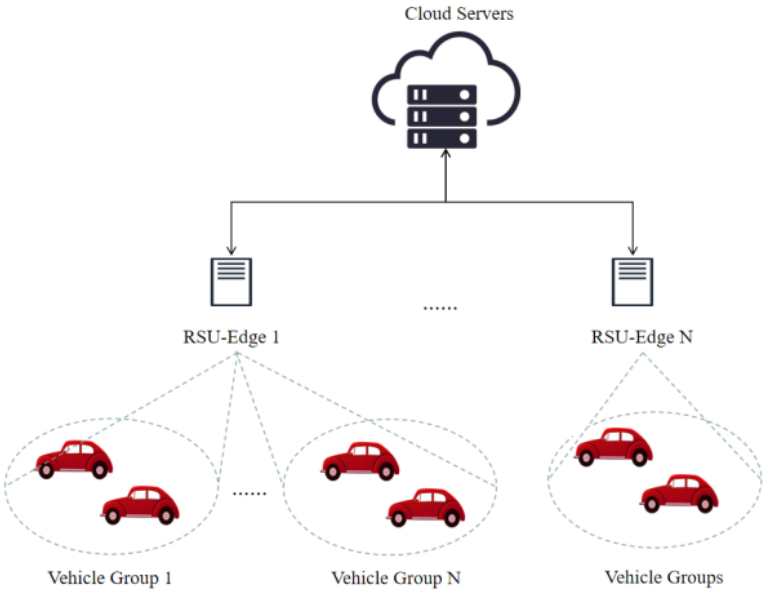

Figure 4 Design diagram of vehicle grouping

During the analysis, num(G) signified the number of vehicles in the initial group G. RSU-Edge had to ensure that num(G) was greater than the minimum participant number t and less than twice the total participant number n, i.e., 2n. When num(G) < t, it would not have been possible to collect enough sub-IDs to reconstruct the ID of vehicle. In addition, when num(G) > 2n, the group had to be split into two or more subgroups to maintain the efficiency of sub-IDs. Algorithm 1 showed that RSU-Edge initialized an array group[] and added vehicle from group G into this array, including vehicle U which needed to report privacy data. The system then calculated the number of vehicles in the group[] array. When t < num(G) < 2n, TSSA was used to compute sub-IDs, which were then distributed to n vehicle. Moreover, when num(G) > 2n, the group was divided into two or more subgroups to ensure that vehicle U could efficiently collect sub-IDs. Before reporting privacy data, vehicle U used V2V communication to retrieve the necessary sub-IDs from other vehicles (Naouri et al., 2024), and it only reported data after reaching the minimum participant number t. When the group was too large, the retrieval process could have become less efficient and more challenging. To optimize the difficulty of sub-IDs retrieval, RSU-Edge calculated a weight value W for each vehicle in group[] relative to vehicle U. This weight was determined by considering both the distance between vehicle and the average speed. A lower weight W showed that communication with vehicle was easier for vehicle U, while a higher weight W made communication more difficult. After completing the calculations for all vehicles in group[], RSU-Edge selected 2n vehicle to form a new group[], calculated the sub-IDs, and distributed to all vehicles. When num(G)<t, showing insufficient number of vehicle, RSU-Edge expanded the group radius by doubling the initial radius r which was based on the product of the average speed v and time tolerance T. A new group with radius 2r was then formed and the process was repeated until a sufficient number of vehicle was included or the time tolerance T was exceeded.

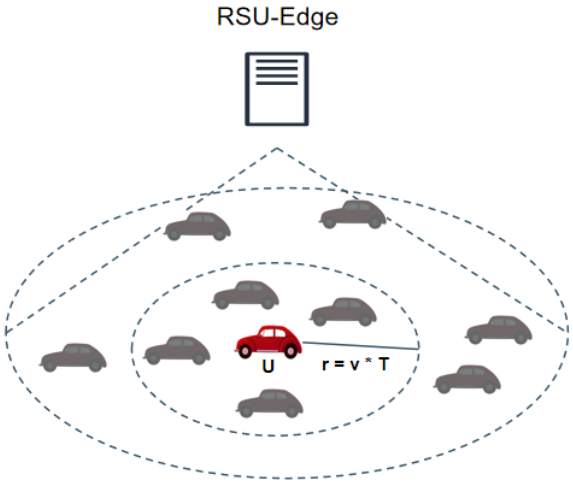

Figure 5 Design diagram of dynamic grouping

Algorithm 1 RSU-Edge Group Formation and Sub-IDs Distribution

Input: Parameters for (t, n), time tolerance T, average speed v (of vehicle U)

