



Secure and Privacy-Preserving Vehicle Renting in VANETs Using a Zero-Trust Framework

Madhab Chandra Jena, Tamal Paul, Om Krishna Jena

GIFT Autonomous, Bhubaneswar, Odisha, India, madhab_jena@rediffmail.com

GIFT Autonomous, Bhubaneswar, Odisha, India, tamalpaul@gift.edu.in

CIPET, Bhubaneswar, Odisha, India. omkrishnajena2007@gmail.com

How to Cite this Article:

Jena, M. C., Paul, T. & Jena, O. K. (2026). Secure and Privacy-Preserving Vehicle Renting in VANETs Using a Zero-Trust Framework. International Journal of Creative and Open Research in Engineering and Management, 2(10), 1-9.
<https://doi.org/10.55041/ijcope.v2i9.265>

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.



<https://doi.org/10.55041/ijcope.v2i9.265>

Abstract

The rapid development of connected and intelligent transportation systems has increased the adoption of Vehicular Ad Hoc Networks (VANETs) for vehicle sharing and rental services. However, vehicle renting in VANETs introduces significant security and privacy challenges, including unauthorized access, identity disclosure, driver tracking, Sybil attacks, credential misuse, and difficulties in establishing accountability. Conventional authentication approaches often rely on persistent identities, which can compromise driver privacy, while fully anonymous mechanisms may make it difficult to identify malicious users when security incidents occur. This paper presents a privacy-preserving and zero-trust approach for secure vehicle renting in VANETs that integrates anonymous authentication, controlled accountability, and Sybil resistance. The proposed framework follows a zero-trust principle in which vehicles, drivers, and service entities are not implicitly trusted and access requests are subjected to appropriate verification before rental resources are authorized. Privacy-preserving credentials are used to minimize unnecessary disclosure of driver identities, while conditional traceability enables an authorized entity to establish the identity of a malicious participant when required. The framework also incorporates mechanisms to restrict the creation and misuse of multiple pseudonymous identities, thereby strengthening resistance against Sybil

attacks. A security analysis is presented against major threats, including impersonation, replay, man-in-the-middle, credential misuse, and Sybil attacks. The paper further discusses computational and communication considerations, scalability, and practical deployment challenges. The proposed approach provides a unified perspective for achieving secure, privacy-aware, and accountable vehicle-rental services in future connected vehicular environments.

Keywords: Vehicular Ad Hoc Networks, VANETs, vehicle renting, privacy preservation, zero-trust security, authentication, driver accountability, Sybil attacks, pseudonymous credentials, connected vehicles.

1. Introduction

The rapid development of intelligent transportation systems (ITS) has transformed vehicles from isolated transportation devices into highly connected computing platforms capable of communicating with other vehicles, roadside infrastructure, cloud services, and mobility platforms. Vehicular Ad Hoc Networks (VANETs) provide an important communication foundation for these systems by supporting applications such as cooperative driving, traffic



management, emergency warning, intelligent parking, vehicle sharing, and connected vehicle renting. However, the open, dynamic, and distributed characteristics of vehicular communication also create substantial cybersecurity and privacy risks. Authentication, identity protection, message integrity, accountability, and resistance to malicious participants are therefore fundamental requirements for dependable VANET services [5–10].

Vehicle renting is particularly challenging because it combines vehicular communication with digital identity, access control, financial transactions, and physical resource management. A typical connected vehicle-rental ecosystem may involve a driver, rental provider, vehicle, roadside unit (RSU), authentication authority, cloud or edge infrastructure, and other network participants. Each entity may exchange security-sensitive information during registration, authentication, vehicle selection, rental authorization, vehicle operation, and rental termination. Consequently, compromising any important component can potentially affect both the digital service and the physical vehicle.

A central challenge is that conventional authentication mechanisms may require users or vehicles to repeatedly disclose persistent identifiers. Although this simplifies identity verification, it can expose drivers to tracking and profiling. Vehicular communication may reveal information about a driver's movement, travel patterns, vehicle usage, and interactions with mobility services. Privacy-preserving authentication has therefore received substantial attention in VANET research [5–7]. Existing approaches employ pseudonyms, anonymous credentials, group signatures, certificateless cryptography, and other mechanisms to allow legitimate participants to authenticate without continuously exposing their permanent identities [11–16].

Privacy preservation, however, introduces another security problem. If a participant is allowed to use multiple pseudonyms without appropriate control, a malicious entity can exploit those identities to appear as multiple independent vehicles. Such a Sybil attack can influence trust decisions, manipulate network information, evade blacklists, circumvent rental restrictions, or obtain multiple services simultaneously. Akil et al. developed a non-interactive privacy-preserving Sybil-free authentication scheme for VANETs, demonstrating the importance of addressing privacy and Sybil resistance together [1]. This principle is especially important in vehicle renting, where multiple unauthorized identities could potentially be used to bypass user-level rental policies.

Another fundamental requirement is accountability. Complete anonymity may protect legitimate drivers from unnecessary tracking, but it can also make it difficult to investigate serious violations. A rental vehicle may be involved in fraudulent transactions, unauthorized use, malicious network activity, or other security incidents. Therefore, a practical privacy-preserving system should support conditional accountability: the driver's identity remains protected during legitimate activities but can be revealed by an authorized entity when predefined security or legal conditions are satisfied. Akil et al. investigated this privacy-accountability relationship in vehicle renting and demonstrated the relevance of privacy-preserving driver accountability for VANET-based rental services [2].

The emergence of zero-trust security provides an additional opportunity to strengthen connected vehicle-rental systems. Traditional security architectures often rely on implicit trust after successful authentication or network admission. Such assumptions are increasingly unsuitable for connected mobility environments because a previously legitimate account, vehicle, RSU, edge node, or cloud component may subsequently become compromised. Zero-trust security instead follows the principle that access should be explicitly verified rather than automatically trusted. Recent research has begun examining the applicability of zero-trust principles to connected vehicles and automotive networks [30,31,33,34]. Akil et al. specifically proposed a secure and privacy-preserving authentication scheme using a zero-trust approach for vehicle renting in VANETs [3].

The major security requirements of a privacy-preserving vehicle-rental ecosystem are summarized in Table 1.



Table 1. Security and Privacy Requirements for VANET-Based Vehicle Renting

Requirement	Purpose	Security significance
Privacy-preserving authentication	Verify legitimate users without unnecessary identity disclosure	Reduces identity exposure and tracking
Secure authorization	Determine whether a driver is permitted to access a particular vehicle or service	Prevents unauthorized vehicle usage
Conditional accountability	Enable identity resolution only under legitimate conditions	Balances privacy with responsibility
Sybil resistance	Prevent one participant from exploiting multiple identities	Protects rental and network policies
Zero-trust verification	Avoid implicit trust after initial authentication	Limits damage from compromised entities
Credential protection	Prevent theft, duplication, and misuse of authentication credentials	Protects rental accounts and vehicles
Message integrity	Prevent unauthorized modification of vehicular messages	Protects communication reliability
Confidentiality	Protect sensitive rental and authentication information	Prevents information leakage
Revocation	Disable compromised or malicious credentials	Prevents continued unauthorized participation
Non-repudiation	Provide evidence of authorized transactions or actions	Supports dispute resolution and investigation
Scalability	Support large numbers of vehicles and users	Necessary for real-world deployment

As shown in Table 1, secure vehicle renting cannot be achieved through authentication alone. Privacy, authorization, accountability, Sybil resistance, and credential management must operate together. This requirement becomes even more important as connected vehicles increasingly depend on cloud and edge infrastructure.

