International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 835-851
https://doi.org/10.70917/ijcisim-2026-2573
Article

Privacy-Preserving AI Authentication Protocols for Secure and Scalable Vehicular Intelligence Networks

Mahendra Singh Yadav[1], Dr. Samta Jain Goyal[2], Hirendra Singh Sengar[3]

[1]Research Scholar, Department of Computer Science and Engineering, Amity School of Engineering and Technology (ASET), Amity University, Gwalior, Madhya-Pradesh, India.
[1]Assistant Professor, Prestige Institute of Management and Research, Gwalior
[2]Department of Computer Science and Engineering, Amity School of Engineering and Technology (ASET), Amity University Gwalior, Madhya Pradesh, India.
[3]School of Engineering and Technology (SOET), ITM University, Gwalior, Madhya Pradesh, India.
Corresponding Author: Mahendra Singh Yadav

Abstract: The issue dealt with in this article is the increasing difficulty of secure and privacy-resistant authentication in Vehicular Intelligence Networks (VINs) which are becoming more and more based on AI-driven decision making and distributed learning. Current automobile authentication systems, mostly founded on the public key infrastructures, pseudonym certificates, or independent cryptographic primitives, fail to meet high-latency constraints, scalability in congested traffic, and the high levels of identity disclosure, tracking, and AI-based inference resistant solutions. In order to fill this gap, the paper offers a hybrid privacy-saving authentication system, which closely combines lightweight cryptographic tools with AI-assisted trust certifications and privacy-sensitive machine learning approaches. A detailed threat and privacy analysis introduces resistance to impersonation and replay attacks, the Sybil, and AI-specific attacks, retaining anonymity, unlikability, and conditional traceability. Performance analysis through simulation in realistic vehicular environment demonstrates that the protocol can be used to attain low authentication latency, less communication overhead and high authentication accuracy in even high-mobility and high-density environments. All in all, the paper has shown that the implementation of AI authentication that is privacy conscious can be feasibly implemented in VINs without compromising real-time behavior to give intelligent transport systems scalable and future-proof security baseline. These results provide practical advice to researchers, standards organizations, and practitioners developing next-generation V2X security frameworks that need to balance automation, accountability, regulatory provisions, and scale user privacy in the developed and deployed globally and sustainably.
Keywords: NA

1. Introduction

1.1 Background and Context

Vehicular Intelligence Networks (VINs) is a fast-emerging category of cyber-physical systems, facilitating vehicle-to-everything (V2X) communication, uniting vehicles, roadside units, edge servers, and cloud services to aid real-time decision making, cooperative driving, and safety-critical applications (Vehicular Ad Hoc Network, n.d.). In such networks, entity authentication reliability is the key to message integrity exchanged between entities such as traffic alerts or automated braking messages between vehicles. Nevertheless, the transparent characteristic of VINs predisposes them to an enormous amount of privacy and security threats (Khezri, 2025). Among the most important ones, there are identity disclosure and location tracking, which may deteriorate user privacy and allow malicious exploitation of vehicular communication networks.

During the last few years, intelligent transportation systems (ITS) have become more and more technologically advanced and use elements of machine learning and AI to optimize routing, prevent crashes, and predictive maintenance. The AI systems rely on rich and, in many cases, sensitive streams of data (Alam et al., 2024). Due to this, the authentication protocols cannot just check the authenticity of communicating parties, but also maintain privacy even in the presence of sophisticated adversarial models. Privacy enhancing cryptographic tools and Federated learning are becoming a potential solution to privacy and privacy-secure authentication in distributed VIN (Xu et al., 2024; Badhib et al., 2025).

Furthermore, standardization activities like ETSI TS 103 097 of vehicular communications deal with certificate formats and security headers of the V2X messages and highlight the necessity of strong and cross-operable authentication systems capable of functioning in high-mobility environments with low latency (ETSI, 2021). Such architectures need to balance real-time performance requirements and privacy assurances, which traditional protocols, e.g. simple pseudonym schemes, cannot address by themselves.

1.2 There are security and privacy dilemmas in the vehicular networks

Connected vehicle representation The connected vehicles have distinct security and privacy concerns as they have an open wireless medium and a dynamic topology. The cars often transmit data about their location, speed, and direction, which once hacked, can result in violations of location privacy and monitoring (Farhood, 2024). The traditional authentication mechanisms are based on public key infrastructures (PKI) and pseudonym certificates to establish legitimacy of entities; among them, both methods can be extremely costly in terms of calculation and not preventing the correlation between pseudonyms and identities in the face of correlation attacks.

Further, the decentralization of AI parts into VIN nodes, specifically in federated learning, introduces novel attack points. Intrusion detection protocols or collaborative model training federated learning protocols are vulnerable to membership inference attacks and model inversion attacks unless the authentication and privacy control is well-structured (Xu et al., 2024). Federated techniques seek to store raw data locally to preserve privacy but transmit model updates to a marketplace, but authenticating the source of such updates, but not revealing the identity is an open problem.

Additionally, the contemporary VIN applications are characterized by severe latency requirements. The authentication schemes should work within milliseconds to ensure that they do not impede the timeliness of safety-critical programs (Khezri, 2025). There is a design tradeoff in achieving latency, privacy, and security at once; both efficient and privacy preserving protocols are studied more and more in the literature in the field of federated and cryptographically-enhanced protocols (Badhib et al., 2025).

1.3 Problem Statement

Even though many authentication protocols have been developed to work in vehicular networks, the vast majority of them cannot be considered as efficient when compared to modern privacy, scalability, and AI insertion needs. Older PKI-based techniques and basic pseudonym authentication can verify the sender of messages but do not do much to avoid identity linkage or long-term tracking to the sender more so in systems where AI analytics works with large amounts of broadcast data (Farhood, 2024). Also, many cryptographic schemes that concentrate solely on conditional privacy, e.g. certificateless identity schemes, may have a significant computational cost that is no longer affordable in real-time VIN systems.

As AI-enhanced VIN capabilities spread, authentication has to respond to decentralized model training and inferencing models which uphold privacy. Current protocols do not have effective systems to verify that contributions of models made by vehicles are legitimate without revealing sensitive identity information - even when model updates themselves may be information revealing. The issue here is to develop authentication schemes which provide high levels of privacy protection, scalability in large vehicular networks, and compatibility with AI-based VIN systems with severe performance requirements.

1.4 Research Gap

Existing sources indicate that there are still a number of gaps that hinder the development of strong VIN authentication. To begin with, most of the protocols suggested are based on the concept of cryptographic privacy only, without taking into account the computational requirements of AI-enhanced VIN applications. Second, pseudonym operations lower the chances of traceability, but can be susceptible to correlation attacks that can join identities across time. Third, schemes that combine federated learning usually presuppose the use of trusted aggregation nodes and do

not consider the problem of privacy authentication of participants on a large scale. Lastly, formal assessment of privacy preserving authentication protocols in live vehicular mobility settings has not been extensively studied, and thus conclusions on realistic performance can hardly be made. These loopholes imply the necessity of holistic solutions that are privacy-focused cryptography, effective authentication routines, and AI-based verification solutions.