1. Initialize an empty array group[]
2. Determine the set of vechicle in radius r = v * T, including vehicle U, and populate group[]
3. Calculate the number of vechicle in group[]:

   if t < num(G) < 2n then

   - Execute (t, n) threshold encryption to generate sub-IDs
   - Assign sub-IDs to a selected subset of n vechicle in group[]

   else if num(G) > 2n then

   - Divide group[] into subgroups to improve sub-IDs collection efficiency
   - Proceed with the distribution of sub-IDs in each subgroup as determined by the method

4. If num(G) < t then

   - Check if the time tolerance T is exceeded:

   if T is not exceeded then

   - Double the search radius to 2r
   - Recalculate group[] by including additional vechicle in the expanded radius
   - Recursively apply Algorithm 1 until t < num(G) < 2n or time tolerance T is exceeded

   else

   - Terminate the algorithm as the time tolerance T is exceeded

Output: Sub-IDs distributed among the selected vechicle or algorithm terminated due to time constraints

When num(G) > 2n, vehicle had to be divided into two or more groups. The grouping criteria were based on vehicle U, selecting 2n vehicle closest in distance and average speed to U to form a new group[]. Equation 6 signified that Wiu represented the communication weight between vehicle i and vehicle U. A smaller value of Wiu showed that the distance, as well as average speed between vehicle i and U were more similar. Moreover, the parameters α and β were weight factors used to adjust the influence of distance as well as speed on the final weight value, with the sum equal to 1. A larger α had to be selected when distance was more critical to communication, and a larger β

when speed was more important. In addition, when no specific preference existed, the values could be set equally at 0.5. The $\frac{d_{iu}}{d_{\max}}$ represented the normalized distance between vehicle i and vehicle U, which was calculated by dividing the distance diu by the maximum distance dmax in the group. A higher value showed a greater distance and more challenging communication. The $1-\frac{|v_i-v_u|}{v_{\max}}$ represented the normalized speed difference between vehicle i and U. The process first calculated the absolute value of the speed difference $|v_i-v_u|$ and then normalized it by the maximum speed difference v_{max} in the group. As the speeds between vehicles became closer, the differences as well as weight values decreased. This led to more stable channel signals between the values, making data interactions more efficient and reliable (Sodhro et al., 2020).

$$W_{iu} = \alpha \cdot \frac{d_{iu}}{d_{\max}} + \beta \cdot \left(1 - \frac{|v_i - v_u|}{v_{\max}}\right) \quad (6)$$

This dynamic grouping method effectively addressed the issue of dynamic vehicle membership by forming temporary groups as well as computing and distributing sub-IDs only when vehicle needed to report data. This transformed TSSA from a static to dynamic process, enabling both newly joined and soon-to-exit vehicle to dynamically form groups as well as report data, offering privacy protection with dynamic characteristics.

5. Experimentation and analysis

PriDUS was a privacy-preserving scheme designed to protect sensitive data, such as speed and location, during the transmission of vehicle data to RSU-Edges. Given the high real-time requirements of IoV, PriDUS ensured privacy protection and also optimized data transmission performance. This section first analyzed the security of PriDUS from a privacy protection perspective. Subsequently, a simulation platform was used to model the process of vehicles collecting and uploading data to RSU-Edges. Comparative evaluations were conducted against CE-IoV (Benarous and Kadri, 2022) and K-Anonymity Protection Scheme to validate the performance of PriDUS, (Qi and Chen, 2023).