Several studies have examined privacy-preserving authentication as a means of reducing identity exposure in VANETs. Mundhe et al. presented a comprehensive survey of authentication and privacy-preserving schemes and highlighted the trade-offs among authentication security, anonymity, computational efficiency, and communication overhead [5]. Other surveys have similarly identified privacy preservation, authentication efficiency, and attack resistance as major challenges for vehicular communication [6–10]. These studies establish that authentication mechanisms must be designed specifically for the highly dynamic and resource-sensitive characteristics of vehicular networks.

Cryptographic approaches have also been developed to improve authentication efficiency. Zhong et al. proposed a privacy-preserving authentication mechanism using full aggregation, reducing the overhead associated with verifying multiple vehicular messages [11]. Qi et al. investigated pseudonym-based certificateless authentication to provide privacy while avoiding some of the limitations of conventional certificate-management mechanisms [12]. Other conditional privacy-preserving authentication schemes have investigated efficient key establishment, vehicle-to-infrastructure authentication, and scalable revocation [13–17].

Although these mechanisms provide strong foundations, the requirements of vehicle renting extend beyond ordinary vehicle-to-vehicle authentication. In a rental environment, the system must establish not only whether a communication participant is legitimate but also whether that participant is authorized to use a particular physical vehicle. The rental provider may need to enforce conditions such as rental duration, vehicle category, user eligibility, credential validity, and security status. Consequently, authentication must be closely connected to authorization and access control.

Conditional privacy-preserving mechanisms address another part of this problem. Such schemes allow a vehicle or driver to communicate through temporary identities while retaining a mechanism for authorized identity recovery [13–19].



This approach is highly relevant to driver accountability because it avoids the need to expose the renter's permanent identity during every communication session. However, the identity-resolution mechanism itself becomes a sensitive security component and must be protected against unauthorized disclosure or misuse.

Sybil resistance introduces a further complication. The use of pseudonyms can improve privacy but may simultaneously create opportunities for identity multiplication. Li et al. proposed the use of trajectory-related characteristics as a basis for privacy-preserving and Sybil-resistant authentication, demonstrating that behavioral or contextual information can contribute to Sybil detection while protecting actual identities [19]. Other work has examined trust-based adaptive privacy preservation, where security and privacy decisions can respond to participant behavior [20]. These studies suggest that Sybil resistance should not necessarily depend solely on revealing permanent identities.

Blockchain has also emerged as a potential technology for addressing authentication, trust management, identity management, and revocation in VANETs. Blockchain-based authentication schemes can provide distributed verification and tamper-resistant records while reducing dependence on a single centralized authority [21–28]. Feng et al. proposed a blockchain-assisted privacy-preserving authentication system for vehicular networks, while other researchers have explored blockchain-based conditional privacy preservation and trust management [18,21,23–27].

However, blockchain-based approaches introduce their own challenges. Consensus mechanisms, distributed storage, transaction processing, and communication between blockchain nodes can increase system overhead. For vehicle-rental services, where authentication and authorization may need to occur rapidly, excessive blockchain processing can negatively affect usability. Blockchain should therefore be viewed as a potential supporting mechanism rather than a universal replacement for efficient cryptographic authentication.

Trust management represents another major research direction. Authentication determines whether an entity possesses valid credentials, whereas trust management attempts to assess whether the entity's behavior or information should be accepted. This distinction is important because an authenticated participant may still behave maliciously. Research has consequently investigated behavioral analysis, blockchain-based trust management, and context-aware trust models for identifying unreliable vehicles [24–27]. These mechanisms can complement authentication by providing information about participant behavior, but they do not eliminate the need for secure identity and access-control mechanisms.

The security of supporting cloud and distributed infrastructure must also be considered. Connected vehicle-rental platforms may use cloud services to maintain user credentials, rental information, authorization policies, and security logs. Akil et al. examined multi-covert-channel attacks in cloud environments and demonstrated the broader importance of protecting communication and computing infrastructure from unintended information-transfer mechanisms [4]. Although covert-channel attacks represent a different threat category from Sybil or authentication attacks, the study reinforces the need for an end-to-end security perspective covering both vehicular and supporting infrastructure.

The literature reviewed in this study is summarized in Table 2.

Table 2. Representative Literature on VANET Security and Privacy

Reference	Research focus	Main contribution	Relevance to vehicle renting
[1]	Sybil-free authentication	Privacy-preserving non-interactive authentication	Supports Sybil-resistant rental authentication
[2]	Vehicle renting and accountability	Privacy-preserving rental with driver accountability	Supports conditional accountability
[3]	Zero-trust vehicle renting	Privacy-preserving authentication under zero-trust principles	Directly supports the proposed security model
[4]	Cloud security	Analysis of multi-covert-channel attacks	Highlights infrastructure-level threats
[5–10]	VANET authentication surveys	Comprehensive analysis of authentication and privacy mechanisms	Establishes major research challenges



[11–12]	Cryptographic authentication	Aggregation and pseudonym-based authentication	Improves privacy and authentication efficiency
[13–17]	Conditional privacy	Anonymous authentication, key agreement, and revocation	Supports privacy and traceability
[18,21–23]	Blockchain authentication	Decentralized authentication and privacy protection	Supports distributed security management
[19]	Sybil-resistant authentication	Uses trajectory-related characteristics	Addresses identity multiplication
[20]	Trust-based privacy	Adaptive privacy based on trust	Supports behavior-aware security
[24–27]	Trust management	Blockchain, behavioral, and context-aware trust	Complements authentication
[28]	Blockchain key management	Secure authentication and key management	Supports distributed credential protection
[29]	Security analysis	Identifies weaknesses in privacy-preserving authentication	Demonstrates need for rigorous analysis
[30–34]	Zero-trust and automotive security	Application of zero-trust concepts to connected vehicles	Supports continuous verification

As indicated in Table 2, the existing literature provides important solutions for individual security requirements. Nevertheless, the requirements of privacy-preserving vehicle renting remain distributed across different research directions.

2. Literature Review and Research Gap

The literature on secure VANETs demonstrates that privacy-preserving authentication has evolved from conventional identity-based mechanisms toward pseudonymous and conditional authentication. Early approaches established the need for anonymous communication and secure authentication, while more recent research has focused on reducing computational overhead, improving revocation, and strengthening resistance against advanced attacks [5–19].