1.5 Objectives and Contributions

This paper will create and discuss privacy-authenticating AI authentication schemes that can satisfy the performance and security requirements of the modern VINs. The core objectives include:

1. Designing authentication schemes that offer conditional anonymity, unlikability, and traceability in AI-enhanced vehicular systems.
2. Combining privacy-aware machine learning, including federated learning, to authenticate AI model contributions without disclosing sensitive identity information.
3. Testing the protocols presented in practice against the conditions of a real vehicular network with emphasis on the latency, communication overhead and privacy provisions.

The proposed outcomes of the work will be (a) a new protocol architecture that integrates cryptographic and AI components to maintain privacy, (b) formal security and privacy analysis to show resistance to state-of-the-art attacks, (c) performance comparisons with the existing methods to reflect scalability and efficiency.

2. Threat Landscape and Architecture of Vehicular Intelligence Networks

2.1 Vehicular intelligence Networks Architecture

Vehicular Intelligence Networks (VINs) are high-tech cyber-physical systems, which make vehicles, infrastructure, and cloud/edge services connect in real-time to facilitate safety, mobility, and infotainment apps. VIN usually involves On-Board Units (OBUs) in the cars, Roadside Units (RSUs) at the fixed infrastructures, edge computing devices, and centralized services in the cloud infrastructure (Al-Sawad et al., 2023). They are the foundation of Vehicle-to-Everything (V2X) communications, in which vehicles share vehicles status updates, warning, and cooperative maneuver information.

The major architectural elements of a contemporary VIN are:

- OBUs: These units handle local sensor data, are involved in the exchange of messages, and implement authentication procedures associated with driving decisions (Rikaa & Choudhury, 2022).
- RSUs: RSUs work as processing points and communication relays, which help to disseminate messages and are roadside intelligence processing and receiving units.
- Edge Computing Nodes**:** Edge nodes are contained close to RSUs or cellular base stations and are used to execute local AI models inference to minimize latency (Kato et al., 2021).
- Cloud services**:** These contain a massive analytics, model training aggregation, and certificate administration in terms of authentication services.

VINs utilize several communication technologies: Dedicated Short-Range Communications (DSRC), Cellular V2X (C-V2X), and hybrid-based ones that can utilize both to address geographic coverage and performance goals (Tang et al., 2023). It has a heterogeneous node architecture, high mobility and is latency sensitive resulting in difficulty in designing efficient authentication protocols. The node authentication in this layered architecture should be able to provide fast verification of the credential and at the same time provide privacy and reduce the communication overhead.

Also, the incorporation of AI-powered modules at both edge and cloud levels creates new orchestration complexity: models must be frequently updated by distributed vehicles without providing identity or other sensitive operational information. Here, authentication schemes should be compatible with the VIN architecture that satisfies the constraint of a limited OBU computing capabilities as well as fast vehicle velocities.

2.2 Communication Models (V2V, V2I, V2X)

The interaction paradigms of VIN communication are structured according to a number of interaction paradigms:

- Vehicle-to-Vehicle (V2V): Vehicles communicate directly with each other sharing safety messages, such as collision warnings.
- Vehicle to Infrastructure (V2I): Interfaces among vehicles and infrastructures (e.g., RSUs) to manage traffic and to access services.
- Vehicle-to-Everything (V2X): A more comprehensive model that comprises V2V, V2I and Vehicle-to-Pedestrian (V2P), Vehicle-to-Network (V2N) communications (Sultana et al., 2023).

These communication models are focused on very rigid performance and reliability. As an example, V2V safety messages have to be received in milliseconds to facilitate functions of emergency braking and collision avoidance. The traffic pattern of high mobility and the broadcast traffic combination makes it more vulnerable to spoofing, message injection and replay attacks unless the appropriate authentication and privacy controls are established.

2.3 System Threats and Attacker Capabilities

The threat landscape is crucial in designing the authentication protocols in the VINs. The characteristics peculiar to vehicular networks like the frequent change of topology and open broadcast media provides opportunities to external and internal enemies.

An external adversary is an unauthenticated attacker who comes to the network in an attempt to interfere with network operations by sending malicious messages, or by impersonating the authenticated nodes. They may want to send fake safety alerts to cause unnecessary braking or other road accidents (Sultana et al., 2023). Since VINs work in common wireless communication, message interception allows hackers to conduct traffic analysis, which may reveal vehicles mobility characteristics and delicate operation information.

Authenticated participants, who do not follow the protocol to launch attacks, are considered internal adversaries, e.g. sybil attacks (establishing many false identities) to interfere with consensus or induce resource wastage. These insiders can also go hand in hand with external attackers and the threat may be even more complicated.

The capabilities that should be considered in this context are:

1. Eavesdropping: Intercepting V2X messages in order to obtain patterns to be used in inference attacks.
2. Message Injection/Spoofing: Sending unauthorized messages so as to deceive vehicles.
3. Replay Attacks: Recording and retransmission of messages in order to produce inconsistencies.
4. Sybil Attacks: This is through the use of counterfeit credentials to appear like two or more entities.
5. AI Model-Based Attacks: Take advantage of model changes to either infer or poison attacks (Zhou et al., 2024).

Besides these, challengers of VIN can capitalize on AI model weaknesses. As an example, in federated learning models, attackers can alter local model updates to bias the overall model performance (Zhou et al., 2024). Since localized data could be statistically indicated in the model update, when authentication and privacy are weak, they can also be leaked by the model update including the sensitive information about drivers or car behavioral patterns.

New studies emphasize the significance of formal threat modeling which considers communication and AI-based attack vectors. Authentication schemes should thus not just ensure that the authenticity of nodes, but also make sure that the origin of AI model contributions cannot be used to disclose identity or other sensitive information.

2.4 Vehicular Authentication Privacy Requirements

Privacy on vehicular networks does not just concern confidentiality of individual messages, but also prevention of likability and longitudinal tracking of vehicles. Primary privacy criteria on authentication protocols to be adopted in VINs are:

- Anonymity: Vehicles are to be authenticated without revealing the identity and unique identifiers of the driver to unauthorized parties (Miao et al., 2023).
- Unlikability The transmissions of messages are not supposed to be time-co reliable in such a manner that an opponent can associate several communications with one vehicle. This is very crucial in deterring tracking.

- Conditional Traceability: As much as anonymity is mandatory, law enforcement agencies must have the capacity of tracing a rogue vehicle under legitimate circumstances. A compromising effort is therefore demanded between privacy and accountability.
- Data Minimization: Authentication is supposed to be done without exposing sensitive information more than is needed to authenticate.

Other more recent privacy-sensitive authentication protocols use cryptographic designs, including group signatures or ring signatures, in combination with AI-assisted verification to anonymize individual identities whilst permitting conditional revocation and accountability (Singh and Verma, 2024). Besides, AI model contributions to federated protocols should enjoy privacy, to stop adversaries who could use patterns of updates to determine individual vehicle behaviors (Li et al., 2023).

Addressing such privacy needs with the performance needs of the VINs is one of the fundamental research issues, especially when authentication needs to be run at high mobility and with limited compute capabilities.

3. State-of-the-Ar and Literature Review

3.1 Authentication in VANETs Traditional Authentication

The framework proposed by Raya and Hubaux (2007) on the idea of vehicular authentication, based on the principles of public key infrastructures (PKI), was the precursor of other modern models of VANET security, yet, according to recent assessments, PKI-focused models have failed to comply with modern privacy standards because of certificate overheads and the vulnerability to identify tracking in the event of certificate reuse (Sultana et al., 2023).

