sensors

MDPI

Article

Resilient Privacy Preservation Through a Presumed Secrecy Mechanism for Mobility and Localization in Intelligent Transportation Systems

Meshari D. Alanazi [1], Mohammed Albekairi [1], Ghulam Abbas [2], Turki M. Alanazi [3], Khaled Kaaniche [1], Gehan Elsayed [4,*] and Paolo Mercorelli [5,*]

1 Department of Electrical Engineering, College of Engineering, Jouf University, Sakakah 72388, Saudi Arabia
2 School of Electrical Engineering, Southeast University, Nanjing 210096, China
3 Department of Electrical Engineering, College of Engineering, University of Hafr Al Batin, Hafr Al Batin 39524, Saudi Arabia
4 Department of Interior Design, College of Engineering, Jouf University, Sakakah 72388, Saudi Arabia
5 Institute for Production Technology and Systems (IPTS), Leuphana Universität Lüneburg, 21335 Lüneburg, Germany
* Correspondence: gaielsayed@ju.edu.sa (G.E.); paolo.mercorelli@leuphana.de (P.M.)

Abstract: An intelligent transportation system (ITS) offers commercial and personal movement through the smart city (SC) communication paradigms with hassle-free information sharing. ITS designs and architectures have improved via information and communication technologies in recent years. The information shared through the communication medium in SCs is exposed to adversary risk, resulting in privacy issues. Privacy issues impact the contingent mobility and localization of the ITS path. This paper introduces a novel resilient privacy preserving (RPP) method through presumed secrecy (PS) to provide a robust privacy measure. The privacy of the progressive communication sessions is preserved based on the previous security depletion levels. The interruptions in traffic data-related communication sessions are recurrently identified, and re-handoffs are recommended with dodged transfer learning. The empirical results indicate a 25% reduction in computational overhead and a 30% enhancement in privacy protection over conventional methods, demonstrating the model's efficacy in secure ITS communication. Compared with existing methods, the proposed approach decreases security depletion rates by 15% across varying traffic densities, underscoring ITS resilience in high-interaction scenarios.

Keywords: forward secrecy; intelligent transportation; smart cities; transfer learning; machine learning

check for updates

Academic Editor: Qiong Wu

Received: 12 November 2024
Revised: 26 December 2024
Accepted: 26 December 2024
Published: 27 December 2024

Citation: Alanazi, M.D.; Albekairi, M.; Abbas, G.; Alanazi, T.M.; Kaaniche, K.; Elsayed, G.; Mercorelli, P. Resilient Privacy Preservation Through a Presumed Secrecy Mechanism for Mobility and Localization in Intelligent Transportation Systems. *Sensors* **2025**, *25*, 115. https://doi.org/10.3390/s25010115

1. Introduction

Data and communication privacy are critical in intelligent transportation systems (ITSs), which handle sensitive information such as vehicle positions and personal details. The connectivity between automobiles and infrastructure raises the possibility of data leaks [1]. Unauthorized access can result in catastrophic consequences, such as identity theft and data manipulation. Protecting communication privacy is critical for maintaining user safety and confidence [2]. Encryption and anonymization techniques contribute to the security of sensitive data. The dynamic nature of these systems necessitates ongoing attention to privacy concerns. A well-secured communication channel increases security and public trust [3,4]. Effective privacy protections keep hostile actors from exploiting transportation data. Strong privacy protection techniques are required as digital communication merges with transportation [5]. Data integrity and privacy are critical for efficient operations in smart city infrastructures. Addressing privacy concerns safeguards consumers and enhances transport systems. Cities that promote privacy can provide a safer environment for their citizens. A dedication to communication privacy is critical to the future of an ITS [6,7].

Session authentication is critical for secure communication in an ITS because it confirms the identities of all parties involved. Such a method prevents unauthorized access and ensures that only legitimate users share sensitive transportation data [8]. Variable key exchanges establish secure connections, lowering the danger of interception or manipulation. Regular re-authentication improves communication security, particularly in real-time traffic systems requiring consistent data flow [9]. Lightweight cryptographic approaches ensure that security measures do not reduce data transmission efficiency. These techniques are critical for preserving the speed and dependability of an ITS. Authentication protocols detect and respond to potential security risks, resulting in a safe environment for data exchange [10,11]. Proper session authentication prevents unauthorized access and ensures communication integrity. Such security is critical for establishing trust in intelligent transportation technologies [12]. Effective session authentication protects sensitive information and increases user confidence. To satisfy changing security requirements, authentication systems must be continuously improved. New strategies are always being developed to successfully address difficulties [13].

Machine learning (ML) techniques are essential for ensuring privacy in an ITS. These allow for the real-time identification and mitigation of potential security issues. These algorithms can find trends in massive datasets from transportation systems that indicate weaknesses or assaults [14]. ML models improve security by predicting and preventing future intrusions. Automated detection and response systems that use ML eliminate the need for manual monitoring [15]. Such technologies evaluate the degree of security issues, enabling more precise responses. ML improves encryption algorithms and detects holes in existing security protocols [16]. The capacity to handle huge amounts of data enables an ITS to avoid new hazards. Using ML improves privacy and overall security in transportation networks [17]. Such integration results in more efficient operations and improved resource allocation. As technology improves, ML's significance in ensuring security will become more important [17]. A bi-level planning model was proposed in [18] to locate and size Multi-Functional Charging Station (MFCS) which can recharge Battery Electric Vehicle (BEV), Hydrogen Fuel-Cell Vehicle (HFCV), and Natural Gas Vehicle (NGV) at the same time in a medium-sized city with different functional areas. The proactive strategy allows organizations to respond quickly to anticipate difficulties. ML and intelligent transportation will collaborate to create future developments and improve system performance [19].

Several limitations exist to the efficiency of the existing privacy-preserving techniques for mobility and localization in intelligent transportation systems (ITSs). For real-time use, a reasonable compromise between privacy and location accuracy is lacking in many existing solutions. Even with encryption and obfuscation, they are still susceptible to complex attacks like inference and de-anonymization attacks that utilize machine learning to reveal user identities. In addition, these methods are not always scalable; thus, they cannot keep up with the increasing volume of cars and gadgets in large-scale ITS schemes. However, as most of these techniques fail to work with advanced localization algorithms, including those based on probabilistic or deep learning, the system performance is less than ideal. Due to these difficulties, a more robust, scalable, and integration-friendly strategy is required to guarantee strong privacy in ever-changing ITS environments.

The contributions are as follows:

- A resilient privacy preserving (RPP) mechanism with adaptive security, which proposes enhanced privacy in intelligent transportation systems (ITSs).
- A dodged transfer learning approach is developed for proactive breach detection and optimized re-handoff recommendations.
- A mutual lightweight key exchange protocol is introduced to reduce adversarial access during vehicle handoffs.
- Comparative analysis is conducted, which demonstrates the improved security and computational efficiency of the existing method.

The remainder of the paper is as follows: Section 3 discusses the recent literature review on the proposed topic. Section 3 describes in detail the proposed methodology and the results obtained. The discussion is carried out in Section 4. The conclusion of the paper is drawn in Section 5.

2. Related Works

Qureshi et al. [20] developed a blockchain (BC)-based privacy-preserving authentication (BPPAU) model for intelligent transportation systems (ITSs). Data storage and processing management are analyzed to identify the threats that cause data leakage and data losses. The BPPAU model provides a secure solution to complex ITS application threats. The developed BPPAU model improves the performance and security range of an ITS. Chen et al. [21] introduced a differential privacy (DP)-based privacy-preserving data publishing (PPDP) algorithm for smart transportation. A query probability model is employed here to identify the errors while performing preserving tasks. The introduced algorithm analyzes the impact of smart card trajectory data, producing a feasible set of information for PP services. The introduced algorithm maximizes the computational efficiency range of the systems. Gao et al. [22] proposed a location privacy-oriented task offloading (PPO2) method for an ITS. A deep reinforcement learning (DRL) algorithm is implemented to provide necessary planning services. The proposed method is used to identify the offloading problems that cause issues with the PP service. The DRL algorithm minimizes the risk factor, elevating the systems' efficiency. The proposed PPO2 method reduces the computational cost and privacy data loss rate in an ITS.

Li et al. [23] developed a PP-distributed transfer learning protocol for an ITS. The protocol solves the system's scarcity level, elevating the functional capabilities. The developed protocol provides effective PP services to ensure the safety and security range of users' data during data transmission and sharing processes. The developed protocol enlarges the efficiency and effectiveness of ITS applications. Saleem et al. [24] designed a conditional-privacy access control protocol for intelligent customer-centric communication in VANET. A trusted authority (TA) is employed here to tackle the issues that cause risks and threats to the user's data. The TA also analyzes the data's security range, eliminating the process's compactional cost. Experimental results show that the designed protocol achieves high accuracy and efficiency in providing privacy services. Din et al. [25] introduced a context-aware cognitive memory trust management system (CACMTM) model for an ITS. The introduced model is used to provide trustworthy communication services to the users of ITS applications. The context-aware cognitive memory trust management system (CACMTM) model identifies the demands and requests that the users make. The identified demands are analyzed to provide optimal services. The introduced model enlarges the safety and privacy ratio of user data.