One important research direction involves pseudonym-based authentication. Pseudonyms allow legitimate users to communicate without revealing permanent identities, but effective pseudonym management is essential. If pseudonyms are frequently reused, they may enable tracking; if they can be freely generated, they may facilitate Sybil attacks. PRIVANET and related pseudonym-management approaches demonstrate the importance of carefully managing pseudonym changes to balance privacy and security [34]. Consequently, a vehicle-rental system should provide controlled pseudonymity rather than unrestricted anonymity.

Conditional privacy-preserving authentication provides a more balanced solution. Research has demonstrated that a legitimate vehicle can authenticate using a temporary identity while an authorized authority retains the ability to resolve that identity when necessary [13–19]. Such mechanisms are particularly suitable for rental services because they allow routine privacy while maintaining a mechanism for resolving responsibility following serious incidents.

However, accountability must be carefully designed. If the authority responsible for identity resolution can freely access driver identities, the system may become a surveillance mechanism. Therefore, identity resolution should require predefined conditions and appropriate authorization. The vehicle-rental model proposed by Akil et al. [2] is particularly relevant because it connects privacy preservation with driver accountability.

Sybil resistance remains another unresolved challenge. Existing Sybil-resistant mechanisms demonstrate that multiple identities can be detected or prevented through cryptographic, behavioral, or contextual approaches [1,19,20]. However, integrating such mechanisms with rental authorization introduces additional requirements. A renter should not be able to use multiple legitimate-looking credentials to circumvent restrictions, while legitimate users should retain sufficient privacy.



Blockchain-based approaches provide another potential solution for credential and trust management [18,21–28]. Their ability to maintain tamper-resistant records can support rental auditing, revocation, and accountability. Nevertheless, performance and privacy concerns remain. A rental platform cannot simply store all driver and vehicle activity on an immutable public or distributed ledger because such records may themselves become a source of privacy leakage.

Trust management provides complementary protection against authenticated but malicious entities. Behavioral and context-aware approaches [24–27] can help identify suspicious participants. Nevertheless, trust should not replace authentication. An entity should first establish its legitimacy and then be evaluated according to applicable security and behavioral policies.

The emerging zero-trust paradigm addresses this limitation by removing implicit trust assumptions. Zero-trust research in connected vehicles emphasizes continuous verification, least-privilege access, segmentation, and policy-based authorization [30,33,34]. ZeroVCS further demonstrates the feasibility of zero-trust authentication without relying entirely on a conventional trusted authority [31]. These developments suggest that zero-trust principles can provide an effective security layer for connected vehicle ecosystems.

The major difference between a conventional VANET authentication model and a zero-trust vehicle-rental model is summarized in Table 3.

Table 3. Conventional Trust Model versus Zero-Trust Vehicle Renting

Feature	Conventional approach	Zero-trust approach
Initial authentication	Establishes identity	Establishes identity but does not imply permanent trust
Trust assumption	May trust authenticated entities	No implicit trust
Access control	Often linked to initial authentication	Continuously policy-driven
Credential compromise	Potentially broad impact	Access can be restricted or revalidated
Authorization	Often static	Context and policy dependent
Privacy	Depends on authentication mechanism	Can incorporate privacy-preserving credentials
Accountability	Usually identity based	Can use conditional traceability
Sybil protection	Often separate mechanism	Can be integrated with credential and access policies
Rental security	May focus on initial access	Can cover the complete rental lifecycle

As shown in Table 3, zero-trust principles provide a natural mechanism for connecting authentication with continuous authorization. This is particularly useful in vehicle renting because a renter's authorization may change during a rental session and should not necessarily provide unrestricted access to every connected vehicle service.

Despite these advances, several gaps remain. First, privacy-preserving authentication, Sybil resistance, accountability, and zero-trust authorization are often investigated as separate research problems. Second, many authentication schemes focus on vehicular communication without explicitly considering the complete vehicle-rental lifecycle. Third, blockchain-based approaches may introduce overhead that is undesirable for latency-sensitive vehicular services. Fourth, conditional accountability requires careful protection of the identity-resolution process. Fifth, authenticated entities may still become malicious, making continuous verification and authorization important.

These gaps are consolidated in Table 4.



Table 4. Identified Research Gaps

Research gap	Existing limitation	Required direction
Privacy versus accountability	Anonymity can make investigation difficult	Controlled conditional traceability
Privacy versus Sybil resistance	Multiple pseudonyms may be abused	Controlled pseudonymous credentials
Authentication versus trust	Legitimate entities can behave maliciously	Continuous verification and authorization
Static versus dynamic authorization	Initial authentication may provide excessive access	Policy-based zero-trust authorization
Rental-specific security	General VANET protocols may ignore rental workflows	End-to-end rental security
Credential revocation	Revocation can be computationally expensive	Efficient credential lifecycle management
Blockchain overhead	Consensus and storage can increase latency	Selective use of distributed ledgers
Infrastructure security	Cloud and edge threats may be overlooked	End-to-end vehicular and infrastructure threat model
Scalability	Large-scale authentication can create overhead	Efficient and scalable security mechanisms

The research gap identified in Table 4 motivates the development of an integrated privacy-preserving and zero-trust framework for vehicle renting. The central premise is that **privacy, accountability, authentication, and Sybil resistance should not be treated as competing isolated functions**. Instead, they should be designed as mutually supporting components.

The proposed approach consequently builds on the following principles:

- **Privacy by design:** legitimate drivers should not be required to expose permanent identities during routine rental operations.
- **Zero implicit trust:** successful authentication should not automatically grant unrestricted access.
- **Controlled accountability:** identity resolution should be restricted to authorized circumstances.
- **Sybil resistance:** privacy-preserving credentials should not be freely exploitable to create multiple effective identities.
- **Least-privilege authorization:** renters should receive only the vehicle and services necessary for the authorized rental.
- **Credential lifecycle protection:** credentials should be securely issued, validated, monitored, and revoked.
- **End-to-end security:** protection should extend from the vehicle and driver to RSUs, edge/cloud infrastructure, and rental services.

The resulting research direction seeks to combine the strengths of privacy-preserving authentication [1,11–19], Sybil-resistant mechanisms [1,19,20], distributed trust and blockchain approaches [18,21–28], and zero-trust automotive security [3,30–34]. This integration distinguishes the proposed framework from approaches that focus exclusively on authentication or anonymity.

3. Proposed Privacy-Preserving Zero-Trust Framework

The proposed framework integrates privacy-preserving authentication, zero-trust access control, driver accountability, and Sybil resistance into a unified architecture for secure vehicle renting in VANETs. The framework is designed to address the limitations identified in the literature by separating a driver's real identity from the temporary credentials



used during routine vehicular communication. At the same time, the framework prevents authenticated entities from receiving implicit trust and provides controlled mechanisms for investigating malicious behavior.

The overall framework consists of several interacting entities: the driver, rental provider, vehicle, roadside unit (RSU), authentication authority, and supporting cloud or edge infrastructure. Each entity has a specific role in the rental lifecycle. The driver requests access to a vehicle, the rental provider determines rental eligibility, the authentication authority manages privacy-preserving credentials, the vehicle enforces access decisions, and RSUs or edge/cloud infrastructure support communication and security services.