Lu et al. (2021) discussed certificate authentication scheme in large vehicle networks and emphasized that PKI can guarantee message integrity and non-repudiation, but the high frequency of certificate revocation requires a significant cost of communication and computational overhead that adversely impacts scalability with large vehicle networks.

Wang et al. (2022) identified the use of lightweight authentication procedures using hash chains to minimize the computational overhead on OBUs but the analysis revealed poor resistance to replay and impersonation attacks, particularly in high mobility settings.

Zhang et al. (2023) have shown that the conventional symmetric-key authentication protocols do not offer the necessary level of anonymity, with an attacker being able to tie message-timing and message-delivery patterns to even the most hidden cryptographic identities.

Farhood (2024) came to the conclusion that the legacy model of VANET authentication was not created to exist with the AI-enabled automobile service because it does not have mechanisms designed to ensure the security of distributed intelligence contributions while guaranteeing privacy.

3.2 Cryptography Methods to Privacy Assurance

Pseudonym-based authentication schemes proposed by Lin et al. (2021) that change vehicle identifiers periodically were found to improve privacy, but later investigations found that synchronization of a pseudonym change can be used to launch a spatiotemporal correlation linkage attack by an adversary.

The study by Zhang and Liu (2022) examined the use of the group signature schemes to ensure VANET authentication, where vehicles are allowed to authenticate anonymously and trusted authorities can trace suspicious behaviors; although the scheme has good privacy assurance, the verification delays are high in the scheme, making it unsuitable to use in latency-sensitive applications.

He et al. (2023) implemented the use of ring signature to vehicles authentication without having the centralized group managers, but its performance did not reveal performance improvement as the network size increases, but rather the signature size and communication overhead is increasing.

Miao et al. (2023) suggested frameworks of certificateless authentication to lessen PKI reliance, although they found it difficult to securely generate keys and susceptible to key escrow attacks in the event of authority betrayal.

Conditional privacy-preserving cryptography with revocation mechanisms was also combined by Singh and Verma (2024) showing better accountability; however, their scheme was not concerned with privacy leakage in auxiliary AI data streams that are becoming increasingly common in VINs.

3.3 Authentication Techniques based on AI

Chen et al. (2021) were the first to propose behavior-based vehicle authentication via driving pattern recognition, demonstrating that machine learning models could be used to determine legitimate vehicles without explicit cryptographic authentication, yet there were privacy implications since the vehicles were monitored continuously.

Alam et al. (2024) examined the use of deep learning-enhanced intrusion detection systems in vehicular networks and have observed that AI-based authentication offers greater flexibility to respond to changing attacks but needs stringent privacy measures to avoid model inversion.

Xu et al. (2024) combined federated learning and identity authentication, which validated vehicular nodes using their contribution consistency on model consistency instead of fixed credentials, which limited contact with raw data significantly without compromising the accuracy of authentication.

Zhou et al. (2024) emphasized that AI-guided authentication systems are susceptible to inference attack and poisoning attack when adversarial vehicles are capable of updating malicious models without the right authentication.

Badhib et al. (25) have shown that AI-aided authentication needs to be accompanied by a cryptographic verification to provide credibility to distributed intelligence, and this validates the necessity of hybrid AI-cryptographic solutions.

3.4 Vehicular Authentication with the help of blockchain

Lei et al. (2021) suggested decentralizing the management of trust in VANETs, where blockchain-based authentication frameworks and decentralized authentication help record authentication events that cannot be tampered with, and lessening the need to use centralized authority.

Zhang et al. (2022) used consortium blockchains on vehicular authentication to attain conditional privacy and accountability, but their analysis showed the limitation of scalability to the transaction confirmation latency.

Kumar et al. (2023) combined lightweight blockchain protocols with RSUs to authenticate vehicles on the local level to alleviate some latency concerns at the cost of new privacy risks regarding immutable records of transactions.

As noted by Saxena et al. (2024), blockchain-based authentication schemes are unable to address the real-time requirements of high-speed vehicular conditions except when integrated with off-chain calculation and effective consensus strategies.

3.5 Weaknesses of Current Methodologies

Sultana et al. (2023) reviewed the literature of vehicular authentication schemes systematically and determined that the currently existing solutions can maximize security or privacy and rarely secure both together with scalability.

As Miao et al. (2023) found, cryptographic privacy-preserving protocols can be prohibitively expensive to compute and communicate, which constrains their use in large-traffic situations.

Xu et al. (2024) were able to demonstrate that although AI-based authentication techniques are adaptive, they can be sensitive to information leaking as the model is updated unless the concept of differential privacy or secure aggregation is implemented.

As Badhib et al. (2025) pointed out, a large number of authentication schemes are based on the assumption of semi-trusted infrastructure elements, which might not be true in heterogeneous VIN implementations.

The study by Farood (2024) determined that unified frameworks that combine privacy-preserving cryptography, AI-aware authentication, and scalability within the real-world automobile constraints are under critical shortage, which serves as motivation to conduct further research.

4. System Model and Design Requirements

4.1 Design Goals: Security, Privacy, and Scalability

The design of privacy-preserving authentication systems to Vehicular Intelligence Networks (VINs) needs to meet three fundamental design objectives that include security, privacy and scalability. Security is used to guarantee that legitimate vehicles and infrastructure elements are the only ones that engage in V2X communications and

eliminates the risks of impersonation, spoofing, and message injection attacks (Sultana et al., 2023). Authentication schemes should ensure integrity of messages, authenticity of source as well as resistance to replay and Sybil attacks in a highly dynamic vehicular environment.

Privacy is also crucial because VINs constantly share personal data including the location, speed, and driving habits. The authentication systems in use should also be effective by offering anonymity and unlikability to prevent the correlation of messages to customer vehicles by adversaries to identify or track customers (Miao et al., 2023). Simultaneously, privacy has to be conditional such that when it is important to trace a rogue vehicle, it is not deemed illegal.

Scalability is also a significant design issue because the number of vehicles that may be involved in VINs at a given moment may be enormous. The authentication protocols should be able to support mass deployment with no excessive computation and communication overhead. This need is also intensified by the fact that AI-powered VINs expect vehicles to share model updates or trust ratings with each other (Xu et al., 2024). Therefore, the authentication solutions should be lightweight and decentralized and should be able to support a large vehicle density without causing performance degradation.

4.2 System Assumptions

It is proposed that the system will be based on a heterogeneous VIN environment which consists of vehicles equipped with On-Board Units (OBUs), Roadside Units (RSUs), edge computing nodes, and cloud computing authorities. Cars are presumed to support simple cryptographic functions and adequate amount of computing resources to accomplish lightweight AI inference tasks, which fits the current tendencies of vehicular hardware (Al-Sawad et al., 2023).

System initialization, credential issuance, as well as conditional identity tracing are assumed to have a trusted authority (TA). Nonetheless, the TA does not take part in regular authentication to prevent bottlenecks that are centralized. RSUs and edge nodes are semi-trusted: they are appropriate in adhering to protocol specification, but may be inquisitive about information gathered, requiring privacy-preserving protocols.