Zhu et al. [26] developed a poisoning attack method using federated learning (FL) with a perturbation coefficient multiplied by maximum value (PMM) for ITS applications. The developed method is used to identify the hierarchical poisoning attacks and defenses that occur during data transmission. The method also provides specific PP services to secure the data leakage range in an ITS. The developed method maximizes the effectiveness level of the systems. Qu et al. [27] proposed a new personalized FL (PFL)-based information fusion method for privacy protection in an ITS. The PFL is used here to analyze the data nodes which contain users' personal information. It also eliminates the unwanted noise which is presented in the data. The method evaluates the parameters and provides feasible PP services to the data. Compared with others, the proposed method enhances the accuracy of privacy protection in an ITS applications. The methods and findings from [28–37] are summarized in Table 1.

Table 1. Summary of the purposes, methodologies and findings from [28–37].

Author	Purpose	Methodology	Findings
Jiang et al. [28]	It is used to encrypt user's data from third parties.	BC technology is used here to analyze the keywords during data sharing.	Reduces the computational cost.
Zuo et al. [29]	It is used to ensure the safety and security range of personal data.	Modified Paillier cryptosystem is employed to protect data loss.	Maximizes the performance.
Fan et al. [30]	The model is used to identify the threats that cause issues to PP policies.	A decentralized autonomous organization (DAO) is implemented in the model to analyze the relevant data for providing PP services.	Elevates the effectiveness level of the systems.
Zhu et al. [31]	It provides feasible security policies to ensure the safety of users' data.	The reinforcement learning (RL) algorithm is also used here to encrypt the necessary data before sharing processes.	Reduces the communication cost and application overheads.
Gupta et al. [32]	It is used to enhance the performance of communication services.	ML algorithm is used here to detect unwanted threats while travelling.	Elevates the efficiency range of the systems.
Zhang et al. [33]	It is used to ensure the safety and privacy level of the communication process.	V2C requires effective PP policies to secure data while sharing.	Increases the performance range of the system.
Sun et al. [34]	It is used to analyze the main source of the images.	The actual purpose and necessity of the images are identified for the encryption process.	Minimizes the computational cost and complexity range.
Sun et al. [35]	It is used to enhance the storage capacity by improving the security.	BC technique is employed here to identify the optimal authentication and access request over data.	Enhances the efficiency and performance range of the systems
Xu et al. [36]	It is used to solve privacy issues while performing communication services.	BC is used to analyze the key values and factors for the authentication process.	Increases the effectiveness ratio.
Qiong Wu et al. [37]	It provides edge caching for next-generation networks by empowering caching units in small-cell base stations (SBSs), allowing user equipment (UE) to fetch users' requested contents that are pre-cached in an SBS.	A cooperative edge caching scheme based on elastic federated and multi-agent deep reinforcement learning (CEFMR) is used to optimize the cost in the network.	Enhancing the overall performance ratio

Developing an ITS in smart cities is familiar in areas where road side units (RSU) aid autonomous vehicle transmission. The role of this RSU is to sense the traffic on the road and transmit it to the nearby vehicle that reaches the same traffic flow path. This communication facilitates information exchange from the RSU to avoid unnecessary traffic. It includes mutual key authentication with secure traffic data exchange between the vehicles. Using a handoff mechanism, the RSU is responsible for sharing the data with the nearby vehicle. This mechanism is used to identify the interlinked vehicle and the ITS data that are to be exchanged with each other. Analyzing this traffic management phase, the security-related process is executed using encryption and decryption. Accuracy, privacy, and scalability are challenges for traditional approaches when dealing with the massive amounts of real-time data produced by infrastructure, connected vehicles, and sensors. Machine learning algorithms effectively, efficiently and accurately predict outcomes from massive datasets containing various variables. Machine learning (ML) improves the balance between privacy and system efficiency, allows for reliable localization even in unpredictable environments, and adjusts to new security risks. The suggested system can adapt to changing network circumstances, complex privacy assaults, and the need to integrate with other ITS components due to ML.

3. Proposed Resilient Privacy Preservation (RPP) Through Presumed Secrecy (PS)

The proposed work focuses on mutual key exchange by reducing adversary control and evaluating the security level of data sharing. In this processing step, smart cities allow autonomous vehicles to transmit among each other, and the analysis is used to observe the key generation, which is said to be a handoff. The handoff works remotely on two vehicles; based on the user, access is given on one device, paused, and then continues on toward other devices with the required security. From this examination phase, the handoff key is used to observe the interrelated road traffic management issues. This work mainly focuses on privacy-related issues handled using handoff- and recommendation-based techniques. As discussed in the section below, the proposed technique is one of transfer learning for a dodged mechanism.

In the execution step, traffic management is used to decrease the traffic flow and reduce congestion. This is undertaken using transfer learning with the existing knowledge of autonomous vehicles and roads; knowledge which provides the relevant information needed to avoid traffic. This step measures the security level without any adversary accessing the data from the vehicle. The initial step is to discuss the challenges faced when there are interrelated traffic management systems, which are observed in the equation below.

$$Yi'\left(T_f, M_g\right) = \sum_{h_0}^{h_1} (M_s + f_w) * n' + F_d * pr_0 \tag{1}$$

The above Equation (1) represents the traffic management analysis for the traffic flow. The analysis is described as Yi', T_f is the traffic and M_g is the management, vehicle is h_0, n number of vehicles is h_n, and the information is n'. The smart cities are labeled as M_s, identification is F_d, and the transportation is pr_0. From these derivatives, the transportation of information is carried out $pr_0(n') \to h_0$.

Definition 1. *Consider* $Yi'(h_n) * n' > f_w$*, this refers to the higher traffic flow on the road. So, to avoid this* $n'(pr_0) * M_s + R'$*,* R' *is the RSU, where* $R' \in M_s\left(T_f\right) + h_n$*. This observation step illustrates the data exchange and the condition is* $x_h(h_0 \to h_1) * pr_0 + T_f < f_w$*.*

$$h_n = n'(f_w + F_d) * M_s\left(T_f\right) - pr_0$$

$$F_d{}^2 = Yi' + \{(R' + x_h) \rightarrow h_n\}$$

$$T_f \cup R' = h_0 + \{(pr_0 \vee F_d), (x_h \wedge h_1)\}$$

$$T_f \cap R' = h_0 + \{(pr_0 \wedge F_d), (x_h \vee h_1)\}$$

These are used to examine vehicle transportation and the exchange of information, and are symbolized as x_h, with h_1 as the nearby vehicle. The union of $T_f \cup R'$ for $\{(pr_0 \vee F_d), (x_h \wedge h_1)\}$, whether the data exchange between vehicles is achieved or not, is represented in union data, whereas the transportation of data and identification is always carried out. The same case inversely acts on the interaction of $T_f \cap R'$, as the condition delivers $\{(pr_0 \wedge F_d), (x_h \vee h_1)\}$. The conditions work for the union and intersection of two vehicles, and the optimization strategy works for the smart city's data exchange. From this, traffic management in smart cities is observed in the following Equation.

$$T_f(M_g) = (n_v - \alpha) + [R'(x_h) + Yi'] + f_w \tag{2a}$$

This is expressed as,

$$F_d(h_0, \ldots h_n) = \left[\sqrt{n_v} + n' * \prod_{I_r}^{\alpha} (pr_0 * R')\right] * (x_h \rightarrow o_x) - pr_0 \tag{2b}$$

From the above Equations (2a) and (2b), traffic management plays a vital role in traffic flow. Here, the identification of traffic on the road is achieved with the use of an RSU, which provides the necessary action according to $R'(F_d * f_w) * n_v$. The navigation is completed if there is no traffic, or if less traffic is detected, and is represented as n_v. Congestion occurs due to traffic on the roadside, and is described as α, with the interaction labelled as I_r. In this case, the formula is $M_g(R' + f_w) * F_d \rightarrow h_n$. On this basis, congestion is when a security level for the traffic management system is provided. The evaluation occurs for the RSU and roadside vehicles when the smart city observes a vehicle causing congestion. The congestion is managed in the below derivative.

Definition 2. *Consider the congestion rate* $\left(\alpha + T_f\right) * \sum_{F_d}(Yi' + M_g)$*, where it is denoted as* $(F_d * R') + M_s(h_n)$*. This is observed for the RSU-based road traffic observation and finds the trafficless route with the navigation* $n_v\left(T_f * n'\right) * x_h$.

$$Yi' = (n' + R') * |n_v - F_d| + \left\{pr_0^2 + (h_0 * f_w)\right\}, \textit{ where } pr_0 < h_n$$

This means that

$$h_n > f_w(n' + x_h) * |F_d + R'|, \textit{ for all } R' \in M_s$$

which is similarly represented as,

$$\left\{\left((R' + M_g)^2 * |n' + x_h|^{-1}\right) * \left(T_f + pr_0\right)\right\}, \textit{ for all } pr_0 \in T_f$$

$$\text{Thus, } 0 \leq h_0\left(pr_0 + T_f\right) * n_v$$

$$R'(pr_0, I_r) = h_0(M_s, \alpha)$$

$$\left(T_f\right).n'^{(h_0, pr_0)} = 1 \Leftrightarrow \sqrt{\left[\prod_{n_v}^{R'}(n_v + M_g)\right] + \prod_{I_r}(h_1 \rightarrow h_n) + M_s} \tag{3a}$$

$$pr_0(n_v, M_s) = x_h(\alpha, n')$$

$$pr_0.I_r = 0 \Rightarrow \sum_{h_0}^{h_n} \left(T_f + n_v\right) * M_s + \sqrt{o_x + \left(T_f * R'\right)} \tag{3b}$$

The congestion rate is addressed in the above Equations (3a) and (3b), where the interaction is represented as I_r, o_x and is described as communication $I_r(h_0 \to h_1) * o_x(x_h) > 0$. Navigation is used to provide traffic on the road on which the congestion has been managed during the communication $R' + o_x(h_0 \to h_1)$. The information exchange and congestion-based traffic management are illustrated in Figure 1.