Table 5. Entities and Responsibilities in the Proposed Framework

Entity	Primary responsibility	Security role
Driver	Requests and uses a rental vehicle	Holds privacy-preserving credentials
Rental Provider	Manages vehicles and rental agreements	Determines rental authorization
Rental Vehicle	Provides physical transportation service	Verifies access and executes policies
RSU	Facilitates roadside communication	Supports authentication and secure message exchange
Authentication Authority	Registers participants and manages credentials	Provides identity and credential services
Edge/Fog Node	Performs nearby security and processing functions	Reduces latency and processing burden
Cloud Service	Stores protected service information and policies	Supports scalable service management
Accountability Authority	Resolves identities under authorized conditions	Enables conditional traceability

As shown in Table 5, the framework avoids placing all security responsibilities on a single entity. This separation is important because compromise of one component should not automatically provide unrestricted control over the rental ecosystem.

3.1 System Architecture

The proposed architecture follows a layered security model. At the user layer, drivers interact with the rental platform through an authorized application or vehicle interface. The service layer contains rental providers responsible for vehicle availability, rental contracts, and access policies. The vehicular layer contains connected vehicles and RSUs. The security layer provides authentication, authorization, credential management, revocation, and accountability. Finally, edge and cloud infrastructure provides scalable computation and protected storage.

The communication process begins when a driver requests a rental service. Rather than directly transmitting a permanent identity to the vehicle, the driver uses a privacy-preserving credential. The rental provider verifies the request and determines whether the driver satisfies the applicable rental policy. A successful authentication does not automatically result in unrestricted access. Instead, the zero-trust mechanism evaluates the specific resource and operation being requested.

For example, a renter authorized to unlock and operate a vehicle should not automatically be authorized to modify security settings, access another vehicle, change ownership information, or retrieve another user's rental data. This implements the principle of least privilege.



Table 6. Main Communication and Security Phases

Phase	Main activity	Security objective
1	Driver registration	Establish legitimate membership
2	Credential issuance	Provide privacy-preserving identity
3	Vehicle discovery	Identify an available rental resource
4	Rental request	Submit protected rental information
5	Authentication	Verify driver legitimacy
6	Authorization	Determine permitted vehicle/service access
7	Secure session establishment	Protect subsequent communication
8	Rental operation	Enforce access and security policies
9	Monitoring	Detect abnormal or malicious behavior
10	Revocation/accountability	Restrict compromised users and investigate violations
11	Rental termination	Revoke temporary access and close the session

The sequence in Table 6 shows that authentication represents only one stage of the proposed security lifecycle. The framework continues to enforce authorization and security controls after authentication.

3.2 Threat Model

The proposed framework assumes that an attacker may operate outside or inside the vehicular communication environment. An external attacker may attempt to intercept messages, impersonate legitimate participants, replay previously transmitted authentication information, or create multiple identities. An internal attacker may possess valid credentials but misuse them to obtain unauthorized access or perform malicious activities.

The threat model considers the following major attack categories:

- **Impersonation attacks:** an attacker attempts to act as a legitimate driver or vehicle.
- **Replay attacks:** previously valid authentication messages are retransmitted.
- **Man-in-the-middle attacks:** an attacker attempts to intercept and manipulate communication.
- **Sybil attacks:** one malicious participant creates or controls multiple identities.
- **Credential theft:** legitimate authentication credentials are compromised.
- **Unauthorized access:** an authenticated participant attempts to access a resource outside the granted privileges.
- **Insider attacks:** a legitimate system participant abuses its privileges.
- **Identity-linking attacks:** multiple pseudonymous sessions are correlated to identify a driver.
- **Privacy attacks:** sensitive rental, identity, or location information is exposed.
- **Infrastructure attacks:** cloud, edge, or supporting communication infrastructure is compromised.

The framework assumes that cryptographic primitives are computationally secure and that the authority responsible for initial credential issuance is protected through appropriate organizational and technical controls. However, individual vehicles, drivers, and network nodes are not assumed to remain trustworthy after authentication.

3.3 Privacy-Preserving Registration and Credential Issuance

The registration phase establishes the relationship between a legitimate driver and the security infrastructure. The driver's permanent identity is verified by the appropriate authority during registration. Instead of using this permanent identity during every rental interaction, the system generates a privacy-preserving credential or pseudonymous identifier.

The credential contains sufficient cryptographic information for authentication but does not directly reveal the driver's permanent identity to ordinary communication participants. Credential issuance is controlled so that a malicious user cannot freely generate unlimited valid credentials.



This controlled credential model is particularly important for Sybil resistance. The system can associate credential issuance with an authorized registration relationship without exposing the underlying identity during routine communication.

3.4 Privacy-Preserving Authentication

When a driver requests a vehicle, authentication is performed using the privacy-preserving credential rather than directly transmitting the driver's permanent identity. The receiving entity verifies the cryptographic validity of the credential and determines whether it remains valid.

A successful authentication establishes that the requester possesses a legitimate credential without unnecessarily disclosing the permanent identity. Authentication messages should also include freshness information, such as nonces or timestamps, to prevent replay attacks.

The authentication process can be conceptually represented as:

Driver → Rental Provider/RSU: Authentication Request + Pseudonymous Credential

Rental Provider/RSU → Authentication Authority: Credential Verification Request

Authentication Authority → Rental Provider/RSU: Verification Result

Rental Provider/RSU → Driver: Authentication Response

Following successful authentication, the system proceeds to authorization rather than automatically granting complete access.

3.5 Zero-Trust Authorization

The principal distinction between the proposed approach and conventional authentication-based rental systems is the introduction of zero-trust authorization. The system does not consider a driver trustworthy merely because the driver's credential has been successfully authenticated.

Each sensitive request is evaluated according to applicable security policies. Relevant attributes may include credential validity, rental status, requested vehicle, permitted rental period, requested operation, security status, and other contextual information.

For example, a renter may be authorized to:

- unlock a specific vehicle;
- start and operate that vehicle;
- access permitted vehicle services; and
- terminate the rental.

The same renter may not be authorized to:

- access another renter's vehicle;
- modify authentication policies;
- issue credentials;
- alter vehicle ownership information; or
- access protected administrative functions.



This least-privilege approach reduces the consequences of credential compromise.

Table 7. Example Zero-Trust Access-Control Decisions

Request	Authentication status	Authorization status	Decision
Unlock assigned rental vehicle	Valid	Permitted	Allow
Start assigned vehicle	Valid	Permitted	Allow
Access another renter's vehicle	Valid	Not permitted	Deny
Modify security configuration	Valid	Not permitted	Deny
Extend rental period	Valid	Policy dependent	Re-verify
Access rental history	Valid	Authorized user only	Conditional
Administrative credential issuance	Valid renter	Not permitted	Deny
Suspicious high-risk operation	Valid	Requires additional verification	Challenge/deny

As shown in Table 7, authentication and authorization are deliberately separated. A valid identity is necessary but not sufficient for access.

3.6 Driver Accountability and Conditional Traceability

The framework preserves driver privacy during ordinary rental operations while maintaining controlled accountability. The pseudonymous credential used during a rental session is not intended to expose the driver's permanent identity to vehicles, RSUs, or other ordinary participants.