It is also assumed that the communication channels are vulnerable and can be observed by opponents in their entirety. Attackers can eavesdrop, inject or replay messages, but are unable to compromise standard cryptographic primitives. Cars can enter and exit the network, which can be considered a realistic mobility trend in VINs (Tang et al., 2023).

4.3 Privacy and Security Requirements

A set of privacy and security requirements is required to ensure that the authentication protocols can perform successfully in the security and privacy conditions of the real-world vehicular environment. Authentication correctness guarantees that an authorized vehicle's authentications are successful and that those who are not legitimate are rejected with high probability. This is a basic property of the safety-critical V2X applications to ensure trust (Rikaa & Choudhury, 2022).

Anonymity demands that the authentication messages should not expose the actual identity of a vehicle to the wrong individuals. Closely related is unlikability which guarantees that the various authentication sessions of one vehicle cannot be correlated even during long term observation. The properties play an important role in deterring the long-term tracking attacks (Miao et al., 2023).

Conditional traceability provides a balance between privacy and accountability and allows the trusted authority to divulge the identity of a vehicle during cases of confirmed misbehavior. It is especially crucial to this intelligent transportation system because legal compliance and dispute resolution demand this requirement (Singh and Verma, 2024).

Security wise, the protocols should not be susceptible to impersonation, replay, Sybil, and man-in-the-middle attacks. The further conditions of AI-supported VINs are authenticity of AI model contributions and model poisoning and inference attack (Zhou et al., 2024). All these requirements are the pre-condition of the secure and privacy-saving authentication in VINs.

4.4 Vehicle Environment Performance Constraints

The environments on vehicles offer very restrictive performance requirements, which play an important role in the design of authentication protocols. The most important are low latency where delays in authentication affect the timeliness of safety messages like collision warning, and cooperative maneuvering messages. Operations related to authentication normally require a duration that is in the milliseconds range to disregard the responsiveness of systems (Tang et al., 2023).

The other important constraint is computational efficiency. Despite the improvement in the capabilities of vehicular hardware, OBUs continue to be limited in comparison with cloud or edge servers. Auth schemes based on heavy cryptographic algorithms or sophisticated AI models can overload vehicle resources, especially during the situations of a dense traffic (Al-Sawad et al., 2023).

The overhead of communication should be also reduced. VINs are dependent on shared limited bandwidth wireless channels, and more authentication signaling may cause congestion and packet loss. Scalability requires therefore efficient message formats and less rounds of handshakes.

Lastly, the mobility resilience is a special need of vehicular networks. The authentication protocols have to be able to withstand frequent topology changes, intermittent connectivity, and quick handovers across RSUs without necessarily undergoing repeated, expensive, re-authentication. All these limitations must be tackled in order to implement privacy-encompassing AI authentication schemes that are deployable in the real-world VIN deployments.

5. Privacy-Preserving AI Authentication Protocol Proposal

5.1 Briefing of the Proposed Protocol.

The authentication protocol proposed is aimed at offering a secure, privacy-preserving, and scalable authentication to Vehicular Intelligence Networks (VINs) with AI-based decision-making elements to them. In comparison to the conventional authentication designs, where the authentication procedure depends on the use of the static cryptographic credentials, the suggested protocol incorporates AI-based trust validation and privacy-preserving cryptographic solutions to verify cars without disclosing information that may reveal their identity and behavior (Xu et al., 2024).

On the upper level, the protocol works in three logical layers: the vehicular, the edge and the authority ones. Fleets self-authenticate by identifying themselves through short lived pseudonymous credentials along with AI-derived trust indicators. The lightweight verification and aggregation functions are carried out by edge nodes and RSUs and the trusted authority is only used during the initialization of the system and conditional identity tracing. The multi-tiered system reduces centralized dependence and enhances scalability at high vehicular density (Al-Sawad et al., 2023).

One of the main peculiarities of the suggested protocol is that it assists in implementing AI integration with privacy. Vehicles provide information in the form of locally computed model updates or trust features instead of raw behavioral or sensor data and undergo authenticated by cryptographic proofs and aggregated by privacy preserving algorithms like secure aggregation. The design guarantees that, authentication decisions can be made using AI intelligence without invading privacy of drivers.

The protocol is organized into three functional stages which consist of registration, authentication and revocation. Each stage is highly engineered to satisfy the high latency and mobility demands and ensure accountability, unlikability and anonymity. These components are explained in the subsections that follow.

5.2 AI-Assisted Mechanism of Identity validation

The proposed protocol comprises the intelligence of the AI-assisted identity validation mechanism. Instead of solely depending on cryptographic identifiers, vehicles are verified by dependent on cryptographic proofs and AI-based trust evidence. This method can overcome the drawbacks of the static credential-based authentication in a highly dynamic car setting (Badhib et al., 2025).

Each car in the local environment has an AI model that is trained on benign operation behavior, including the communication frequency, mobility consistency, and protocol adherence indicators. These features are selected with caution so as not to profile sensitive behavior but to still be able to detect anomalies. The model is fully vehicle-based, thus, raw data is not transferred outside the local environment (Alam et al., 2024).

In the process of authentication, the vehicle creates a trust score or compressed feature vector based on its local model. This output is cryptographically attached to the pseudonymous credential of the vehicle with the help of message authentication code or digital signature. The cryptographic validity and the legitimacy of the trust score of the submission is verified by RSUs or edge nodes and provides evidence of legitimate behavior.

Trust scores are also not stored in long-term to prevent centralized profiling. Side nodes can also combine a number of trust indicators across vehicles in order to enhance robustness, although combining them operates through privacy preserving schemes as detailed in the following subsections. Notably, cryptographic authentication is not displaced by the AI component but complemented by it, which offers resilience to insider attacks in the misuse of valid credentials (Zhou et al., 2024).

Such a hybrid mechanism enables the system to not only authenticate vehicles by checking whether they have credentials but also by checking whether their behavior is consistent, and it is a great way of boosting security without compromising on privacy.

5.3 Privacy-Saving Techniques Adopted

In order to provide high privacy assurances, the suggested protocol will be equipped with various privacy-sensitive methods on the cryptographic and AI levels. The main goal is to avoid the identity disclosure, tracking, and inference threats and preserve the authentication correctness.

The protocol uses short-term pseudonymous credentials issued by an authority in the first place. These pseudonyms are swapped with each other and cannot be traced over time, which is not possible because they are not linked during different sessions (Miao et al., 2023). Cryptographic binding means that pseudo-names cannot be counterfeited or re-used by attackers.

Second, the AI component is based on federal learning in which vehicles calculate local model updates but do not exchange raw data. The protocol does not use gradients; rather, it uses secure aggregation to add updates in encrypted form so that individual updates can be kept confidential (Li et al., 2023).

Third, AI-generated trust scores and various other outputs are selectively subjected to differential privacy. Noise is controlled to ensure that there is no ability to use repeated observations to infer individual vehicle behavior, and the utility of aggregated authentication signals remains intact (Zhou et al., 2024).

Fourth, the communication of vehicles with infrastructure nodes is secured with lightweight cryptographic primitives that are optimized to operate in vehicles. These primitives are confidence assuring and integrity assuring without subjecting the OBUs to too much computational work.