5.1. Security Analysis

The scheme of the model effectively addressed privacy challenges in IoV by using TSSA and introducing dynamic grouping mechanisms. The theoretical foundations of the scheme provided strong guarantees for protecting vehicle IDs and ensuring secure, efficient data exchanges, even in highly dynamic vehicle environments. TSSA was central to PriDUS, offering a mathematically sound method for privacy preservation. In this scheme, the vehicle ID was treated as a secret S, which was divided into n sub-IDs distributed among participating vehicle. Each sub-IDs corresponded to a unique point on a polynomial $\boldsymbol{f(x)}$ of degree $\boldsymbol{t-1}$, where $\boldsymbol{t}$ was the minimum number of sub-IDs required to reconstruct the original ID. As shown in Equation 1, the coefficients $\boldsymbol{a_1, a_2, \ldots, a_i}$ were randomly selected. This randomness ensured that fewer than $\boldsymbol{t}$ sub-IDs provided no meaningful information about $\boldsymbol{S}$, as the interpolation of $\boldsymbol{f(x)}$ without sufficient data points was mathematically infeasible. Consequently, TSSA effectively neutralized brute force or interpolation attacks, as reconstructing the secret would have required solving an NP-hard problem over large finite fields (Li et al., 2020).

The model extended the applicability of TSSA by incorporating a dynamic grouping mechanism adapted to the mobility of IoV. This mechanism addressed a major limitation of static schemes, which often assumed fixed participant sets and failed in scenarios where vehicle frequently entered or left communication ranges. PriDUS ensured the consistent availability of t sub-secrets, even in high-mobility environments by dynamically forming groups based on real-time proximity and speed. Additionally, the temporary nature of the sub-IDs assigned in these groups significantly enhanced privacy. Since sub-IDs were regenerated for each interaction, the system eliminated the

risk of long-term associations, a common vulnerability in static privacy-preserving schemes. This ensured that adversaries could not correlate sub-IDs across multiple interactions to identify the vehicle.

PriDUS scheme showed theoretical resilience against several common IoV attack vectors. For instance, eavesdropping was rendered ineffective, as intercepted sub-IDs could not show any meaningful information unless the threshold t was met. Collusion attacks were also mitigated even when multiple malicious participants pooled sub-IDs, the group would not be able to reconstruct the original vehicle ID without a sufficient number of sub-IDs. Replay attacks were countered by the reliance of the scheme on dynamically generated sub-IDs, which were valid only for a specific group and time interval. This ensured that reused data could not be authenticated or linked to the originating vehicle. The real-time generation and distribution of sub-IDs prevented adversaries from exploiting incomplete or outdated information. Each interaction remained independent, with no reliance on past communications, further reducing the attack surface.

Despite TSSA including computationally intensive polynomial calculations, the design of PriDUS ensured that these operations were efficiently managed. By offloading sub-ID generation and verification tasks to RSU-Edges, the computational burden on individual vehicle was minimized. Through advanced processing capabilities, these RSU-Edges were able to handle such tasks effectively, ensuring real-time performance even in densely populated IoV environments. The dynamic grouping mechanism also improved efficiency by localizing operations to smaller groups of vehicles, avoiding the overhead of network-wide computations. Furthermore, the system dynamically adjusted the group radius and member compositions to account for vehicle mobility, ensuring that sub-IDs were collected promptly without unnecessary delays or resource usage.

5.2. Performance Testing

This study used OPNET simulation platform to evaluate privacy protection and the performance of PriDUS. The setup ran on an Intel Core i7-7700K @4.0GHz with 16GB RAM. During the analysis, a two-way, two-lane highway (14.8m wide, 10km long) was simulated, with vechicle traveling at 30 km/h for 20 minutes. A total of 200 vechicle transmitted 3,200-bit privacy data packets in a 10-second reporting window. Network communication used a 55 kHz channel, affecting data rates and interference. Moreover, Nakagami model adjusted the m parameter to simulate real-world wireless fading characteristics, significantly impacting network performance.

This study aimed to assess the effectiveness of PriDUS by comparing the model with CE-IoV system presented by Benarous and Kadri (2022) and K-Anonymity Protection Scheme developed by Qi and Chen (2023), respectively. CE-IoV system combined cloud computing, IoV, and IoT to offer entertainment services for drivers. However, a significant issue arose when vehicle shared location data, potentially exposing the automobiles to tracking as well as compromising user privacy and safety. Studies proposed privacy protection method based on obfuscation procedures to address the concern. This method included performing alterations and implementing time frames to reduce the association between location data as well as personal information. The main objective of this method was to prevent vehicle tracking by strengthening privacy measures in traffic settings where large anonymous groups could lower the chances of tracking by malicious entities. In the context of the discussion, K-Anonymity Protection Scheme tackled privacy breaches and network latency issues in vehicle positioning services. The scheme ensured the security and confidentiality of vehicle location privacy data by incorporating this technology with a fault consensus mechanism. Rapid clustering K-anonymity method was used to safeguard vehicle location privacy while simplifying the establishment of anonymity zones.