If a serious security violation occurs, an authorized accountability authority can initiate an identity-resolution process. Identity resolution should require appropriate authorization and predefined conditions rather than being available to every participant.

Potential accountability events include:

- deliberate vehicle misuse;
- fraudulent rental activity;
- repeated security-policy violations;
- credential sharing;
- Sybil activity;
- serious malicious communication; and
- unauthorized access attempts.

This mechanism creates a balance between privacy and accountability. Legitimate drivers can use the service without continuous identity exposure, while malicious behavior can remain attributable when required.

3.7 Sybil-Resistance Mechanism

Sybil resistance is integrated into the credential-management process rather than being treated as an independent detection mechanism. The basic principle is that a legitimate participant may use privacy-preserving credentials, but credential generation remains controlled by the authentication infrastructure.

The system can maintain protected relationships between the registered participant and issued credentials. The relationship does not need to be publicly visible. During normal communication, only the pseudonymous credential is presented. However, credential issuance and usage policies can prevent a participant from obtaining an unlimited number of simultaneously valid rental identities.



A suspicious pattern, such as multiple concurrent rental requests or repeated attempts to use unrelated credentials, can trigger additional verification. If sufficient evidence of abuse exists, the corresponding credentials can be revoked and, where appropriate, the underlying identity can be resolved through the accountability mechanism.

This design is consistent with the privacy-preserving Sybil-free authentication principle investigated by Akil et al. [1].

3.8 Secure Session Establishment

After successful authentication and authorization, the driver and vehicle establish a protected communication session. A fresh session key can be generated using an authenticated key-establishment procedure. Subsequent communication is protected using the session key rather than repeatedly exposing long-term credentials.

Session protection provides confidentiality and integrity for sensitive messages such as vehicle-control requests, rental status, authorization updates, and service commands.

Fresh session parameters also help limit the consequences of credential compromise. If a previous session key is compromised, it should not automatically provide access to future sessions.

3.9 Credential Revocation and Misbehavior Handling

Credential revocation is essential when a credential is compromised, stolen, expired, or associated with malicious behavior. The framework therefore treats credentials as having a defined lifecycle rather than permanent validity.

A simplified lifecycle consists of:

Registration → Issuance → Activation → Validation → Monitoring → Expiration/Revocation

A revoked credential should no longer be accepted by rental providers, vehicles, RSUs, or other participating components. Revocation information can be distributed through the appropriate infrastructure, including edge, cloud, or distributed mechanisms where suitable.

For privacy protection, revocation information should avoid unnecessarily exposing the permanent identity of the affected driver.

Table 8. Credential Lifecycle Management

Lifecycle stage	Security action
Registration	Verify legitimate participant
Issuance	Generate controlled privacy-preserving credential
Activation	Associate credential with authorized rental service
Validation	Verify credential before access
Monitoring	Detect abnormal credential behavior
Suspension	Temporarily restrict suspicious credential
Revocation	Permanently invalidate compromised/malicious credential
Expiration	Automatically terminate time-limited credential
Accountability	Resolve identity only when authorized

3.10 Integrated Security Workflow

The proposed framework combines the mechanisms described above into a single workflow. First, a driver registers with the authentication infrastructure and receives a controlled privacy-preserving credential. When the driver wishes to



rent a vehicle, a rental request is submitted using the protected credential. The rental service verifies the credential and evaluates the driver's eligibility.

After successful authentication, zero-trust authorization determines whether the requested vehicle and operation are permitted. If authorization is granted, a secure session is established between the relevant entities. During the rental, security policies remain active and abnormal behavior can trigger additional verification or access restrictions.

At the end of the rental period, the temporary access authorization is terminated. If malicious activity is detected, the relevant credential can be revoked. In severe cases, the authorized accountability mechanism can resolve the pseudonymous identity.

The complete conceptual workflow is summarized in Table 11.

Table 9. Integrated Privacy-Preserving Zero-Trust Rental Workflow

Stage	Input	Security mechanism	Output
Registration	Driver identity	Identity verification	Registered participant
Credential issuance	Verified identity	Privacy-preserving credential generation	Pseudonymous credential
Rental request	Credential + rental request	Secure communication	Protected request
Authentication	Credential	Cryptographic verification	Authenticated requester
Authorization	Authenticated request	Zero-trust policy evaluation	Allow/Deny decision
Vehicle access	Authorized request	Access-control enforcement	Vehicle access
Session	Authorized driver and vehicle	Secure key establishment	Protected communication
Monitoring	Session activity	Policy/security monitoring	Normal or suspicious status
Misbehavior	Security violation	Revocation/accountability	Restricted or revoked access
Rental termination	End of rental	Credential/session termination	Closed rental session

As shown in Table 11, the framework is designed as an end-to-end security lifecycle rather than as a single authentication protocol. Privacy preservation protects legitimate drivers, zero-trust authorization restricts access, Sybil resistance controls pseudonymous credentials, and conditional accountability provides a mechanism for addressing serious violations.

The proposed architecture therefore addresses the principal research gap identified in Part 2 by combining these mechanisms within a common vehicle-rental environment. The next part evaluates the framework against major security threats and examines its computational, communication, and scalability characteristics.

4. Discussion and Future Scope

The proposed privacy-preserving and zero-trust framework combines secure authentication, pseudonymous identity management, Sybil resistance, conditional accountability, and zero-trust authorization for VANET-based vehicle renting. The preceding part described the principal security mechanisms and their expected behavior against common attacks. This part extends the analysis by discussing the practical implications of the framework, its limitations, deployment considerations, and future research directions.

4.1 Security Analysis

The proposed framework adopts a layered security strategy in which authentication, authorization, privacy, accountability, and attack resistance are treated as complementary mechanisms. This is necessary because a vehicle-



rental platform operates at the intersection of cyber and physical systems. A successful attack may therefore compromise not only information but also access to a physical vehicle.

The principal security properties are summarized in Table 12.

Table 10. Security Properties of the Proposed Framework

Security property	Mechanism	Expected protection
Authentication	Privacy-preserving credentials	Prevents unauthorized participants
Authorization	Zero-trust policy evaluation	Restricts access to permitted resources
Identity privacy	Pseudonymous credentials	Reduces driver identity exposure
Accountability	Conditional traceability	Enables investigation of serious violations
Sybil resistance	Controlled credential issuance	Limits multiple-identity abuse
Confidentiality	Secure session communication	Protects sensitive information
Integrity	Cryptographic verification	Detects message modification
Replay protection	Nonces/timestamps	Prevents reuse of old messages
Credential security	Lifecycle management	Limits credential misuse
Revocation	Credential invalidation	Removes compromised participants
Non-repudiation	Protected audit records	Supports dispute resolution
Least privilege	Policy-based access control	Limits excessive permissions

As indicated in Table 10, the framework does not depend on a single security mechanism. Instead, different mechanisms address different stages and threats within the rental lifecycle.