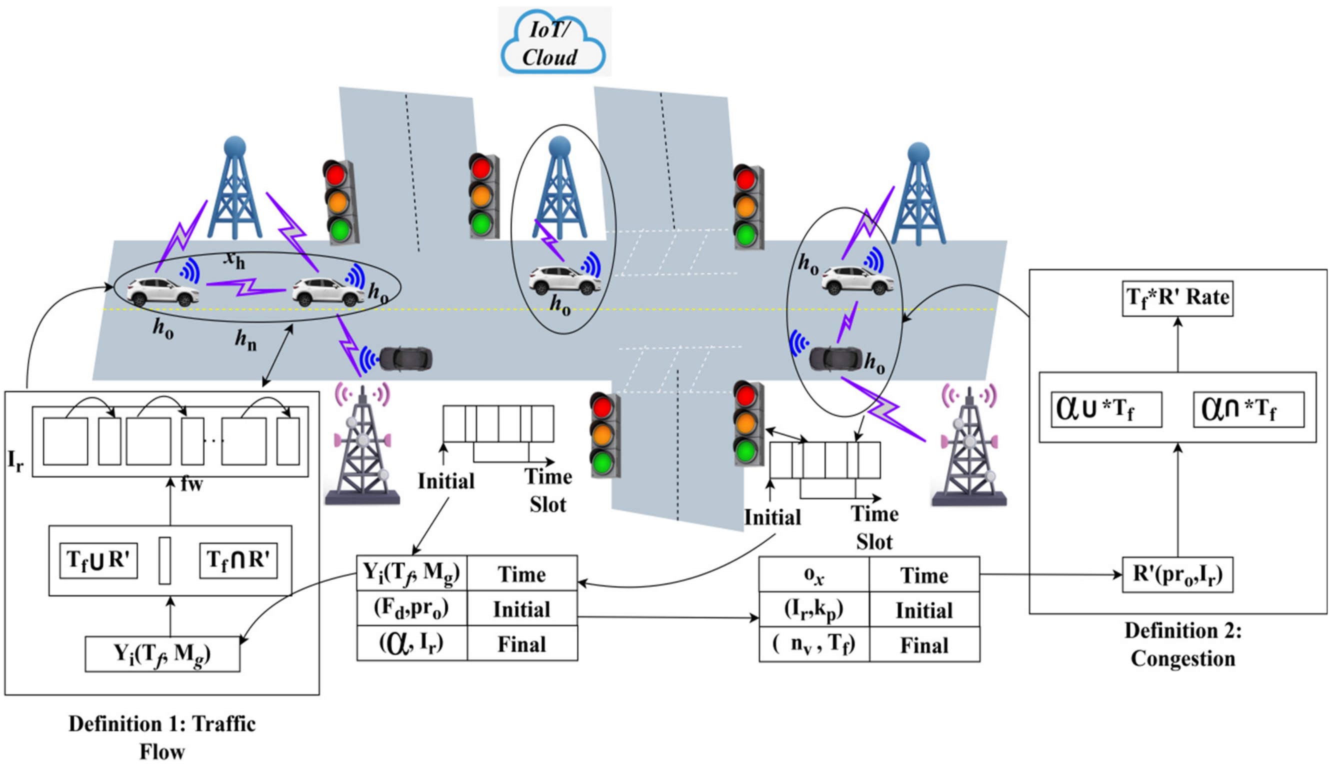

Figure 1. Information exchange and congestion-based traffic management.

Figure 1 illustrates the information exchange for traffic flow and congestion detection. The I_r (initial) to final o_x defines the rate of communication between $h_o \in h_n$ and the RSU's. The $Y_i\left(T_f, M_g\right)$ observed at the initial I_r is used to extract (F_d, pr_o) until (α, I_r) becomes the final x_h. In the increasing o_x, the I_r with k_p and n_v, while using T_f, are acknowledged to maximize congestion detection. In the detection and x_h process, $\left(\alpha \cup T_f\right)$ and $\left(\alpha \cap T_f\right)$ are validated with $\left(T_f \cup R'\right)$ and $\left(T_f \cap R'\right)$ to identify the maximum difference. If the difference maximization is pursued, then $F_d(h_o, \ldots, h_n)$ is performed for precise information updates. Based on the above information sharing, the I_r in any o_x interval is evaluated, as in Figure 2.

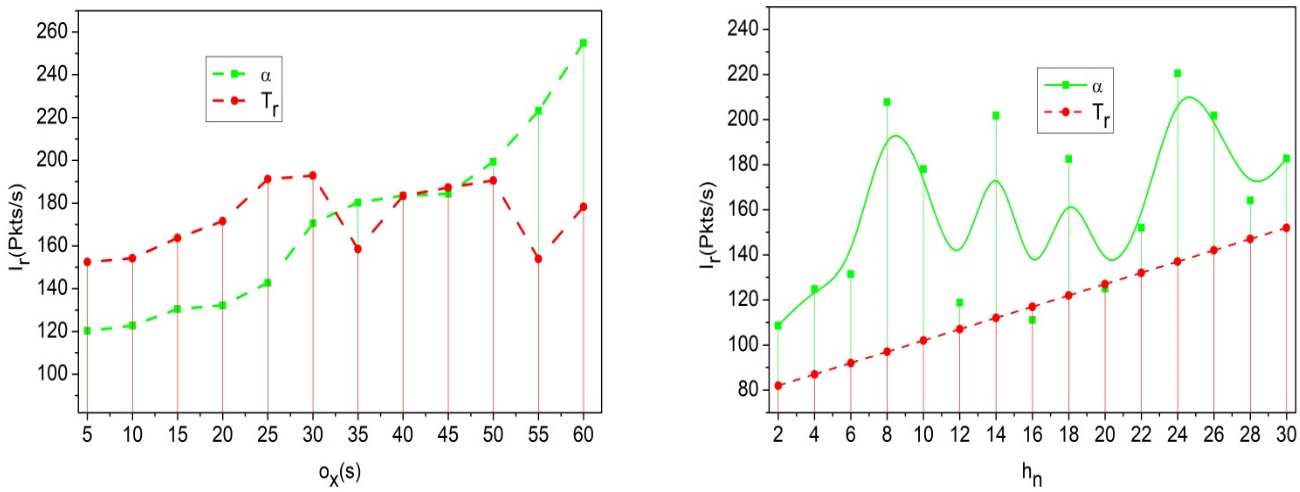

Figure 2. Interaction in different communication intervals.

The communication rate increases for the mutual key authentication, where transfer learning is used to analyze the secure communication with a pre-trained model $o_x(t_p + A_0) + h_0$. This evaluates the communication link among the vehicles and looks for the recommendation for handoff or re-handoff $H_f + L_v(f_w + t_p) * D_a$. Based on this recommendation, it uses the four parameters of transfer learning and produces a higher communication rate within the required time frame (Figure 2). The navigation is then examined and the security level is verified using a handoff. This illustrates the initialization and decision making discussed in the below section.

3.1. Handoff

Switching between the same access point or a different network can be either intra- or inter-technology. This is proposed in order to reduce the congestion rate between vehicle access points.

3.1.1. Handoff Algorithm: Initialization

1. This is used in the initialization state of congestion to avoid unnecessary handoffs and misinterpretation, as follows: $(i_m + F_d) * \sum_{n_v} f_w > R', \ where\ R' \in \alpha$ represent the vehicle data transfer, the misinterpretation of which is i_m and results in the below issues.
   - QoS degradation
   - Bandwidth and system load are increased or unused, leading to unused data sharing.
   - Packet losses occur due to blocking and termination during vehicle communication intervals.

   [align=parleft,leftmargin=*,labelsep=4.8mm]
2. The factors mentioned above are addressed with the vertical handoff mechanism, whereas switching to access points on a different network is undertaken as follows: $x_h(n' \rightarrow h_1) * |Yi' + M_s|^2$.

$$Int = \sum_{T_f}^{F_d} f_w + \{(M_g * R') + n_v\} - \alpha|Yi' + M_s|^2$$

That computes as follows:

$$x_h(n' \rightarrow h_1) > 0, \ where\ x_h \in M_g$$

This is substituted in Equation (3a), and is formulated as follows:

$$f_w(h_0, M_g) = \sqrt{o_x + \left(T_f * R'\right)} * i_m - k_p \tag{4}$$

To manage the issues mentioned above in Equation (4), an initialization is performed that addresses the packet losses and is described as k_p. The initialization is labelled as Int. This shows that the initialization of the handoff aids in the reduction of traffic using RSU.