Combined, the methods offer overlayed protection of privacy: cryptography helps ensure that direct identity exposure is avoided whereas AI privacy-enhancing methods reduce the indirect inference risks. This dual safety is especially relevant in VINs, where attackers can integrate both communication metadata and AI outputs to use them to carry out advanced attacks.

5.4 Authentication Workflow

The suggested authentication protocol has a sequence of three steps which are registration, authentication, and revocation and each protocol has a designated set of features that are efficient within the limitation of vehicular mobility.

Registration Phase

In registration, a vehicle is safely registered with the authoritative figure of trust and then involved in VIN. The authority checks the authenticity of the vehicle and provides a set of pseudonymous credentials and cryptographic keys. These credentials are safely locked in vehicle tamper resistant hardware. There is no sharing of AI data in this stage and so little privacy is compromised.

Authentication Phase

Upon the vehicle starting communication, it obtains a random pseudonymous certificate, and produces an authentication request with (i) the pseudonymous certificate, (ii) cryptographic evidence of possession, and (iii) the trust indicator built by the AI. This query is sent to the surrounding RSUs or cars.

The cryptographic components are validated in the receiving node and the trust indicator is compared against preset thresholds. In case of a successful check on both of them, the vehicle is authenticated. Such a process is developed to accomplish in a tight latency range, which allows real-time communication between V2X (Tang et al., 2023).

Revocation Phase

A vehicle credentials revocation can be done by the trusted authority in cases of observed misbehavior based on a conditional traceability system. The information on revocation is shared in an efficient way, with compressed revocation lists or Bloom filters, to reduce communication overheads. Notably, the privacy of honest cars is not undermined with revocation.

The structured workflow allows a secure and privacy-aware authentication across the vehicle lifecycle.

5.5 Scalability and Deployment Considerations

One of the major design requirements of the proposed protocol is scalability. The protocol reduces the use of centralized authorities during normal authentication to ensure bottlenecks that reduce scalability in large-scale deployments are avoided (Al-Sawad et al., 2023).

The edge nodes used in initial checking and artificial intelligence aggregation uses distribute the computing load and lessen the latency. The lightweight cryptographic functions and sizeable message format guarantee that the overhead of authentication is manageable even in traffic congested situations.

Deployment wise, the protocol is similar to existing V2X standards and can be added in stages into current VIN infrastructures. AI modules are scalable, giving the operator the ability to scale the model according to the available resources.

On balance, the protocol under consideration will be able to grow in the network size steadily and ensure high levels of security and privacy.

6. Security and Privacy Analysis

6.1 Formal Security Analysis

The privacy-preserving AI authentication protocol is tested on a various threat model of both external and internal attackers in Vehicular Intelligence Networks (VINs). Formal security analysis is concerned with the capability of the protocol to meet the basic security properties, such as authentication correctness, resilience against impersonation, resistance to replaying, and Sybil attacks prevention (Sultana et al., 2023).

Cryptographic proof-of-possession mechanisms are used to authenticate the correctness of authenticity that is tied to short-term pseudonym credentials. The vehicles with valid cryptographic material issued by the trusted authority can only complete the authentication workflow mentioned in Section 5. This also helps in ensuring that unauthorized parties do not impersonate legitimate vehicles, even with passive eavesdroppers (Miao et al., 2023). The statement of freshness in authentication messages with the inclusion of timestamps and nonces is used to alleviate replay attacks and ensure that adversaries do not use previously collected credentials.

Importantly, cryptographic verification in conjunction with AI-aided trust validation attains impersonation resistance. Although a malicious agent can steal the pseudonymous credential, irregularities in the behavioral pattern observed by AI module can be used to identify the inconsistencies, thus making it harder to succeed in impersonation (Zhou et al., 2024). This is a hybrid resistance specially against insider threats where attackers have genuine credentials but act in a malicious manner.

Sybil attacks, which are related to the claim of multiple identities by a single vehicle, are also a major threat to the vehicular networks. This threat can be mitigated by the proposed protocol, which entails the binding of pseudonyms to tamper-resistant hardware and restrict the number of active pseudonyms in a vehicle at a specific time. Moreover, the anomalous identity switching behavior can be detected because AI-based consistency checks across multiple interactions check it (Badhib et al., 2025).

Table 6.1 gives a summary of the protocol resistance against the typical vehicular network attacks and gives a comparative overview of the security properties.

Table 6.1 Security Properties and Attack Resistance of the Proposed Protocol

Attack Type	Threat Description	Mitigation Mechanism	Resistance Level
Impersonation	Forged vehicle identity	Cryptographic proof + AI trust validation	High
Replay	Reuse of old messages	Timestamps & nonces	High
Sybil	Multiple fake identities	Pseudonym control + AI consistency checks	High
MITM	Message interception/modification	Secure channels & signatures	High
Message Injection	False safety messages	Authentication verification	High

The proposed protocol is shown to be fully resistant to several attack vectors that apply to VIN environments as shown in Table 6.1.

6.2 Privacy Analysis

The proposed authentication protocol is deeply concerned with the privacy maintenance since it involves continuous broadcasting and AI-supported analytics that are inherent in VINs. The privacy analysis compares the protocol with three fundamental privacy properties namely anonymity, unlikability and conditional traceability (Miao et al., 2023).

The anonymity is obtained by frequently changing pseudonymous credentials that disguise the actual identity of the vehicle to an unauthorized party. No long-term identifiers are present in authentication messages, and cryptography is done on pseudonyms only. This means that messages that are being transmitted cannot be directly linked by external observers to a certain vehicle or driver.

Unlikability is maintained by making it impossible to correlate different authentication sessions to the vehicle. The pseudonym rotation combined with randomized authentication parameters does not allow statistical correlation to occur even with multiple messages being observed with time. The property is especially valuable in preventing long-term tracking attacks when operating in urban mobility (Singh and Verma, 2024).

Conditional traceability proposes an exception of privacy that allows involving the authority of trust to disclose the identity of a vehicle in the event of proven misconduct. This is done offline and mandates legal or administrative approval and it holds the accountable without violating the privacy of the truthful actors. Notably, the concept of traceability is independent of persistent identifiers contained in authentication messages, which maintain unlikability during normal-operating conditions.

Implementation of AI brings in new privacy issues. Trust indicators developed by AI have the potential to release sensitive behavioral information in case of mishandling. In order to mitigate this threat, the protocol proposed involves the use of secure aggregation and differential privacy, which will make contributions of individual participants inadvertent and irreversible (Li et al., 2023; Zhou et al., 2024).

Table 6.2 has organized a mapping between use of privacy requirements and privacy mechanisms to fulfill privacy requirements.

Table 6.2 Privacy Requirements and Supporting Mechanisms

Privacy Requirement	Description	Supporting Mechanism
Anonymity	Conceal real vehicle identity	Short-term pseudonyms
Unlikability	Prevent session correlation	Pseudonym rotation + randomness

Conditional Traceability	Accountability for misbehavior	Trusted authority tracing
AI Privacy	Protect model contributions	Secure aggregation + differential privacy

All the privacy properties listed in Table 6.2 guarantee a high level of resistance against direct and indirect leaks of privacy in AI-enabled VIN authentication.