4.2 Resistance to Major Attacks

The framework is designed to resist common attacks targeting VANET authentication and connected vehicle services. An impersonation attacker cannot gain access merely by knowing a driver's pseudonymous identifier because successful authentication requires possession of the corresponding cryptographic credentials. Replay attacks are mitigated through fresh authentication parameters, while message integrity mechanisms prevent undetected modification of sensitive messages.

A man-in-the-middle attacker may observe wireless communication but cannot successfully establish a legitimate authenticated session without the required cryptographic credentials. Similarly, Sybil attacks are addressed through controlled credential issuance and credential-management policies.

Credential theft remains a potential threat. However, the impact of a compromised credential can be reduced through credential expiration, status verification, revocation, and zero-trust authorization. Therefore, even when an attacker obtains a valid credential, unrestricted access to the rental ecosystem is not automatically granted.

Table 11 presents the principal threats and corresponding countermeasures.

Table 11. Threats and Countermeasures

Threat	Potential consequence	Countermeasure
Impersonation	Unauthorized rental access	Cryptographic authentication
Replay attack	Reuse of previous authentication	Fresh nonces/timestamps
MITM attack	Communication manipulation	Authenticated secure sessions
Sybil attack	Multiple fraudulent identities	Controlled credentials
Credential theft	Account or vehicle misuse	Credential validation and revocation
Identity tracking	Loss of driver privacy	Pseudonymous credentials



Unauthorized access	Vehicle misuse	Zero-trust authorization
Insider attack	Privilege abuse	Least-privilege policies
Malicious behavior	Service disruption	Monitoring and accountability
Identity-resolution abuse	Privacy violation	Restricted tracing authority
Cloud/edge attack	Infrastructure compromise	End-to-end security controls

The mechanisms summarized in Table 13 demonstrate that privacy preservation is incorporated together with conventional security controls rather than being implemented at the expense of security.

4.3 Privacy–Accountability Balance

One of the most important design challenges is balancing driver privacy with accountability. A rental service that exposes the driver's permanent identity during every transaction creates unnecessary privacy risks. Conversely, a system that provides unrestricted anonymity may make it difficult to investigate serious incidents.

The proposed framework addresses this problem through conditional traceability. During routine operations, the driver uses a pseudonymous credential. The permanent identity is protected from ordinary communication participants. If predefined accountability conditions are satisfied, an authorized entity can initiate identity resolution.

This approach follows the privacy-accountability principle established in previous vehicle-renting research [2]. It also complements conditional privacy-preserving authentication mechanisms investigated in VANETs [13–19].

The objective is therefore not complete anonymity but controlled privacy. Legitimate drivers receive privacy during ordinary operations, while malicious behavior remains attributable under authorized conditions.

4.4 Zero-Trust Security Benefits

The zero-trust component provides an important distinction between authentication and trust. Traditional systems may treat successful authentication as sufficient evidence for granting access. The proposed framework instead treats authentication as one input into an authorization decision.

This provides several advantages. First, a compromised credential does not automatically provide access to every vehicle or service. Second, privileges can be limited according to the rental agreement. Third, sensitive operations can require additional verification. Fourth, access can be revoked when a credential becomes invalid or suspicious behavior is detected.

Recent work on zero-trust connected vehicles and automotive networks supports the applicability of continuous verification and least-privilege principles in automotive environments [3,30,31,33].

4.5 Performance Considerations

The framework introduces additional security operations compared with a basic identity-based authentication system. These include privacy-preserving credential verification, zero-trust authorization, credential-status checking, and optional accountability operations.

However, not all operations need to occur at the same computational cost. Routine authentication can use relatively lightweight cryptographic verification, while identity resolution and detailed forensic analysis can be performed only when required.

The principal performance dimensions are summarized in Table 12.



Table 12. Performance Considerations

Component	Main overhead	Performance strategy
Authentication	Credential verification	Efficient cryptographic primitives
Authorization	Policy evaluation	Lightweight policy processing
Session establishment	Key agreement	Fresh session keys
Communication	Authentication metadata	Compact credentials
Revocation	Credential-status checking	Efficient status distribution
Accountability	Identity-resolution processing	Event-driven execution
Auditability	Record generation	Store only necessary information
Edge/cloud support	Network processing	Distributed processing

The use of edge and fog infrastructure can further reduce the computational burden on vehicles. Fog-assisted authentication research has demonstrated the potential of distributed processing for improving vehicular security performance [22].

4.6 Scalability and Deployment Considerations

Scalability is critical because future rental ecosystems may include thousands or millions of connected vehicles and users. A centralized system that processes every authentication and authorization request through one authority could become a bottleneck.

The proposed architecture therefore supports distributed processing through RSUs, edge/fog nodes, and cloud infrastructure. Authentication and authorization functions can be distributed according to system requirements, while sensitive identity-resolution functions remain under stronger administrative control.

Blockchain may also be used selectively for auditing, revocation, or trust management. Existing blockchain-based VANET research demonstrates the potential of distributed ledgers for these functions [18,21–28]. Nevertheless, storing sensitive driver information directly on an immutable ledger should be avoided because immutability can conflict with privacy requirements.

4.7 Practical Deployment Challenges

Although the proposed framework provides a comprehensive security architecture, practical deployment presents several challenges.

First, interoperability must be achieved between rental providers, vehicle manufacturers, roadside infrastructure, cloud platforms, and authentication authorities. Second, credential-management mechanisms must support large numbers of vehicles without excessive communication overhead. Third, privacy regulations and data-governance requirements must be considered when implementing identity-resolution mechanisms.

Fourth, legacy vehicles may not support advanced cryptographic or zero-trust functions. Hybrid deployment strategies may therefore be required during the transition toward fully connected vehicle ecosystems.

Fifth, network connectivity may not always be available. Vehicles operating in areas with poor connectivity may need limited local verification capabilities while maintaining the overall zero-trust security model.



4.8 Limitations

The proposed framework is primarily a conceptual security architecture and therefore has several limitations.

First, the framework requires experimental validation using realistic VANET and vehicle-rental environments. Second, the exact computational overhead depends on the selected cryptographic primitives, hardware, communication technologies, and credential-management architecture. Third, conditional accountability assumes that the identity-management authority is adequately protected.

Fourth, Sybil resistance cannot necessarily depend on a single mechanism in every deployment scenario. Cryptographic controls may need to be complemented by behavioral or contextual detection. Fifth, the framework does not assume that zero-trust architecture completely eliminates attacks. Instead, its purpose is to reduce the consequences of compromised identities and prevent implicit trust from propagating through the system.

These limitations provide opportunities for future investigation.

4.9 Future Research Scope

Several research directions can extend the proposed framework.

First, formal protocol verification can be conducted using tools such as ProVerif, Tamarin, or automated security-analysis frameworks to mathematically evaluate authentication, privacy, and attack resistance.

Second, large-scale simulation can be performed using VANET simulators such as Veins, SUMO, or ns-3 to measure authentication latency, packet overhead, scalability, and behavior under different vehicle densities.

Third, privacy-preserving machine learning can be investigated to identify suspicious behavior without exposing sensitive driver information. This could strengthen Sybil detection and trust evaluation.