The system included a trust model to manage trust between requesting and cooperating vehicle in K-anonymity framework, using rewards as well as penalties to improve security and efficiency. The model offered privacy protection, lower time complexity, and flexible trust management.

Table 2 Simulation environment parameter settings

Parameter	Parameter unit	Parameter setting
CPU	X86_64	2 CPU
Storage	X86_64	2 CPU
Road width	TB	1
Road length	metres	3.7 * 4
Average vehicle speed	km	10
Vehicle transmission power	km/h	30
Collected data packet	mW	20
Maximum data transmission rate	bit	3,200
Channel spectrum bandwidth	Mbps	2
Channel model	kHz	55
Noise power	–	Nakagami
Number of vechicle	dBm	-100

This study compared PriDUS, CE-IoV, and K-Anonymity Protection Scheme through simulations. Privacy protection algorithms required time for data collection and encryption, introducing latency. Figure 6 compared transmission durations, showing that as data volume increased, transmission time improved. K-Anonymity Protection Scheme had the longest transmission duration, followed by CE-IoV, while PriDUS was the fastest. When uploading data from over 150 vehicles, PriDUS maintained a transmission time of 100–150ms with a 3–6% error margin.

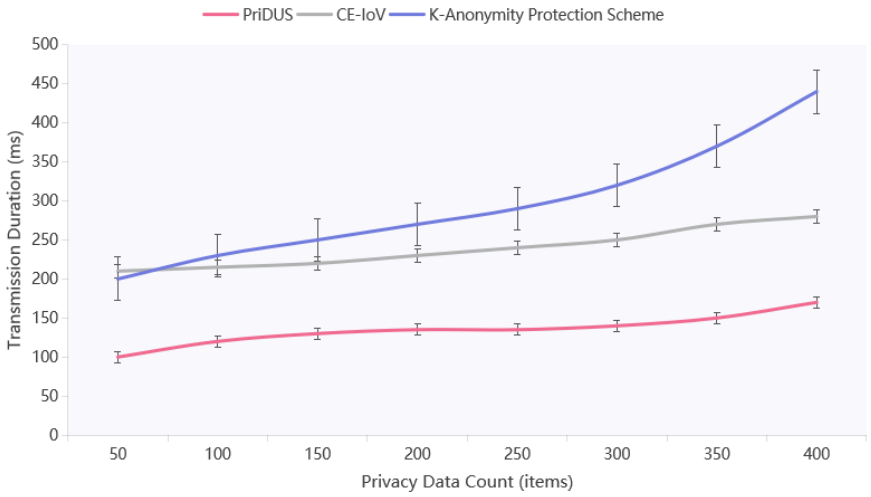

Figure 6 Analysis of Transmission Duration

Besides transmission duration, privacy leakage probability was major. The process measured the risk of unauthorized access to user data in IoV, showing how well privacy-preserving algorithms protected information (Jia et al., 2020). Following the discussion, a lower probability meant stronger protection. As shown in equation 7, the value was calculated as the ratio of successful inferences (n) to the total number of vehicles in a group (num(G)).

$$P = \frac{n}{num(G)} \tag{7}$$

Figure 7 showed that K-Anonymity Protection Scheme signified a relatively high privacy leakage probability, ranging from 9% to 13%. The CE-IoV algorithm performed better, with a leakage

probability between 6% and 8%. During the process, PriDUS outperformed both, reducing privacy leakage probability to approximately 2.5% to 4.5%. Therefore, PriDUS significantly improved user privacy protection during the process.