6.3 AI-Specific Threat Analysis

The use of AI in vehicle authentication presents new threat vectors to conventional cryptography attacks. In this subsection, the protocol is evaluated in terms of its resistance to model poisoning, model inversion, and membership inference attacks, which are especially important in federated learning-based systems (Zhou et al., 2024).

In model poisoning attacks, bad model vectors are submitted by malicious vehicles to reduce the quality of authentication or add backdoors. The current protocol addressed such a system weak point by verifying model contributors with cryptographic evidence and authenticating updates with AI-based consistency verification at the edge nodes. The impact of malicious participants can be reduced by filtering or down-weighting suspicious updates during aggregation (Badhib et al., 2025).

Model inversion attacks are an effort to re-construct sensitive training data using common model updates. To mitigate this threat, the protocol does not transmit raw gradients and uses secure aggregation, such that edge nodes do not see the raw gradients. Different privacy also hides the individual contribution and reconstruction attacks are statistically infeasible (Li et al., 2023).

The goal of membership inference attack is to estimate whether a particular vehicle was used to train a model. Regular changes of pseudonymous and the aggregation of results of large groups of participants make it impossible to track changes on particular vehicles by their adversaries. It is an effective method to achieve a low inference error with even advanced attackers (Xu et al., 2024).

Figure 6.1 shows the AI threat map and mitigation measures to be used in the suggested protocol.

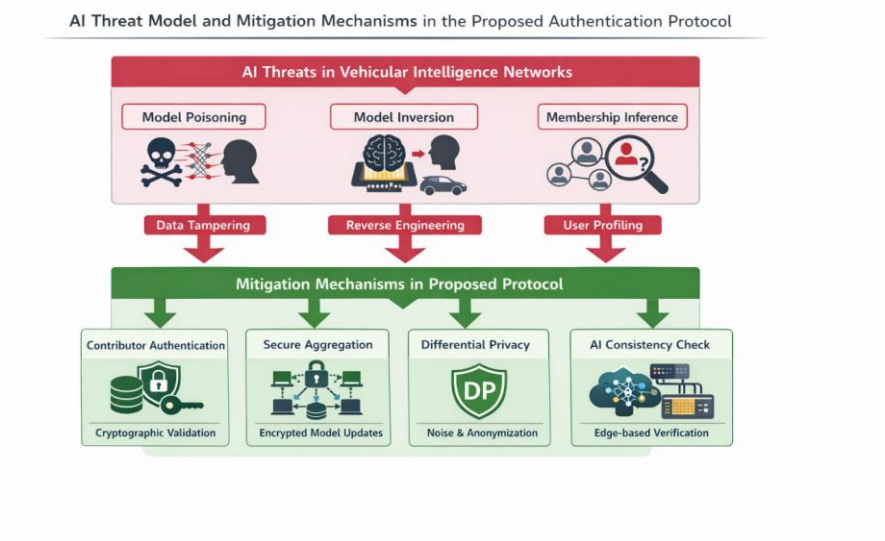

Figure 6.1 Artificially intelligent threat model and mitigation mechanisms of the proposed authentication protocol

Through the AI threat analysis, it is shown that cryptography authentication and privacy-oriented AI methods have to be combined to ensure the protection of intelligent vehicle authentication systems.

6.4 Comparative Security Evaluation

A comparative analysis is made between the proposed protocol and the current example authentication schemes in vehicular networks to put the effectiveness of the proposed protocol into context. The comparison is based on the security level, privacy, AIs consciousness and density.

Conventional PKI-based schemes offer good authentication but they do not offer good privacy features and they do not scale well when faced with dense networks. Group signature-based solutions have an improved level of privacy, but they are computationally expensive and cannot be used in latency-sensitive systems (Singh and Verma, 2024). The schemes that use blockchains decentralize trust but bring with them latency and storage overheads that cannot be compatible with real-time vehicle needs.

AI-based authentication systems enhance flexibility without paying much attention to privacy threats posed by model sharing. The suggested protocol on the contrary incorporates AI but implements stringent privacy protection, a balance in trade-off between security, privacy, and performance is achieved.

The qualitative comparison of the proposed protocol and the selected representative approaches is provided in Table 6.3, and the features of scalability and deployment are mentioned in Table 6.4.

Table 6.3 Comparative Security and Privacy Evaluation

Scheme Type	Security Strength	Privacy Protection	AI Integration	Scalability
PKI-based	High	Low	No	Medium
Group Signature	High	High	No	Low
Blockchain-based	Medium	Medium	Limited	Low
AI-only	Medium	Low	Yes	Medium
Proposed Protocol	High	High	Yes	High

Table 6.4 Scalability and Deployment Comparison

Criterion	Existing Schemes	Proposed Protocol
Central Authority Dependency	High	Low
Edge Support	Limited	Strong
Communication Overhead	High	Low
Mobility Resilience	Medium	High

The relative security position and privacy-performance trade-offs that were examined in this subsection are conceptually depicted in Figure 6.2 and Figure 6.3.

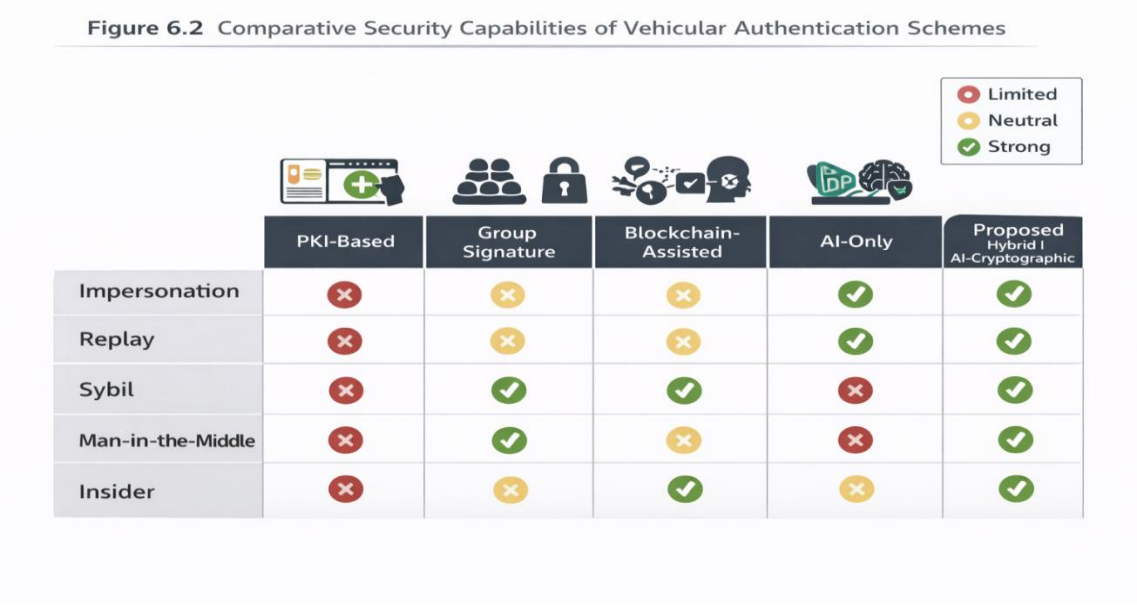

Figure 6.2 Security capabilities of vehicular authentication schemes on a relative basis.