Fourth, blockchain or distributed-ledger mechanisms can be selectively integrated for credential revocation, accountability logs, and inter-provider trust management.

Fifth, post-quantum cryptography should be considered for long-term protection of connected vehicle credentials because future quantum computers may threaten widely deployed public-key cryptographic mechanisms.

Sixth, cross-provider vehicle renting represents an important future scenario. A driver may rent vehicles from different providers while retaining privacy and security. Federated authentication and interoperable privacy-preserving credentials could support this model.

Seventh, real-world testbed implementation should evaluate the framework using connected vehicles, RSUs, edge servers, and rental applications. Such experiments would provide evidence concerning practical latency, energy consumption, computational requirements, and user experience.

Table 13 summarizes the major future research directions.

Table 13. Future Research Directions

Research direction	Objective
Formal verification	Mathematically validate protocol security
VANET simulation	Evaluate latency and scalability
Real-world testbed	Validate practical deployment
Privacy-preserving AI	Detect malicious behavior without exposing identity



Advanced Sybil detection	Strengthen resistance against identity multiplication
Blockchain integration	Support distributed revocation and auditing
Post-quantum security	Protect long-term vehicular credentials
Cross-provider authentication	Enable secure multi-provider vehicle renting
Edge-assisted security	Reduce authentication latency
Adaptive zero-trust policies	Dynamically adjust access according to risk
Privacy-preserving analytics	Reduce tracking and profiling
Regulatory compliance	Align identity management with privacy regulations

4.10 Overall Discussion

The analysis demonstrates that secure vehicle renting requires more than conventional user authentication. The rental ecosystem combines physical vehicle access with sensitive digital identities and network communication. Therefore, a security breach can simultaneously affect privacy, service availability, financial transactions, and physical vehicle usage.

The proposed framework addresses this challenge through an integrated architecture. Privacy-preserving credentials reduce unnecessary identity disclosure, while controlled credential issuance limits Sybil behavior. Conditional traceability maintains accountability without requiring permanent identity exposure. Zero-trust authorization ensures that authenticated users receive only the privileges necessary for their rental activities.

The combined security model is summarized in Table 14.

Table 14. Overall Characteristics of the Proposed Framework

Characteristic	Proposed solution
Authentication	Privacy-preserving cryptographic credentials
Privacy	Pseudonymous identity management
Authorization	Zero-trust, least-privilege policies
Accountability	Conditional identity resolution
Sybil resistance	Controlled credential issuance
Session protection	Fresh secure session keys
Credential lifecycle	Validation, expiration, suspension, revocation
Attack protection	Multi-layer security controls
Scalability	Edge/cloud-supported architecture
Auditability	Protected security and rental records
Future extensibility	Blockchain, AI, and post-quantum integration

As indicated in Table 16, the principal contribution is the integration of security mechanisms that are frequently investigated independently. The framework does not assume that privacy can be achieved simply by removing identity information, nor that authentication automatically establishes trust. Instead, it treats privacy, authentication, authorization, accountability, and Sybil resistance as interconnected security objectives.

5. Conclusion

The increasing deployment of connected vehicles and intelligent transportation services has created significant opportunities for vehicle-rental platforms based on Vehicular Ad Hoc Networks. However, the openness and dynamic nature of VANET communication creates substantial security and privacy challenges. Vehicle-rental systems must simultaneously protect driver identities, authenticate legitimate users, restrict unauthorized vehicle access, prevent Sybil attacks, and retain mechanisms for accountability.



This paper presented a privacy-preserving and zero-trust framework for secure vehicle renting in VANETs. The framework combines pseudonymous authentication, controlled credential issuance, zero-trust authorization, conditional driver accountability, secure session establishment, credential revocation, and Sybil resistance. The design addresses an important limitation in existing approaches, where authentication, privacy, accountability, and trust are frequently treated as separate security problems.

The proposed approach uses privacy-preserving credentials to prevent unnecessary disclosure of drivers' permanent identities during normal rental operations. At the same time, controlled credential management reduces the ability of malicious users to exploit multiple pseudonyms for Sybil attacks. Conditional traceability provides a mechanism for identifying malicious participants when legitimate accountability requirements arise. The zero-trust component further ensures that successful authentication does not automatically result in unrestricted access.

The security analysis indicates that the integrated framework can provide protection against major threats, including impersonation, replay, man-in-the-middle, credential misuse, Sybil attacks, unauthorized access, and identity-tracking risks. The performance discussion also indicates that computational and communication overhead can be managed through lightweight cryptographic operations, efficient credential management, and distributed edge/cloud processing.

Nevertheless, practical implementation requires further evaluation. Formal security verification, large-scale VANET simulation, real-world testbed deployment, adaptive Sybil detection, privacy-preserving artificial intelligence, blockchain-assisted revocation, and post-quantum cryptography represent important future research directions. In particular, cross-provider vehicle renting and interoperable privacy-preserving credentials could enable secure and privacy-aware mobility services across different rental operators and transportation ecosystems.

Overall, the proposed framework provides a foundation for developing secure, privacy-aware, accountable, and zero-trust vehicle-rental services. By combining strong authentication with controlled privacy and continuous authorization, it offers a balanced security model suitable for the evolving requirements of connected and intelligent transportation systems.

References

- [1] Akil, M., Martucci, L. A., & Hoepman, J.-H. (2023). Non-interactive privacy-preserving Sybil-free authentication scheme in VANETs. In Inaugural International Symposium on Vehicle Security and Privacy (VehicleSec 2023). Internet Society. DOI: 10.14722/vehiclesec.2023.23007
- [2] Akil, M., Martucci, L. A., & Hoepman, J.-H. (2024). A secure and privacy-preserving authentication scheme with a zero-trust approach to vehicle renting in VANETs. In Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024) (pp. 114–127). SCITEPRESS. DOI: 10.5220/0012759600003767
- [3] Akil, M., Naskar, S., Martucci, L. A., & Hoepman, J.-H. (2023). A privacy-preserving approach to vehicle renting and driver accountability in VANETs. In Privacy and Identity Management. Sharing in a Digital World (pp. 192–210). Springer. DOI: 10.1007/978-3-031-57978-3_13
- [4] Akil, M., Mancini, L. V., & Venturi, D. (2019). Multi-covert channel attack in the cloud. In 2019 6th International Conference on Software Defined Systems (SDS) (pp. 160–165). IEEE. DOI: 10.1109/SDS.2019.8768563
- [5] Mundhe, P., Verma, S., & Venkatesan, S. (2021). A comprehensive survey on authentication and privacy-preserving schemes in VANETs. Computer Science Review, 41, 100411. DOI: 10.1016/j.cosrev.2021.100411.
- [6] Sutradhar, K., Pillai, B. G., Amin, R., & Narayan, D. L. (2024). A survey on privacy-preserving authentication protocols for secure vehicular communication. Computer Communications, 219, 1–18. DOI: 10.1016/j.comcom.2024.02.024.