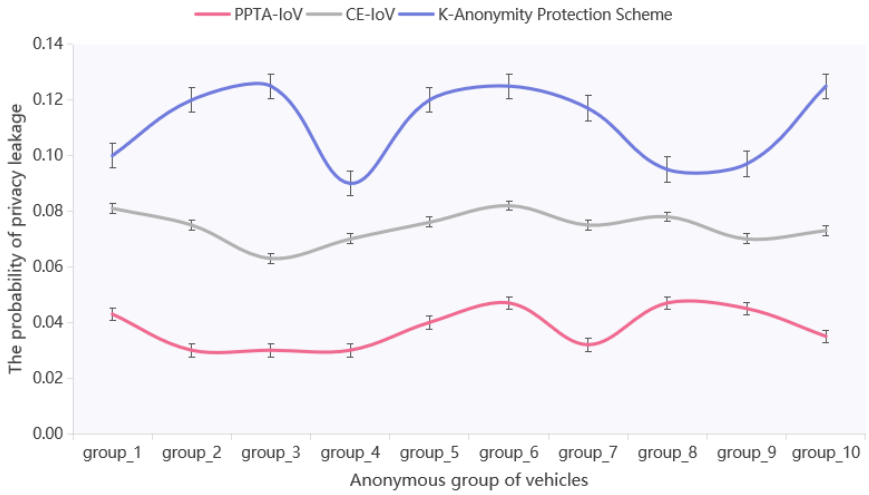

Figure 7 Analysis of privacy leakage probability

5.3. Discussion of performance testing

The results showed that PriDUS provided stronger privacy protection and better efficiency than the other two schemes. A substantial advantage was the lower privacy leakage probability, which ranged between 2.5% and 4.5%, significantly lower than 6%–8% in CE-IoV and 9%–13% in K-Anonymity Protection Scheme, respectively. Moreover, the primary reason for the improvement was the use of sub-IDs in place of direct vehicle identifiers, allowing it to be significantly more difficult for attackers to track vehicle based on uploaded data.

The ability to adapt to dynamic environments was another major distinction. Both CE-IoV and K-Anonymity Protection Scheme relied on static data protection mechanisms that assumed vehicles maintained a stable presence in a specific region. However, IoV networks were inherently dynamic, with vehicle frequently moving in and out of coverage areas. PriDUS addressed this issue by dynamically forming vehicle groups and distributing sub-IDs in real-time. This ensured that privacy protection remained effective even when vehicles joined or left the range of RSU.

Efficiency was a critical factor during this analysis as methods such as K-Anonymity Protection Scheme introduced significant computational overhead due to the need for clustering and anonymization processes, which delayed data uploads. CE-IoV performed better in this area but still incurred additional processing time due to location obfuscation methods. PriDUS optimized performance by offloading computational tasks to RSU-Edge, allowing vehicle to transmit privacy-protected data without requiring excessive processing power.

Transmission duration further showed the differences between the methods in the analysis. Figure 6 showed that PriDUS maintained a stable transmission time of 100–150 ms while K-Anonymity Protection Scheme exceeded 200 ms due to the additional processing required. CE-IoV performed slightly better but still introduced a transmission duration in the range of 150–250 ms. The shorter transmission time of PriDUS allowed it to be more suitable for real-time applications where low-latency communication was essential.

Security against common IoV attacks was another major consideration in this study. K-Anonymity Protection Scheme was particularly vulnerable to long-term tracking attacks, as adversaries could gradually infer vehicle identities by analyzing location updates over time. CE-IoV offered moderate protection but relied on obfuscation methods that might not have been sufficient against advanced tracking methods. Consequently, PriDUS significantly improved security by

dynamically regenerating sub-IDs, allowing it to be nearly impossible in connecting multiple interactions to the same vehicle.

The comparison showed the need for privacy-preserving methods that could adapt to real-time IoV environments. Traditional methods such as location obfuscation and static anonymization struggled to protect privacy in scenarios where vehicle movement was unpredictable. PriDUS overcame these challenges by incorporating TSSA with dynamic grouping, ensuring continuous protection even as network conditions changed. Future improvements could focus on increasing PriDUS with decentralized trust mechanisms, such as blockchain to remove reliance on a central authority for managing sub-IDs. Incorporating clustering-based privacy methods could further optimize computational efficiency, particularly in large-scale IoV deployments. Finally, PriDUS showed significant advantages in privacy protection, adaptability, and efficiency, allowing it to be a strong candidate for future IoV applications where real-time, low-latency communication and dynamic security mechanisms were required.