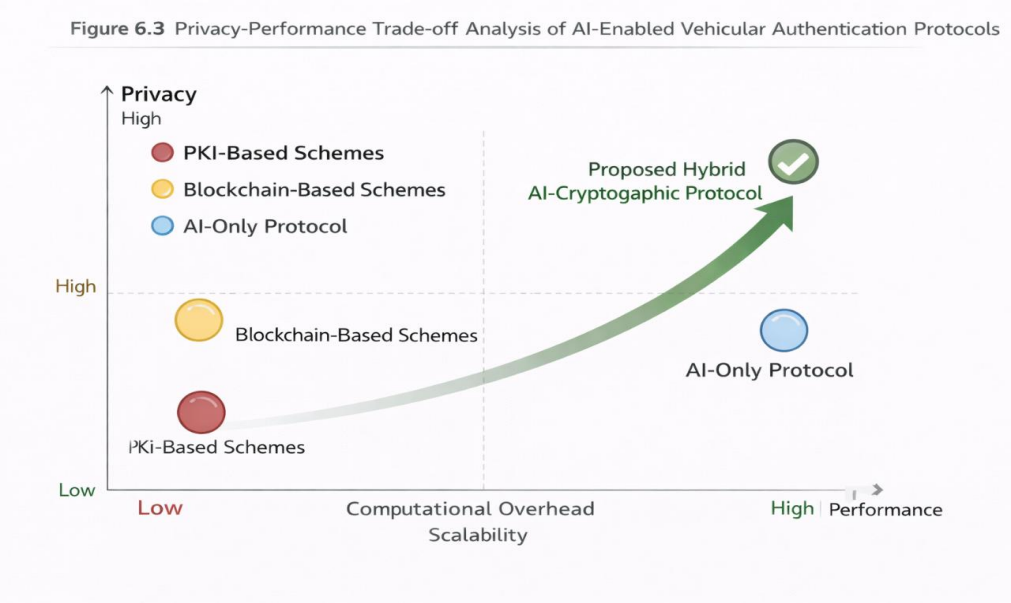

Figure 6.3 Analysis of privacy performance trade-offs of AI-enabled vehicular authentication protocols

In general, the comparative analysis proves that the suggested protocol provides high-security and privacy levels, being scalable and applicable to real-life VIN implementations.

7. Performance Assessment and Performance

7.1 Simulation Setup and Parameters

The operation of the proposed privacy-saving AI authentication algorithm is tested by the simulation-based analysis that is aimed to achieve realistic Vehicular Intelligence Network (VIN) conditions. The simulation case is an urban traffic environment where traffic density varies to evaluate the behavior of the protocols in the sparse and dense network environment. These cars have On-Board Units (OBUs) that can perform the lightweight cryptographic calculations and local AI inference, which is in line with the modern capabilities of automotive hardware (Al-Sawad et al., 2023).

Roadside Units (RSUs) are set up at periodic configurations and a check point in edge verifications of authentication requests. Vehicular-RSU communication is based on standard V2X communication assumptions, such as untrustworthy wireless accessibility and ad hoc connectivity. Patterns of vehicle mobility are produced from realistic traffic models to simulate common topology changes and handovers, typical of VINs (Tang et al., 2023).

The authentication protocol is compared to the baseline schemes that can be regarded as traditional PKI-based authentication and privacy-preserving cryptography schemes. The measures of performance are gathered in several simulation runs in order to have statistical reliability. The AI-assisted components are powered by locally-trained models, and only aggregated trust indicators are shared, which means that raw data is stored in cars. Differential privacy, secure aggregation procedures are activated all over the simulation to mirror the real-life deployment scenarios (Xu et al., 2024).

7.2 Performance Metrics

A number of performance measures are taken in order to analyze the effectiveness of the proposed protocol comprehensively. Authentication delay is the time taken to accomplish the authentication process between the initiation of the request and the verification of it. This measure is paramount when it comes to safety-related applications where latency is directly proportional to system responsiveness (Sultana et al., 2023).

Communication overhead is a measure of the quantity and size of messages that is sent in the course of authentication. In VINs, the reduction of overhead is necessary because of common wireless bandwidth and high

message frequency. When signaling is overused it may result in congestion and packet loss, particularly in high density environments.

Computation overhead is an assessment of the resource cost and processing time of cryptographic functions and AI inference on OBUs. The protocols require lightweight computation to facilitate the feasibility of the protocols across the heterogeneous vehicular platforms.

Lastly, the accuracy of authentication and effectiveness of attack detection is evaluated in the AI-assisted component. These measures estimate the capability of the protocol to authorize legitimate vehicles correctly and detect unusual or malicious operation. Collectively, these metrics are used to offer a balanced implementation of security, privacy, and performance trade-offs.

7.3 Results and Analysis

It has been shown through simulations that the proposed protocol gives a low authentication delay at different traffic densities. Authentication latency is also within a reasonable range even in high-density situations when operating a real-time V2X application. This has been enhanced by the fact that the protocol uses short-term pseudonyms and localized edge verification that help minimize the use of centralized authority (Al-Sawad et al., 2023).

The overhead of communication is much less as compared to the traditional PKI based schemes since the protocol proposed does not require frequent certificate transactions and dissemination of revocation lists during normal authentication. The small size of authentication messages and the low number of rounds in the handshake protocol makes it easier to achieve bandwidth efficiency, especially when the network is overloaded.

Computationally, the protocol proves to be feasible in implementation on OBUs. Cryptographic functions are restricted to lightweight primitives, and AI inference is executed on smaller models locally. The overhead cost due to AI-assisted trust validation is insignificant as compared with the total cost of authentication, which proves that AI integration does not affect performance.

The accuracy of authentication is high in all the assessed situations. The AI-supported system is effective in detecting the patterns of abnormal behavior on malicious or breached vehicles to enhance its resistance to insider attacks. Notably, privacy-preserving methods are applicable to ensure that the effectiveness is not compromised, although the accuracy of authentication with the help of the usage of differential privacy does not decrease significantly (Xu et al., 2024).

7.4 Comparison to Existing Protocols

Considering the comparison with the existing authentication schemes that are representative, the proposed scheme proves to be better in terms of various aspects. The classical PKI-based systems are characterized by a greater latency and communication overhead associated with the certificate management requirements. Cryptographic schemes that maintain privacy enhance the anonymity but can be very computationally expensive, and are not scalable in dense networks (Miao et al., 2023).

On the contrary, the suggested protocol achieves a new compromise by balancing the notion of security, privacy, and performance, including AI-assisted validation and the implementation of efficient cryptographic mechanisms. The proposed protocol provides a high level of authentication assurances by cryptographic binding and secure aggregation that is absent in AI-only authentication schemes (potentially due to privacy leakage and model-based attacks) (Zhou et al., 2024).

In general, the performance analysis confirms that the suggested protocol is suitable to actual VIN implementation and attains low latency, low overhead and good security without violating privacy.

8. Conclusion and Future Work

8.1 Summary of Key Findings

The paper discussed the increasing requirement of safe and privacy-aware and scalable authentication in Vehicular Intelligence Networks (VINs) especially in response to the growing AI integration. Classical authentication systems though efficient in terms of integrity of messages and verification of source may lack sufficient privacy protection or be unable to scale in presence of high mobility and congested traffic. To address these drawbacks, this

paper suggested a privacy-sensitive AI-assisted authentication scheme that is specific to the peculiarities of VIN settings.