3.1.2. Handoff Algorithm: Decision Making

1. From the initialization of the handoff, the decision making is followed up as $Int \approx D'$, where D' is the decision-making process. This refers to the higher initialization factor and resolves the handoff with misinterpretation issues, as follows: $F_d < i_m(x_h)$.
2. The decision is taken regarding the network and surrenders the handoff as the target and provides a seamless connection between the two vehicles, as follows: $\left(H_f + D'\right) + Int^{-1}$

$$D' = Int + \frac{n_v}{h_n} * f_w + \prod_{H_f} x_h * (I_r + i_m) - R'$$

This is represented as follows:

$$= I_r * \left\{(n_v + Int) * R'\right\} * H_f,\ where\ H_f > f_w$$

This is computed as in Equation (5), as follows:

$$= \prod_{H_f}^{h_0} F_d * \left(f_w + T_f\right) * M_g - R',\ for\ all\ M_g \in x_h \tag{5}$$

Thus, the decision-making is followed up for handoff, where the mutual key authentication is administered. The handoff is represented as H_f and the interaction is I_r. The handoff process with M_g is portrayed in Figure 3.

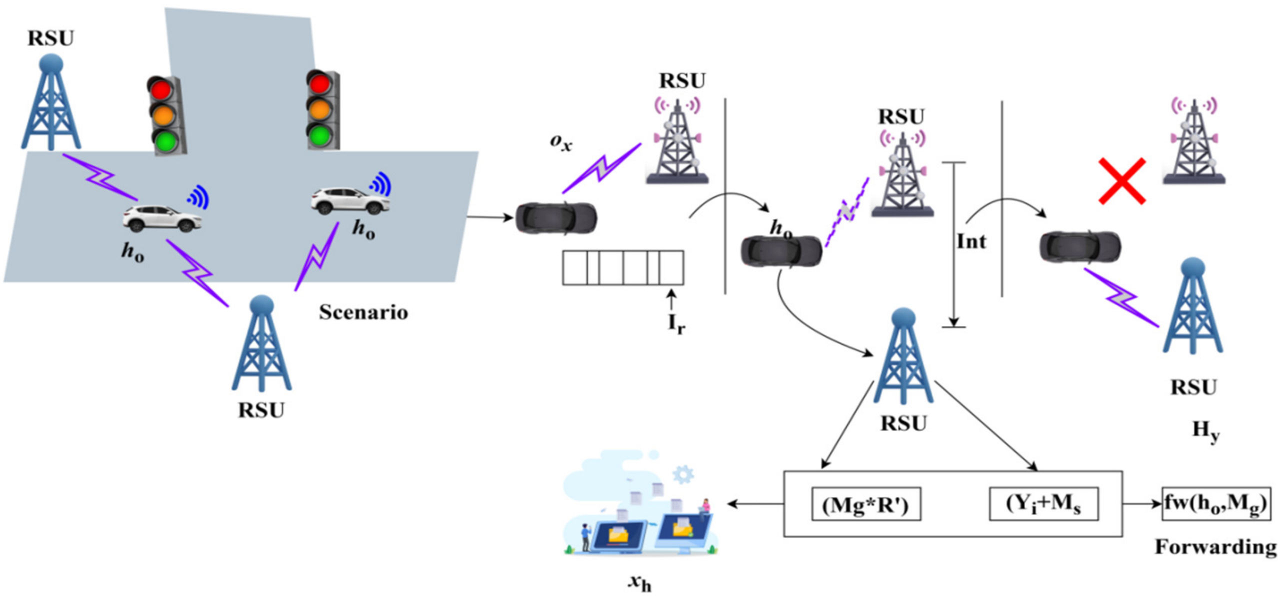

Figure 3. Handoff process illustration with transport management.

The Int and H_f processes are depicted in the above Figure 3. The I_r is interrupted by α information, such that, if $x_h(n' \rightarrow h_1)$ (i.e., the neighbor), then Int is performed. This Int

harmonizes $(M_g * R')\forall h_0$ and h_1 (within the range) provided $(Y_i + M_s)$ is the demanding requirement of the communicating $h_o \in h_n$. Therefore, the $[x_h(n' \to h_1) > 0]$ is a handoff-requiring case due to $k_p \neq 0$ outcomes. Thus, D' and $\left(f_w + T_f\right)$ in any o_x interval is the handoff output needed to ensure (reduce) k_p less I_r. The Presumed secrecy-based privacy is modified using different handoff authentication levels dictated by mutual key authentication, and is explained below.

3.2. Mutual Key Authentication

Mutual authentication is achieved using the encryption and decryption method associated with the key generation process. The private and public keys provide access to a particular vehicle and to traffic information. RSU is responsible for promptly transferring the information to the nearby vehicle without any security issues. As explained below, this ensures the private and public keys needed to access the information.

Definition 3. *By examining information exchange between the vehicles, traffic management, and QoS, bandwidth and packet loss improvements are made:* $x_h(o_x + h_1) * \sum_{n_v} i_m \leq \left(T_f, f_w\right)$.

$$M_k = enc \to x_h\left(n', h_1\right) * f_w + M_g$$

$$M_k = dec \leftarrow \left(\alpha - \left(f_w * x_h\right) + z_p - k_p\right)$$

The encryption and decryption are performed using the mutual key authentication M_k, which ensures higher security and privacy without adversaries.

$$= enc\left(n' \to h_1\right) * R'\left(M_g\right) - f_w$$

From this, decryption works as follows:

$$= dec \leftarrow R'\left(M_g\right) + \left|n' + z_p\right| * o_x$$

This is used as the access-based key generation method, and information sharing is followed up with higher security.

$$= R'(o_x \to h_1) * z_p\left(Yi' + M_g\right) - f_w \tag{6}$$

From the decryption process, the congestion and packet losses are addressed optimally as in Equation (6), and are represented as z_p. The encryption and decryption are represented as *enc* and *dec*, respectively. The analysis takes place for the RSU and provides mutual authentication through encryption. The initial stage is encryption, where the data are digitally modified, and decryption is used to extract the data. This concurrent process utilizes the handoff consolidated by mutual authentication. On this basis, the recommendation for the handoff is discussed in the dodged technique and is equated below.

$$D_a = D' + \left(enc * T_f\right) + f_w * \prod_{Yi'}\left(k_p - \alpha\right) \tag{7}$$

The recommendation is represented as D_a in Equation (7), based on transfer learning, the analysis is undertaken for one vehicle and shares the information with a higher handoff that relies on security. The privacy of the progressive communication sessions is preserved based on the previous security depletion levels. Mutual-key-based authentication is illustrated in Figure 4.

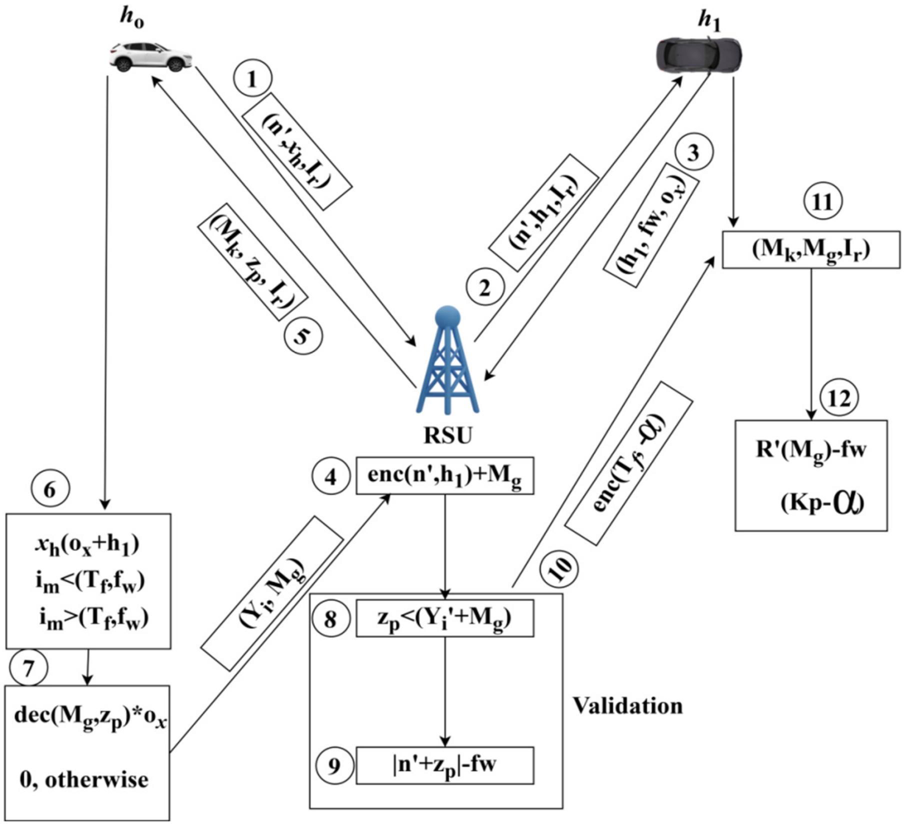

Figure 4. Mutual-key-based authentication illustration.