6. Conclusions

In conclusion, this study proposed PriDUS, an innovative privacy-preserving scheme designed specifically for the Internet of Vehicles (IoV). The scheme effectively protected vehicle IDs during data transmission by incorporating TSSA and introducing dynamic vehicle grouping. The simulation results showed that PriDUS significantly reduced the probability of privacy leakage to approximately 2.5%, much lower than existing methods such as K-Anonymity and CE-IoV, where leakage probabilities ranged from 6% to 13%. Furthermore, the data transmission duration remained in an acceptable range of 100 to 150 milliseconds, even in high-density and dynamic vehicle environments with up to 200 participating vehicles. A major strength of the scheme was its ability to address the challenges associated with dynamic IoV networks. The dynamic grouping mechanism enabled vehicle to adapt to frequent changes in membership in RSU coverage areas, ensuring stable communication and efficient sub-ID collection. PriDUS leveraged computational support through RSU-Edge units for sub-ID generation and data verification in a cloud-edge-vehicle architecture. However, one limitation was the computational burden on RSUs, which could reduce efficiency under high workloads. Incorporating edge computing near RSUs provides a feasible solution to mitigate this challenge and improve scalability. Future improvements could include augmenting PriDUS with blockchain technology to enable decentralized storage of vehicle IDs, reducing risks associated with centralized databases. Additionally, incorporating the scheme with clustering-based methods, such as K-Anonymity, could optimize computational resources and further facilitate its application in large-scale IoV deployments.

Author Contributions

Zheng Jiang conducted the research, developed the proposed PriDUS scheme, performed the simulations, and prepared the initial draft of the manuscript. Fang-Fang Chua and Amy Hui-Lan Lim extensively reviewed the manuscript, provided critical intellectual input, and contributed substantially to revising and refining the manuscript. All authors have read and approved the final manuscript.

Conflict of Interest

The authors declare no conflicts of interest.

References

Babkin, I, Pisareva, O, Starikovskiy, A, Guljakhon, M & Anoshina, Y 2021, 'Justification of an integrated approach to ensuring information security of unmanned vechicle in intelligent transport systems', *International Journal of Technology*, vol. 12, no. 7, pp. 1407-1416, https://doi.org/10.14716/ijtech.v12i7.5399

Benarous, L & Kadri, B 2022, 'Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vechicle', *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 461-472, https://doi.org/10.1007/s12083-021-01233-z

Chen, W, Wu, H, Chen, X & Chen, J 2022, 'A review of studyon privacy protection of Internet of Vechicle based on blockchain', *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, article 86, https://doi.org/10.3390/jsan11040086

Fan, W, Zhang, Y, Zhou, G & Liu, YA 2024, 'Deep reinforcement learning-based task offloading for vehicular edge computing with flexible RSU-RSU cooperation', *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 7, pp. 7712-7725, https://doi.org/10.1109/TITS.2024.3349546

Gao, Z, Zhang, D, Zhang, J, Liu, L, Niyato, D & Leung, VC 2023, 'World state attack to blockchain based IoV and efficient protection with hybrid RSUs architecture', *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 9952-9965, https://doi.org/10.1109/TITS.2023.3268222

Garg, T, Kagalwalla, N, Churi, P, Pawar, A & Deshmukh, S 2020, 'A survey on security and privacy issues in IoV', *International Journal of Electrical & Computer Engineering*, vol. 10, no. 5, pp. 5409–5419, https://doi.org/10.11591/ijece.v10i5.pp5409-5419

Guerna, A, Bitam, S & Calafate, CT 2022, 'Roadside unit deployment in internet of vechicle systems: A survey', *Sensors*, vol. 22, no. 9, article. 3190, https://doi.org/10.3390/s22093190

Hasan, N, Aziz, AA, Mahmud, A, Alias, YB, Besar, RB, Hakim, L & Hamidi, MAB 2024, 'Vehicle sensing and localization in vehicular networks', *International Journal of Technology*, vol. 15, no. 3, pp. 641-653, https://doi.org/10.14716/ijtech.v15i3.5385