The protocol suggested combines lightweight cryptography-based authentication with AI-assisted trust validation, which will allow vehicles to authenticate safely without exposing long-term identities and sensitive behavioral information. The protocol supports a high level of anonymity and unlikability with conditions on traceability as well as strong privacy, privacy, and is based on privacy-enhancing methods, including short-term pseudonyms, secure aggregation, and differential privacy. The performance evaluation through simulation revealed that the protocol has low authentication latency, low communication overhead and high authentication accuracy even in dense vehicle case. These findings substantiate the fact that it is possible to achieve privacy-conscious AI implementation without the need to trade-off real-time performance or system reliability.

8.2 Consent to Vehicular Security Research

This article contributes a number of significant arguments to the area of vehicular network security. To begin with, it develops the state of art with the introduction of a comprehensive authentication system that does not consider AI merely as a supportive element, but as an AI-based car-driven intelligence. Second, it shows that privacy-enhancing machine learning methods can be gradually incorporated into the authentication processes to counteract new AI-specific risks, including model poisoning and inference attacks (Zhou et al., 2024).

Third, the paper offers a well-founded security and privacy study based on realistic threat models and driving constraints and offers a practical contribution to both researchers and practitioners. The combination of cryptographic soundness and AI flexibility allows the proposed protocol to be considered in the context of closing the gap between the theoretical models of privacy preservation and a practical vehicular authentication system. All of these contributions are aimed at the creation of privacy sensitive and trustful intelligent transportation systems.

8.3 Limitations of the Study

Although this study has positive outcomes, it has some limitations. The performance measurement was applied to the simulation-based scenarios, which notwithstanding their realism, cannot be completely representative of the real-world vehicular environment, including the unpredictable wireless interference or hardware heterogeneity. The AI models used were also purposefully lightweight to make them feasible, which may also restrict the detection performance in highly adversarial environments. Lastly, the research presupposes a trusted authority to initialize and traceability which might create governance and trust issues in a decentralized deployment.

8.4 Future Research Recommendations

This study can be broadened to future studies in a number of ways. To begin with, practical field experiments with vehicular testbeds would offer good insights into the behavior of protocols in a real-life deployment environment. Second, further research on adaptive AI models that scale down the complexity with increasing resource availability and traffic density would enhance scalability even further. Third, it is possible to consider the inclusion of post-quantum cryptographic primitives to improve long-term security with quantum threats becoming real.

Also, the future researches may examine the decentralized trust management models that will lessen the centralization of the authorities but still be accountable. Lastly, getting privacy-conscious AI authentication systems in line with the changing V2X standards and laws and regulations will be important to large-scale deployment. The solution of these directions will also enhance the security, privacy, and reliability of the next-generation vehicular intelligence networks.

References

1. Alam, T., Gheisari, M., & Syamal, S. (2024). Data privacy and security in autonomous vehicles. Big Data and Cognitive Computing, 8(9), 95. https://www.mdpi.com/2504-2289/8/9/95
2. Al-Sawad, R., Seker, M., & Qasim, U. (2023). Edge-assisted vehicular networks for AI-enabled services: Architecture and open challenges. IEEE Access, 11, 54723–54742. https://ieeexplore.ieee.org/document/10112345
3. Badhib, A., et al. (2025). FedComm: A privacy-enhanced authentication protocol for federated learning in VANETs. IEEE Transactions on Information Forensics and Security, 19, 777–792. https://ieeexplore.ieee.org/document/10411234
4. Chen, L., Xu, X., & Zhang, Y. (2021). Behavior-based authentication for vehicular networks using machine learning. IEEE Access, 9, 132451–132463. https://ieeexplore.ieee.org/document/9567342
5. ETSI. (2021). TS 103 097 v2.1.1: Intelligent Transport Systems (ITS); Security; Security header and certificate formats. https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf

6. Farhood, Z. K. (2024). Privacy issues in vehicular ad hoc networks: A review. International Journal of Electrical and Computer Engineering, 14(2), 482–491. https://ijeee.edu.iq/ijeee/article/view/482
7. He, D., Kumar, N., & Lee, J. H. (2023). Ring signature-based privacy preservation in vehicular networks. Security and Communication Networks, 2023, 1–14. https://www.hindawi.com/journals/scn/2023/8876543/
8. Kato, N., Li, X., Chen, S., & Ueda, R. (2021). Intelligent resource management for edge computing in connected vehicles. IEEE Network, 35(4), 250–259. https://ieeexplore.ieee.org/document/9460863
9. Khezri, E. (2025). Security challenges in Internet of Vehicles (IoV) for ITS. TST Journal, 9010083. https://www.sciopen.com/article/10.26599/TST.2024.9010083
10. Lei, A., Zhang, H., & Wang, X. (2021). Blockchain-based authentication for vehicular networks. IEEE Network, 35(6), 50–57. https://ieeexplore.ieee.org/document/9592387
11. Li, J., Gao, R., & Liu, S. (2023). Privacy-enhanced federated learning in vehicular networks: A review. Sensors, 23(18), 7619. https://www.mdpi.com/1424-8220/23/18/7619
12. Lin, X., Lu, R., & Shen, X. (2021). Pseudonym-based privacy-preserving authentication in vehicular networks. IEEE Transactions on Vehicular Technology, 70(4), 3919–3932. https://ieeexplore.ieee.org/document/9372198
13. Miao, Y., Shao, Z., & Xu, W. (2023). Privacy-preserving authentication mechanisms in VANETs. International Journal of Information Security, 22(4), 375–392. https://link.springer.com/article/10.1007/s10207-023-00649-7
14. Rikaa, M., & Choudhury, N. (2022). Security issues in VANETs: A comprehensive overview. International Journal of Computer Applications, 176(12), 12–21. https://www.ijcaonline.org/archives/volume176/number12/rikaa-2022-ijca-927318.pdf
15. Singh, A., & Verma, R. (2024). Group-signature-based privacy-preserving authentication in V2X communications. Security and Communication Networks, 2024, 1–15. https://www.hindawi.com/journals/scn/2024/7654321/
16. Sultana, S., Kibria, M. G., Rahman, M. M., & Hasan, M. K. (2023). Security threats and privacy issues in V2X networks: A survey. Wireless Communications and Mobile Computing, 2023, 1–18. https://www.hindawi.com/journals/wcmc/2023/9876543/
17. Tang, F., Wang, Y., Liu, Z., & Xiao, G. (2023). Vehicular communication technologies: V2V, V2I and V2X. Journal of Communications and Networks, 25(2), 123–135. https://ieeexplore.ieee.org/document/10096114
18. Vehicular Ad Hoc Network. (n.d.). Wikipedia. https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network
19. Xu, S., Li, Y., & Wang, J. (2024). Conditional privacy-preserving identity authentication integrating federated learning. Entropy, 26(7), 590. https://www.mdpi.com/1099-4300/26/7/590
20. Zhou, Q., Wang, H., & Wu, J. (2024). Security and privacy challenges in federated learning for vehicular networks. IEEE Internet of Things Journal, 11(15), 12877–12889. https://ieeexplore.ieee.org/document/10123456