For the dodged H_f process illustrated in Figure 3, the sequence of M_k-based authentication for (h_0, h_1) privacy in I_r interval is represented in Figure 4. The numbered sequences in the above figure follow the authentication between two neighboring vehicles experiencing H_f. Depending on the various $\left(Y', M_g\right)$ instances, the $\left[enc(n', h_1) + M_g\right]$ (for $h_1 \rightarrow h_0$) and $\left[enc\left(T_f, -\alpha\right)\right]$ (for $h_0 \rightarrow h_1$) is implied. Unke the encryption process, the decryption is consistent for $z_p\left(Y_i + M_g\right)$ for f_w and T_f concurrently. The RSU is responsible for verifying these sequences [sequences (8) and (9)] to reduce the authentication time. Therefore, $\left[dec[\alpha - (f_w * x_h)]\forall\left(z_p - k_p\right) > 0\right]$ is responsible for balancing $\left(M_k, M_g,\ and\ I_r\right)$ under various o_x intervals (Figure 4). In Figure 5, the authentication time metric is analyzed using the different related variants and functions experienced.

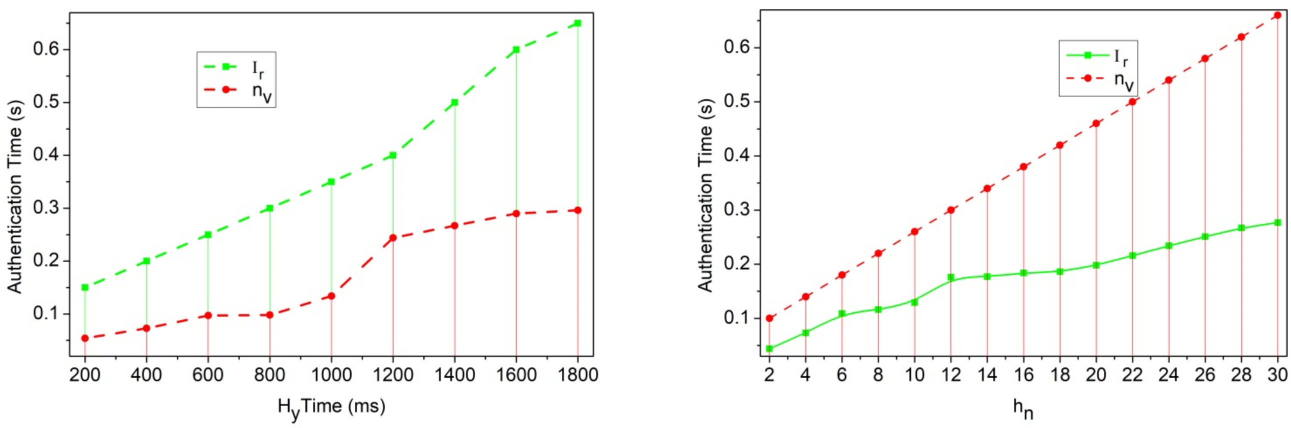

Figure 5. Authentication time analysis for different variants.

The authentication time is reduced among the vehicles and communicates with security. The security level is maintained based on the encryption and decryption of data, where it defines the traffic on the road and provides the data exchange according to $o_x(M_g + L_v) * n'$. On this basis, transportation for the data between the vehicles is achieved on a fixed time slot and so refers to the authentication time $pr_0 * \left(enc + H_f\right) + M_k$. This is balanced between the vehicles, and security is processed to reduce the congestion and packet losses (Figure 5). The interruptions in traffic data-related communication sessions are recurrently identified, and re-handoffs are recommended with dodged transfer learning after this transfer learning is used to identify data-related communication, with recommendations that include the handoff, as in Equation (8).

$$F_d = n_v + \left\|D_a * D'\right\| - i_m,\ where\ D_a \in H_f$$

$$n' = T_f(M_g * R'),\ H_f$$

$$x_h = h_0 * |\alpha + M_s| - pr_0$$

$$i_m = z_p * \sum\nolimits_{D_a} M_g + (Yi' * n_v) \tag{8}$$

The identification occurs regarding the recommendation for communication followed up with the handoff. The mutual authentication process is described below:

1. The initial step discussed here is encryption, where the information is sent to the security, $x_h(n') \rightarrow h_n$. The evaluation takes place by deciding the optimal solution among the vehicle information-sharing, $h_0 \rightarrow h_1\left(H_f * f_w\right)$. Based on the traffic flow, the data exchange is undertaken as follows: $x_h(f_w * enc) \rightarrow o_x(h_1)$.

Examining information exchange between the vehicles relates to traffic management and addresses challenges such as QoS, bandwidth, and packet losses, $x_h(o_x + h_1) * \sum_{n_v} i_m \leq \left(T_f, f_w\right)$.

2. $M_k = enc \rightarrow x_h(n', h_1) * f_w + M_g$
3. $M_k = dec \leftarrow (\alpha - (f_w * x_h) + z_p - k_p)$

The encryption and decryption are examined for the mutual key authentication M_k where it relates to higher security and privacy without adversaries.

$$= ency(n' \rightarrow h_1) * R'(M_g) - f_w$$

From this, decryption works by substitution with step 3 and is computed as follows:

$$= dec \leftarrow R'(M_g) + |n' + z_p| * o_x$$

This is used as the access-based key generation method, and information sharing is followed up with a higher security mechanism. This is observed by integrating point 4 and decryption, defined by $R'(o_x \rightarrow h_1) * z_p(Yi' + M_g) - f_w$.

From the decryption process, the congestion and packet losses are addressed in an optimization manner, represented as z_p. The encryption and decryption are represented as *enc and dec*, respectively. The analysis takes place for the RSU and provides mutual authentication as encryption. The initial stage is encryption, where the data are encrypted, and the decryption is used to open the data; this uses the handoff mechanism for mutual authentication. The privacy assessment rate is analyzed using the representations shown in Figure 6.

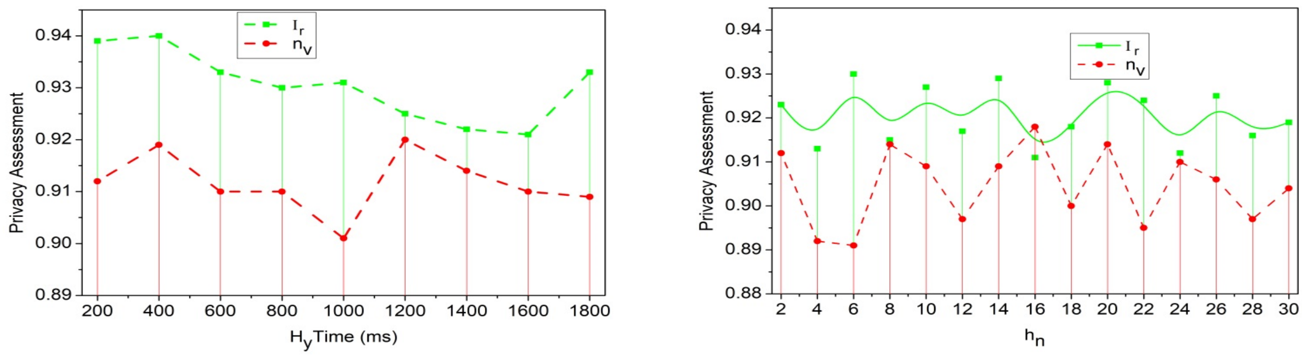

Figure 6. Privacy assessment rate.

The privacy assessment increases if traffic flow is detected on the road studied by an RSU. The RSU is responsible for securely forwarding the information to the nearby vehicle, $x_h \to h_0(o_x * pr_0) - H_f$. The handoff works according to privacy and ensures security among end-to-end vehicles, $H_f(h_0 \to h_1) + z_p(n_v)$. This observes the traffic flow on the road and navigates the vehicle to reduce the traffic. The reduction in traffic augments privacy assessment improvements in the proposed method (Figure 6). This execution evaluates the security-based dodged technique, which relies on transfer learning and is discussed in the following section.

3.3. Process of Dodged Transfer Learning

The neighbor information is fetched by the second vehicle supervised by the pre-trained model. The features and starting point of the vehicles are detected using a handoff, which provides security between the vehicles. This uses four parameters to define the congestion and packet losses, which are evaluated in the equation below.

Pre-trained and base model: the transfer learning performances are based on the pre-trained model, which identifies the vehicle's and road unit's common features and patterns. This information is stored in the database for future reference. The base model refers to the pre-trained layer, among the layers of transfer that have been learned hierarchically.

$$t_p, b_a = \left(I_r^2 + o_x\right) * \sum_{Yi\prime} (L_v + enc) * D_a\left(H_f\right) \quad (9)$$

As shown in Equation (9), the pre-trained model and base model are represented as $t_p \; and \; b_a$, respectively, and the security level is symbolized as L_v. This model progresses on the encryption and recommendation of handoff $L_v\left(enc + H_f\right) * D_a$. This transfers the data to the nearby vehicle for security level assessments.