He, Y, Wang, D, Huang, F, Zhang, R, Gu, X & Pan, J 2023, 'A V2I and V2V collaboration framework to support emergency communications in ABS-aided Internet of Vechicle', *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 4, pp. 2038–2051, https://doi.org/10.1109/TGCN.2023.3245098

Hu, X, Li, R, Wang, L, Ning, Y & Ota, K 2023, 'A data sharing scheme based on federated learning in IoV', *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11644–11656, https://doi.org/10.1109/TVT.2023.3266100

Huang, HF & Chang, CC 2006, 'A novel efficient (t, n) threshold proxy signature scheme', *Information Sciences*, vol. 176, no. 10, pp. 1338–1349, https://doi.org/10.1016/j.ins.2005.02.010

Iwamura, K., & Kamal, A. A. A. M. (2023). Communication-efficient secure computation of encrypted inputs using (k, n) threshold secret sharing. IEEE Access, 11, 51166-51184. https://doi.org/10.1109/ACCESS.2023.3278995

Jeong, H, Shen, Y, Jeong, J & Oh, T 2021, 'A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications', *Vehicular Communications*, vol. 31, no. 1, article 100349, https://doi.org/10.1016/j.vehcom.2021.100349

Jeremiah, SR, Yang, LT & Park, JH 2024, 'Digital twin-assisted resource allocation framework based on edge collaboration for vehicular edge computing', *Future Generation Computer Systems*, vol. 150, pp. 243–254, https://doi.org/10.1016/j.future.2023.09.001

Jia, X, Xing, L, Gao, J & Wu, H, 2020. A survey of location privacy preservation in social internet of vehicles, *IEEE Access*, vol. 8, pp. 201966-201984, https://doi.org/10.1109/ACCESS.2020.3036044

Karim, SM, Habbal, A, Chaudhry, SA & Irshad, A 2022, 'Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions', *Security and Communication Networks*, vol. 2022, article 1131479, https://doi.org/10.1155/2022/1131479

Li, W, Ding, Y, Yang, Y, Sherratt, RS, Park, JH & Wang, J 2020, 'Parameterized algorithms of fundamental NP-hard problems: A survey', *Human-centric Computing and Information Sciences*, vol. 10, article 29, https://doi.org/10.1186/s13673-020-00226-w

Li, Y, Dong, E, Zhang, Y, Xu, S & Zan, J 2023, 'Driving style clustering study based on HighD dataset', *Proceedings of the 2023 5th International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, vol. 2023, pp. 380–383, https://doi.org/10.1109/ICAICA58456.2023.10405469

Liang, J, Peng, H, Li, L, Tong, F, Bao, S & Wang, L 2023, 'A secure and effective image encryption scheme by combining parallel compressed sensing with secret sharing scheme', *Journal of Information Security and Applications*, vol. 75, article 103487, https://doi.org/10.1016/j.jisa.2023.103487

Lin, HY 2023, 'Secure data transfer based on a multi-level blockchain for internet of vechicle', *Sensors*, vol. 23, no. 5, article 2664, https://doi.org/10.3390/s23052664

Liu, R & Pan, J 2023, 'CRS: A privacy-preserving two-layered distributed machine learning framework for IoV', *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1080-1095, https://doi.org/10.1109/JIOT.2023.3287799

Naouri, A, Nouri, NA, Khelloufi, A, Sada, AB, Naouri, S, Ning, H & Dhelim, S 2024, 'BusCache: V2V-based infrastructure-free content dissemination system for Internet of Vechicle', *IEEE Access*, vol. 12, pp. 37663-37678, https://doi.org/10.1109/ACCESS.2024.3374881

Pan, R, Jie, L, Zhang, X, Pang, S, Wang, H & Wei, Z 2022, 'A V2P collision risk warning method based on LSTM in IOV', *Security and Communication Networks*, vol. 2022, article. 7507573, https://doi.org/10.1155/2022/7507573

Qi, Z & Chen, W 2023, 'Location privacy protection of IoV based on blockchain and k-anonymity technology', *Proceedings of the 2023 6th International Conference on Electronics Technology (ICET)*, vol. 2023, pp. 15-21, https://doi.org/10.1109/ICET58434.2023.10211967