- [7] Zhong, H., Han, S., Cui, J., Zhang, J., & Xu, Y. (2019). Privacy-preserving authentication scheme with full aggregation in VANET. *Information Sciences*, 476, 211–221. DOI: 10.1016/j.ins.2018.10.021.
- [8] Pournaghi, S. M., Zahednejad, B., Bayat, M., & Farjami, Y. (2018). NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Computer Networks*, 134, 78–92. DOI: 10.1016/j.comnet.2018.01.015.
- [9] Qi, J., Gao, T., Deng, X., & Zhao, C. (2022). A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs. *Vehicular Communications*, 38, 100535. DOI: 10.1016/j.vehcom.2022.100535.
- [10] Zhou, Y., Long, X., Chen, L., & Yang, Z. (2019). Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs. *Journal of Information Security and Applications*, 47, 295–301. DOI: 10.1016/j.jisa.2019.05.018.
- [11] Ali, I., & Li, F. (2020). An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. *Vehicular Communications*, 22, 100228. DOI: 10.1016/j.vehcom.2019.100228.
- [12] Ming, Y. (2019). Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. *Mobile Information Systems*, 2019, 7593138. DOI: 10.1155/2019/7593138.
- [13] He, D., Zeadally, S., Xu, B., & Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 10(12), 2681–2691. DOI: 10.1109/TIFS.2015.2473820.
- [14] Horng, S.-J., Tzeng, S.-F., Huang, P.-H., Wang, X., Li, T., & Khan, M. K. (2015). An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. *Information Sciences*, 317, 48–66. DOI: 10.1016/j.ins.2015.04.033.
- [15] Kamil, I. A., & Ogundoyin, S. O. (2020). On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network. *Security and Privacy*, 3, e104. DOI: 10.1002/spy2.104.
- [16] Lu, Z., Wang, Q., Qu, G., Zhang, H., & Liu, Z. (2019). A blockchain-based privacy-preserving authentication scheme for VANETs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12), 2792–2801. DOI: 10.1109/TVLSI.2019.2929420.
- [17] Feng, Q., He, D., Zeadally, S., & Liang, K. (2020). BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics*, 16(6), 4146–4155. DOI: 10.1109/TII.2019.2948053.
- [18] Ogundoyin, S. O., & Kamil, I. A. (2021). An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. *Vehicular Communications*, 31, 100384. DOI: 10.1016/j.vehcom.2021.100384.
- [19] Ahmed, W., & Di, W. (2022). Privacy-preserving blockchain-based authentication and trust management in VANETs. *IET Networks*, 11, 89–111. DOI: 10.1049/ntw2.12036.
- [20] Li, B., Liang, R., Zhu, D., Chen, W., & Lin, Q. (2021). Blockchain-based trust management model for location privacy preserving in VANET. *IEEE Transactions on Intelligent Transportation Systems*, 22(6), 3765–3775. DOI: 10.1109/TITS.2020.3035869.



- [21] Liu, H., Han, D., & Li, D. (2021). Behavior analysis and blockchain based trust management in VANETs. *Journal of Parallel and Distributed Computing*, 151, 61–69. DOI: 10.1016/j.jpdc.2021.02.011.
- [22] Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I., & Atiquzzaman, M. (2021). A scalable blockchain based trust management in VANET routing protocol. *Journal of Parallel and Distributed Computing*, 152, 144–156. DOI: 10.1016/j.jpdc.2021.02.024.
- [23] Ahmed, W., Di, W., & Mukathe, D. (2023). Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in VANETs. *Sensors*, 23(12), 5766. DOI: 10.3390/s23125766.
- [24] Tan, H., & Chung, I. (2020). Secure authentication and key management with blockchain in VANETs. *IEEE Access*, 8, 2482–2498. DOI: 10.1109/ACCESS.2019.2962387.
- [25] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2019). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*, 6(2), 1495–1505. DOI: 10.1109/JIOT.2018.2836144.
- [26] Liu, X., Huang, H., Xiao, F., & Ma, Z. (2020). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. *IEEE Internet of Things Journal*, 7. DOI: 10.1109/JIOT.2019.2957421.
- [27] Inedjaren, Y., Maachaoui, M., Zeddini, B., & Barbot, J.-P. (2021). Blockchain-based distributed management system for trust in VANET. *Vehicular Communications*, 30, 100350. DOI: 10.1016/j.vehcom.2021.100350.
- [28] Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. (2019). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, 6(3), 4660–4670. DOI: 10.1109/JIOT.2018.2875542.
- [29] Annabi, M., Zeroual, A., & Messai, N. (2024). Towards zero trust security in connected vehicles: A comprehensive survey. *Computers & Security*, 145, 104018. DOI: 10.1016/j.cose.2024.104018.
- [30] Shipman, M. E., Millwater, N., Owens, K., & Smith, S. (2024). A zero trust architecture for automotive networks. *SAE Technical Paper 2024-01-2793*. SAE International. DOI: 10.4271/2024-01-2793.
- [31] Roy, P. K., Kumar, P., & Bhattacharya, A. (2025). ZeroVCS: An efficient authentication protocol without trusted authority for zero-trust vehicular communication systems. *Future Generation Computer Systems*, 163, 107520. DOI: 10.1016/j.future.2024.107520.
- [32] Boualouache, A., Senouci, S. M., & Moussaoui, S. (2020). PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(8), 3209–3218. DOI: 10.1109/TITS.2019.2924856.
- [33] Xu, Z., He, D., Kumar, N., & Choo, K.-K. R. (2020). Efficient certificateless aggregate signature scheme for performing secure routing in VANETs. *Security and Communication Networks*, 2020, 5276813. DOI: 10.1155/2020/5276813.
- [34] Ali, I., Lawrence, T., & Li, F. (2020). An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs. *Journal of Systems Architecture*, 103, 101692. DOI: 10.1016/j.sysarc.2019.101692.
- [35] Qi, J., Gao, T., Deng, X., & Zhao, C. (2024). An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs. *Vehicular Communications*, 45, 100727. DOI: 10.1016/j.vehcom.2024.100727.



- [36] He, D., Zeadally, S., Xu, B., & Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 10(12), 2681–2691. DOI: 10.1109/TIFS.2015.2473820.
- [37] Khalid, A., Iftikhar, M. S., Almogren, A., Khalid, R., Afzal, M. K., & Javaid, N. (2021). A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs. *Information Processing & Management*, 58(2), 102464. DOI: 10.1016/j.ipm.2020.102464.
- [38] Hacen Diallo, E., Dib, O., & Al Agha, K. (2022). A scalable blockchain-based scheme for traffic-related data sharing in VANETs. *Blockchain: Research and Applications*, 3. DOI: 10.1016/j.bcra.2022.100087.
- [39] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., Panigrahi, B., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, 80, 103352. DOI: 10.1016/j.micpro.2020.103352.
- [40] Raya, M., & Hubaux, J.-P. (2006). Securing vehicular communications. *IEEE Wireless Communications*, 13(5), 8–15. DOI: 10.1109/WC-M.2006.250352.
- [41] Papadimitratos, P., Buttyán, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., & Hubaux, J.-P. (2008). Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine*, 46(11), 100–109. DOI: 10.1109/MCOM.2008.4689252.