Transfer layer and fine-tuning: This defines the vehicle's existing data and is followed by the next layer containing the pre-trained model. The fine-tuning requires re-training particular information if adversaries or misinterpretations are identified during the exchange. Based on these models, the pre-trained mechanism is evaluated based on the desired handoff and security process.

$$A_0, U_g = \sum_{h_0}^{h_n} L_v + \left(n' * x_h\right) + \left(k_p * dec\right) + D_a$$

This is computed as follows:

$$Yi'(x_h) = \left(n' + n_v\right) * \sum_{enc} M_k * (A_1 * p_t)$$

The formulation is followed up as follows:

$$M_k(n_v) = \prod_{A_1} D_a * \{(k_p - i_m) + L_v\},\ for\ all\ D_a \in x_h \quad (10)$$

As inferred in Equation (10), the transfer layer and fine-tuning works on transfer learning to address the adversary and misinterpretation, which are labelled as $A_0\ and\ U_g$, respectively. The security level is maintained for the handoff, with recommendations. The next layer is processed using the pre-trained model, where RSU transports the information to the nearby vehicle. The decryption is followed up with the security level for the vehicle-to-vehicle transfer, $L_v + (n' * x_h) + (k_p * dec)$. The transfer learning evaluates the security level with the handoff process, in which mutual key authentication is followed up. From this evaluation step, the security level analysis of four parameters in transfer learning is completed with the key authentication formulated below.

$$L_v = (A_0 + \ldots + A_n) * \prod_{t_p} (i_m + I_r) - H_f,\ for\ all\ H_f \in t_p$$

This means,

$$M_k(L_v) = enc \leftarrow dec(A_0 * p_t) - k_p(\alpha + F_d)$$

Therefore,

$$F_d(h_n, x_h) = \prod_{A_0}^{A_1} n'(enc * pr_0) * o_x - f_w \quad (11)$$

As found in Equation (11), the security level is maintained using the learning administered using the key authentication with encryption and decryption. Here, A_1 is the next layer in the transfer process, and, from this case, defines the traffic flow $f_w + R'(z_p * L_v) < D_a$. As a condition of the handoff process, a re-handoff is performed if the security level is lower. The dodged transfer learning functions are illustrated in Figure 7.

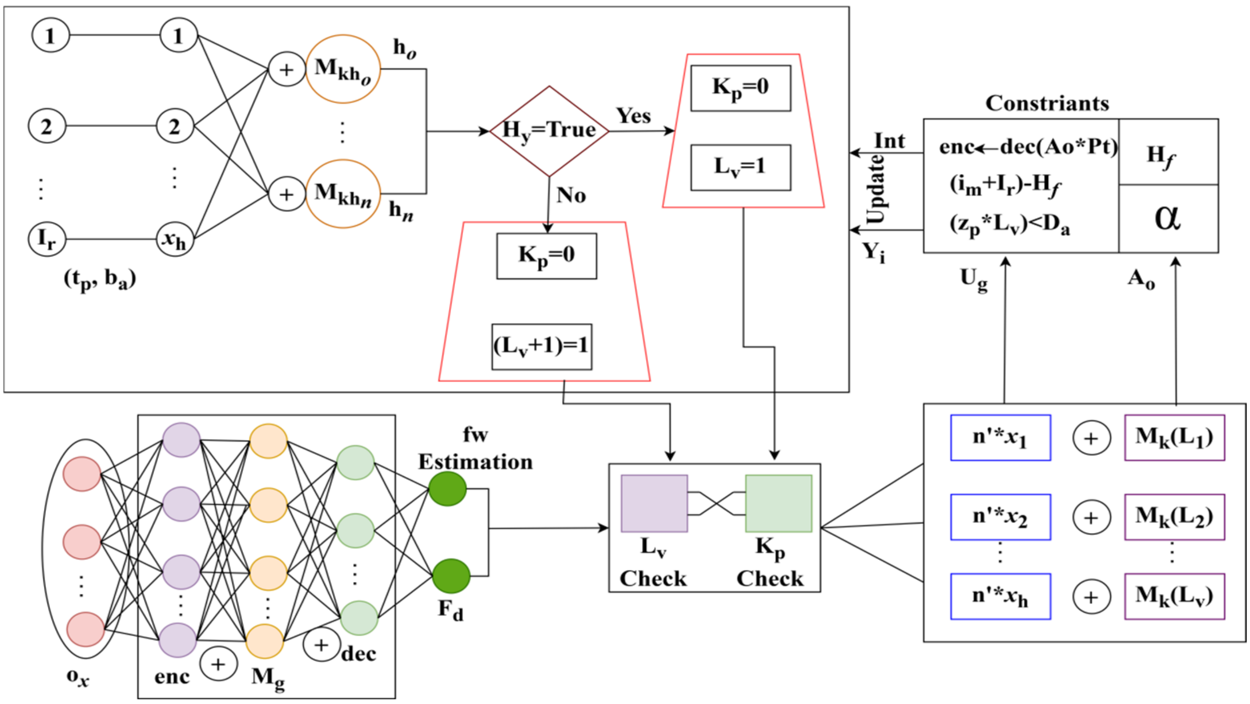

Figure 7. Dodged Transfer Learning Functions for Security Level Estimation.

The $(t_b,\ b_a)$ is the pre-trained model that differentiates $(L_v = 1 = L_v + 1)$ for $k_p = 0$ for (I_r, x_h) combination. The combination verifies $h_y = true/\text{false}$ to differentiate L_v and $(L_v + 1)$ for different o_x intervals. Then, the transfer layer is consented with, $(enc \bigoplus M_g \bigoplus dec)$, provided that f_w or F_d is the output. This layer is responsible for (A_o, U_g) differentiation by inhering L_v and k_p. The tuning for $(L_v + 1)$ or L_v based on k_p using new H_y (or) $Y_i(x_h)\forall\ enc$ satisfies H_y with the same L_v, based on *dec* (Figure 7). Based on the above learning, the loss observed during H_y for different variants is analyzed in Figure 8.

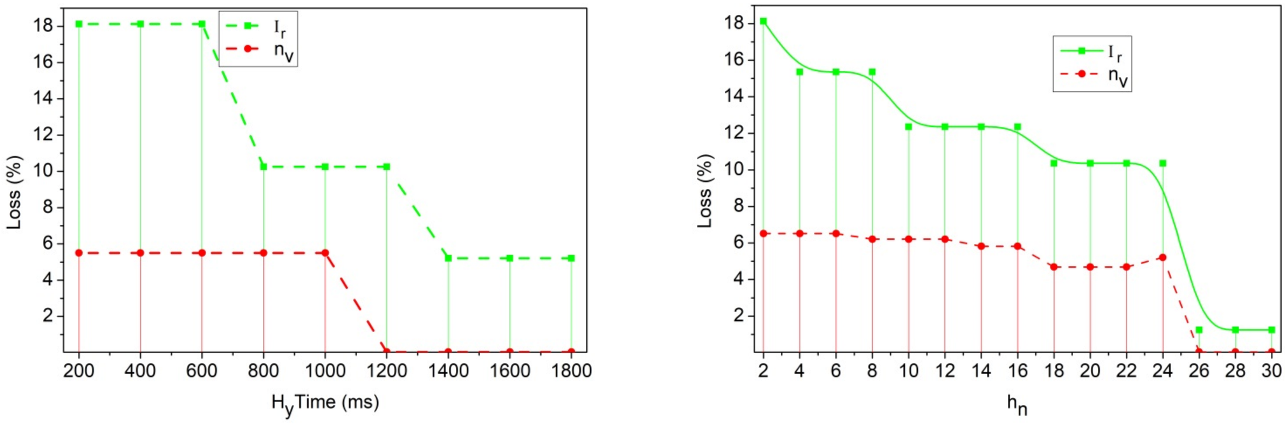

Figure 8. Communication loss assessment for vehicles.

The communication loss is reduced if the traffic flow is detected using RSU. In this examination step, the misinterpretation is identified and prevents the adversaries from accessing the information $n'(o_x + x_h)$. On this basis, communication loss is based on the transportation of information to the vehicle, where the pre-trained model is used to envelope the transfer layer in order to process the secure communication $p_t(o_x * F_d) + f_w$. The loss is addressed, leading to the termination of data exchange if the security degrades, so in this case, communication loss decreases (Figure 8). This addresses the interpretation of traffic-related data communication.

$$R_f = H_f + \sum\nolimits_{pr_0} (A_1 * x_h) - dec\left(n' - i_m\right) + I_r(o_x),\ for\ all\ i_m \in D_a$$

Similarly,

$$= H_f + \sum\nolimits_{o_x} I_r * (z_p + L_v) \leftarrow dec(M_k)pr_0 - (p_k - \alpha),\ where\ pr_0 \in o_x$$

Therefore,

$$= (o_x * pr_0) + \sum\nolimits_{z_p} L_v * \left(i_m - k_p\right) + D' * U_g,\ for\ all\ U_g \in A_0 \quad (12)$$

As shown in Equation (12), the communication is achieved from one vehicle to another vehicle and follows the transfer layer with fine-tuning, the re-handoff is labelled as R_f. The process is undertaken with the interaction among the vehicles, where the misinterpretation and congestion are decreased, $(i_m + \alpha) < pr_0$, where $L_v \in R_f$. This case defines the following: if the security level is lower, a re-handoff is recommended. Thus, optimization is undertaken for the security level observation with the decryption process, and is expressed as $(z_p + L_v) \leftarrow dec(M_k)pr_0$. This learning aids the probabilistic detection of security breaches and ensures robust PS for traffic and location information exchange. The PS-based privacy is modified using different handoff authentication levels dictated by mutual lightweight key exchange, reducing adversary control. The R_f analysis for different h_n and o_x is analyzed using Figure 9.