Rathore, MS, Poongodi, M, Saurabh, P, Lilhore, UK, Bourouis, S, Alhakami, W & Hamdi, M 2022, 'A novel trust-based security and privacy model for internet of vechicle using encryption and steganography', *Computers and Electrical Engineering*, vol. 102, article 108205, https://doi.org/10.1016/j.compeleceng.2022.108205

Sitinjak, C, Ismail, R, Fajar, R, Bantu, E, Shalahuddin, L, Yubaidah, S & Simic, V 2023, 'An analysis of end-of-life vehicle management in Indonesia from the perspectives of regulation and social opinion', *International Journal of Technology*, vol. 14, no. 3, pp. 474–483, https://doi.org/10.14716/ijtech.v14i3.5639

Sodhro, AH, Rodrigues, JJ, Pirbhulal, S, Zahid, N, de Macedo, ARL & de Albuquerque, VHC 2020, 'Link optimization in software defined IoV driven autonomous transportation system', *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3511–3520, https://doi.org/10.1109/TITS.2020.2973878

Teoh, TS, Em, PP & Ab Aziz, NA 2023, 'Vehicle localization based on IMU, OBD2, and GNSS sensor fusion using extended Kalman filter', *International Journal of Technology*, vol. 14, no. 6, pp. 1237-1246, https://doi.org/10.14716/ijtech.v14i6.6649

Tuyisenge, L, Ayaida, M, Tohme, S & Afilal, LE 2018, 'Network architectures in internet of vehicles (IoV): Review, protocols analysis, challenges and issues', *In:* Internet of Vehicle. Technologies and Services Towards Smart City: 5th International Conference, pp. 3-13, https://doi.org/10.1007/978-3-030-05081-8_1

Wang, X, Zhu, H, Ning, Z, Guo, L & Zhang, Y 2023, 'Blockchain intelligence for internet of vechicle: Challenges and solutions', *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp.2325-2355, https://doi.org/10.1109/COMST.2023.3305312

Wang, Y, Hu, X, Guo, L & Yao, Z 2020, 'Research on V2I/V2V Hybrid Multi-hop Edge Computing Offloading Algorithm in IoV Environment', *Proceedings of the 2020 IEEE 5th International Conference on Intelligent Transportation Engineering (ICITE)*, vol. 2020, pp. 336–340, https://doi.org/10.1109/ICITE50838.2020.9231334

Wang, Z, Zhan, J, Duan, C, Guan, X, Lu, P & Yang, K 2022, 'A review of vehicle detection techniques for intelligent vechicle', *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 8, pp. 3811–3831, https://doi.org/10.1109/TNNLS.2021.3128968

Whulanza, Y 2023, 'Progressing the sustainable mobility: View of electric vechicle', *International Journal of Technology*, vol. 14, no. 3, pp. 455–459, https://doi.org/10.14716/ijtech.v14i3.6465

Zayed, AI & Butzer, PL 2001, 'Lagrange interpolation and sampling theorems', In: *Nonuniform Sampling: Theory and Practice*, pp. 123–168, https://doi.org/10.1007/978-1-4615-1229-5_3

Zhang, E, Chang, J & Li, Y 2021, 'Efficient threshold private set intersection', *IEEE Access*, vol. 9, pp. 6560–6570, https://doi.org/10.1109/ACCESS.2020.3048743

Zhou, H, Xu, W, Chen, J & Wang, W 2020, 'Evolutionary V2X technologies toward the Internet of vechicle: Challenges and opportunities', *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308–323, https://doi.org/10.1109/JPROC.2019.2961937

Zhou, X, Bilal, M, Dou, R, Rodrigues, JJ, Zhao, Q, Dai, J & Xu, X 2023, 'Edge computation offloading with content caching in 6G-enabled IoV', *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 3, pp. 2733–2747, https://doi.org/10.1109/TITS.2023.3239599

Zuo, K, Chu, X, Hu, P, Ni, T, Jin, T, Chen, F & Shen, Z 2024, 'Security enhanced privacy-preserving data aggregation scheme for intelligent transportation system', *The Journal of Supercomputing*, vol. 80, pp. 13754–13781, https://doi.org/10.1007/s11227-024-05995-0