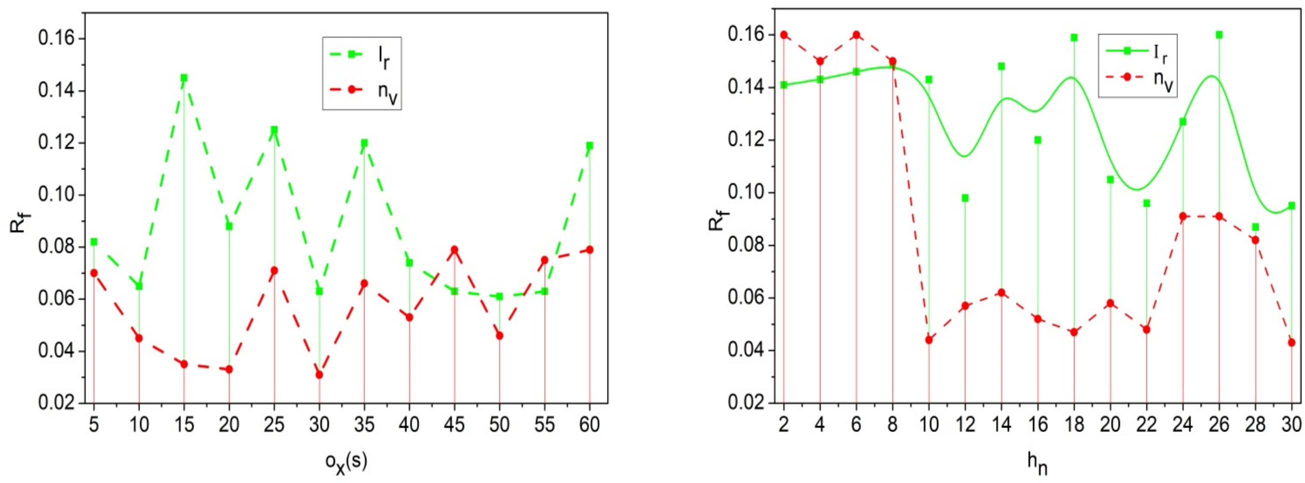

Figure 9. Re-handoff analysis for different vehicles and communication.

The re-handoff rate decreases for the recommendation method for security level. If the security level decreases, then the handoff takes the role of performing the traffic flow, and the re-handoff then works according to $L_v\left(R_f \leftarrow H_f\right) - R'$. This is processed with the recommendation method with which the vehicle navigates the particular road, $n_v(h_0 \rightarrow h_1) * pr_0\left(M_g\right)$. This step illustrates the re-handoff based on the decreased security level and validates the communication with mutual authentication (Figure 9).

4. Discussion

The discussion section presents the proposed method comparisons with the existing CACMTM and PMM methods. The metrics computation overhead and security depletion metrics are analyzed in tabulation format. The proposed method is simulated using VANSIM considering 30 vehicles in a road segment with a 10 km distance. This road segment contains five, three, and two intersections for four, three and two crossroads. The road segment comprises five four-leg intersections, three T-intersections, and two two-way crossings. The five four-leg intersections are standard crossroads, where two roads intersect, each having traffic flows from all four directions. The three T-intersections involve one main road intersecting with a side road, forming a 'T' shape, where traffic from the side road must yield or stop. The two-way crossings are simpler junctions where two roads intersect, but where each road has traffic flowing in only two directions, often requiring fewer traffic control measures. The vehicle density is 30 vehicles per hour, and the speed varies between 20 km/hr and 60 km/hr. A vehicle is allocated 10 to 60 s of interacting time with the RSU, and the maximum RSU deployed in 8 can cover a 500 m radius. The authentication follows a 256-bit encryption key using HECC with temporal characteristics. The minimum handoff time is 180 ms, and the maximum handoff is 320 ms. The re-handoff is to be performed between 60 ms and 210 ms to prevent failure. Based on this simulation setup, the computation overhead for H_f and R_f is tabulated in Table 2. The variants are vehicle count = 10, 20, and 30 and o_x = 20 s, 40 s, and 60 s.

Table 2. Computation overhead assessment.

	H_f Overhead			R_f Overhead		
Vehicles	**10**	**20**	**30**	**10**	**20**	**30**
CACMTM [25]	45.25	48.36	51.06	38.69	37.36	39.47
PMM [26]	41.56	45.36	42.36	32.14	38.69	32.36
RPP-PS	25.485	25.361	26.472	22.474	24.365	27.541
o_x	**20 s**	**40 s**	**60 s**	**20 s**	**40 s**	**60 s**
CACMTM [25]	48.69	48.36	51.04	48.25	45.36	47.47
PMM [26]	32.145	35.69	39.6	29.36	31.23	28.78
RPP-PS	24.892	24.987	25.478	27.417	24.369	25.496

The computation overhead is reduced even as it addresses the congestion and packet losses that lead to the termination of data transportation in smart cities. This illustrates the data exchange process and defines the re-handoff for interaction purposes, $o_x(n') + R_f * h_n$. The interaction takes place among the vehicles, seeks the traffic flow and defines the mutual key authentication $(f_w + F_d) * o_x$. The key authentication plays a role in providing access to the secured vehicle in order to reduce the computation overheads (Table 2). Following this analysis, the security depletion of the proposed method is comparatively analyzed with the existing methods, and the values are presented in Table 3. The vehicles range from 5 to 30 for security depletion, and the communication/interaction time is from 10 to 60 s.

Table 3. Comparative assessment of security depletion.

	Depletion					
Vehicles	**5**	**10**	**15**	**20**	**25**	**30**
CACMTM [25]	0.1558	0.1574	0.1589	0.1574	0.1561	0.1548
PMM [26]	0.1547	0.1536	0.1525	0.1564	0.1512	0.1498
RPP-PS	0.1467	0.1485	0.1477	0.1487	0.1489	0.1491
o_x	**10 s**	**20 s**	**30 s**	**40 s**	**50 s**	**60 s**
CACMTM [25]	0.1587	0.1571	0.1569	0.1517	0.1523	0.1544
PMM [26]	0.1541	0.1532	0.1521	0.1518	0.1511	0.1489
RPP-PS	0.1471	0.1463	0.1481	0.1496	0.1478	0.1467

The security depletion is less for vehicles where the handoff mechanism works with the knowledge of the congestion and communication losses $L_v(\alpha + k_p) \rightarrow h_1$. Both the congestion and packet losses are addressed, as is the security. The security level is benchmarked for the vehicle and communicates with nearby vehicles with authentication, $M_k(enc(n') \rightarrow dec(h_1)$. The authentication relates to the encryption and decryption process and reduces security depletion (Table 3).

Real-time decision-making, the smooth functioning of autonomous vehicles or traffic management systems, and faster data processing are all made possible by a small decrease in computing time for the RPP-PS approach. In the same way, a small security improvement may have a major effect on the system's resilience, making it less vulnerable to data breaches and other security issues. In addition to improving the user experience and system efficiency, these enhancements might also help ensure the long-term viability of an ITS, which is especially important given the increasing number of connected cars and devices. Although the performance advantages of the suggested solution are quantitatively small, they might significantly affect the overall responsiveness, scalability, and security of ITS systems.

5. Conclusions

This article introduced a novel resilient privacy-preserving method with Presumed secrecy for an ITS in smart cities. Presumed secrecy is achieved by reducing re-handoff rates through the maximum possible privacy assessments. Dodged transfer learning is used and the model differs from a conventional ITS process by retaining the previous state until the switchover. After this switchover, mobility, localization, and privacy retention are ensured throughout the driving distance. The lightweight authentication with encryption and decryption concurrency minimizes re-handoffs due to privacy failures. Furthermore, the communication loss for the high interaction intervals defines the security depletion across various dodging processes that maximize the privacy assessment. The proposed method is analyzed using extensive simulation and validated using appropriate parameters and comparative analysis. Presumed secrecy is achieved through privacy assessment. Security administration contains less validation during the intervals. This is observed due to the maximum concurrent access to the roadside units and privacy assessments. Therefore, the assessment interval is less than that of conventional assessment. To address this issue, backwards and forward secrecy with interaction weights will be used and added in the future. This type of interaction improves the privacy level verification across various handoff and re-handoff intervals with unanimous assessments. Compared with existing methods, the proposed approach decreases security depletion rates by 15% across varying traffic densities, underscoring ITS resilience in high-interaction scenarios.

Author Contributions: Conceptualization, P.M.; methodology, M.D.A., M.A., G.A., T.M.A., K.K. and G.E.; validation, G.E.; formal analysis, M.A., G.A. and K.K.; investigation, M.D.A., M.A., T.M.A., P.M. and G.E.; data curation, M.D.A., G.A. and K.K.; writing–original draft, M.D.A., M.A., G.A. and T.M.A.; supervision, G.A. and P.M.; project administration, P.M.; funding acquisition, P.M. and G.E. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. DGSSR-2024-02-01229.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Costantino, G.; De Vincenzi, M.; Martinelli, F.; Matteucci, I. A privacy-preserving solution for intelligent transportation systems: Private driver DNA. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 258–273. [CrossRef]
2. Miao, Y.; Yang, Y.; Li, X.; Choo, K.K.R.; Meng, X.; Deng, R.H. Comprehensive Survey on Privacy-Preserving Spatial Data Query in Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 13603–13616. [CrossRef]
3. Tang, L.; He, M.; Xiong, L.; Xiong, N.; Luo, Q. An efficient and privacy-preserving query scheme in intelligent transportation systems. *Inf. Sci.* **2023**, *647*, 119448. [CrossRef]
4. Pal, K.; Shakshuki, E. Supply chain transport management, use of electric vehicles, review of security and privacy for cyber-physical transportation ecosystem and related solutions. *Procedia Comput. Sci.* **2024**, *238*, 135–142. [CrossRef]
5. Wang, X.; Garg, S.; Lin, H.; Kaddoum, G.; Hu, J.; Hassan, M.M. Heterogeneous blockchain and AI-driven hierarchical trust evaluation for 5G-enabled intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2074–2083. [CrossRef]
6. Feng, X.; Wu, J.; Bashir, A.K.; Li, J.; Shen, A.; Alshehri, M.D. Vulnerability-aware task scheduling for edge intelligence empowered trajectory analysis in intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 4661–4670. [CrossRef]

7. Yan, K.; Ma, W.; Yang, Q.; Sun, S.; Wang, W. Info-Chain: Reputation-Based Blockchain for Secure Information Sharing in 6G Intelligent Transportation Systems. *IEEE Internet Things J.* **2023**, *11*, 9198–9212. [CrossRef]
8. He, X.; Wang, J.; Liu, J.; Ding, W.; Han, Z.; Wang, B.; Nebhen, J.; Wang, W. DNS rebinding threat modeling and security analysis for local area network of maritime transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2643–2655. [CrossRef]
9. Yamany, W.; Moustafa, N.; Turnbull, B. OQFL: An optimized quantum-based federated learning framework for defending against adversarial attacks in intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 893–903. [CrossRef]
10. Liu, P.; Shen, J.; Zhang, P. Multi-attribute group decision-making method using single-valued neutrosophic credibility numbers with the Dombi extended power aggregation operator and its application in intelligent transportation system data collection scheme selection. *Eng. Appl. Artif. Intell.* **2024**, *133*, 108639. [CrossRef]
11. Carbo, J.; Pedraza, J.; Molina, J.M. Agents preserving privacy on intelligent transportation systems according to EU law. *Artif. Intell. Law* **2024**, 1–34. [CrossRef]
12. Munawar, A.; Piantanakulchai, M. A collaborative privacy-preserving approach for passenger demand forecasting of autonomous taxis empowered by federated learning in smart cities. *Sci. Rep.* **2024**, *14*, 2046. [CrossRef] [PubMed]
13. Cai, K.; Yu, Z. Research on the antecedents of data privacy concern toward intelligent connected vehicles. *Int. J. Hum.-Comput. Interact.* **2024**, 1–14. [CrossRef]
14. Kabil, A.; Aslan, H.; Azer, M.A.; Rasslan, M. CHAM-CLAS: A Certificateless Aggregate Signature Scheme with Chameleon Hashing-Based Identity Authentication for VANETs. *Cryptography* **2024**, *8*, 43. [CrossRef]
15. Wang, S.; Fan, Z.; Su, Y.; Zheng, B.; Liu, Z.; Dai, Y. A Lightweight, Efficient, and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks. *Electronics* **2024**, *13*, 1418. [CrossRef]
16. Kaleem, S.; Sohail, A.; Tariq, M.U.; Asim, M. An improved big data analytics architecture using federated learning for IoT-enabled urban intelligent transportation systems. *Sustainability* **2023**, *15*, 15333. [CrossRef]
17. Latif, R.M.A.; Jamil, M.; He, J.; Farhan, M. A novel authentication and communication protocol for urban traffic monitoring in VANETs based on cluster management. *Systems* **2023**, *11*, 322. [CrossRef]
18. Wu, Z.; Zhuang, Y.; Zhou, S.; Xu, S.; Yu, P.; Du, J.; Luo, X.; Abbas, G. Bi-Level Planning of Multi-Functional Vehicle Charging Stations Considering Land Use Types. *Energies* **2020**, *13*, 1283. [CrossRef]
19. Zhou, Y.; Tan, H.; Iroshan, K.C.A.A. A secure authentication and key agreement scheme with dynamic management for vehicular networks. *Connect. Sci.* **2023**, *35*, 2176825. [CrossRef]
20. Qureshi, K.N.; Jeon, G.; Hassan, M.M.; Hassan, M.R.; Kaur, K. Blockchain-based privacy-preserving authentication model intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 7435–7443. [CrossRef]
21. Chen, C.; Hu, X.; Li, Y.; Tang, Q. Optimization of Privacy Budget Allocation in Differential Privacy-Based Public Transit Trajectory Data Publishing for Smart Mobility Applications. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 15158–15168. [CrossRef]
22. Gao, H.; Huang, W.; Liu, T.; Yin, Y.; Li, Y. PPO2: Location privacy-oriented task offloading to edge computing using reinforcement learning for intelligent autonomous transport systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 7599–7612. [CrossRef]
23. Li, Z.; Wang, H.; Xu, G.; Jolfaei, A.; Zheng, X.; Su, C.; Zhang, W. Privacy-preserving distributed transfer learning and its application in intelligent transportation. *IEEE Trans. Intell. Transp. Syst.* **2022**, *25*, 2253–2269. [CrossRef]
24. Saleem, M.A.; Li, X.; Mahmood, K.; Shamshad, S.; Ayub, M.F.; Bashir, A.K.; Omar, M. Provably secure conditional-privacy access control protocol for intelligent customers-centric communication in vanet. *IEEE Trans. Consum. Electron.* **2023**, *70*, 1747–1756. [CrossRef]
25. Din, I.U.; Awan, K.A.; Almogren, A. Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems. *IEEE Access* **2023**, *11*, 65407–65417. [CrossRef]
26. Zhu, Y.; Liu, C.; Chen, C.; Lyu, X.; Chen, Z.; Wang, B.; Hu, F.; Li, H.; Dai, J.; Cai, B.; et al. Privacy-Preserving Large-Scale AI Models for Intelligent Railway Transportation Systems: Hierarchical Poisoning Attacks and Defenses in Federated Learning. *Comput. Model. Eng. Sci.* **2024**, *141*, 1305–1325. [CrossRef]
27. Qu, Z.; Tang, Y.; Muhammad, G.; Tiwari, P. Privacy protection in intelligent vehicle networking: A novel federated learning algorithm based on information fusion. *Inf. Fusion* **2023**, *98*, 101824. [CrossRef]
28. Jiang, S.; Cao, J.; Wu, H.; Chen, K.; Liu, X. Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems. *Inf. Sci.* **2023**, *635*, 72–85. [CrossRef]
29. Zuo, K.; Chu, X.; Hu, P.; Ni, T.; Jin, T.; Chen, F.; Shen, Z. Security enhanced privacy-preserving data aggregation scheme for intelligent transportation system. *J. Supercomput.* **2024**, *80*, 13754–13781. [CrossRef]
30. Fan, L.; Zeng, C.; Meng, Z.; Xia, X.; Liu, Y.; Ma, J.; Wang, F.Y. A secured vehicle brain: DAO-based collaborative perception and decision-making systems for intelligent vehicles in CPSS. *IEEE Trans. Intell. Veh.* **2023**, *9*, 52–54. [CrossRef]
31. Zhu, R.; Li, M.; Yin, J.; Sun, L.; Liu, H. Enhanced federated learning for edge data security in intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 13396–13408. [CrossRef]
32. Gupta, B.B.; Gaurav, A.; Marín, E.C.; Alhalabi, W. Novel graph-based machine learning technique to secure smart vehicles in intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 8483–8491. [CrossRef]

33. Zhang, J.; Ying, R.; Cui, J.; Zhong, H.; Bolodurina, I.; He, D. Secure and Efficient User-Centric V2C Communication for Intelligent Cyber-Physical Transportation System. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 7674–7689. [CrossRef]
34. Sun, Y.; Yu, K.; Bashir, A.K.; Liao, X. Bl-IEA: A bit-level image encryption algorithm for cognitive services in intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 1062–1074. [CrossRef]
35. Sun, X.; Dou, H.; Chen, S.; Zhao, H. A Novel Block-chain based secure cross-domain interaction Approach for intelligent transportation systems. *Phys. Commun.* **2024**, *63*, 102223. [CrossRef]
36. Xu, S.; Wang, T.; Sun, A.; Tong, Y.; Ren, Z.; Zhu, R.; Song, H.H. Post-Quantum Anonymous, Traceable and Linkable Authentication Scheme Based on Blockchain for Intelligent Vehicular Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 12108–12119. [CrossRef]
37. Wu, Q.; Wang, W.; Fan, P.; Fan, Q.; Zhu, H.; Letaief, K.B. Cooperative edge caching based on elastic federated and multi-agent deep reinforcement learning in next-generation networks. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 4179–4196. [CrossRef]