



# Privacy-Preserving Security in Vehicular Networks: A Review of Authentication, Vehicle Renting, and Driver Accountability

**Madhab Chandra Jena, Tamal Paul, Om Krishna Jena**

GIFT Autonomous, Bhubaneswar, Odisha, India, [madhab\\_jena@rediffmail.com](mailto:madhab_jena@rediffmail.com)

GIFT Autonomous, Bhubaneswar, Odisha, India, [tamalpaul@gift.edu.in](mailto:tamalpaul@gift.edu.in)

CIPET, Bhubaneswar, Odisha, India. [omkrishnajena2007@gmail.com](mailto:omkrishnajena2007@gmail.com)

## How to Cite this Article:

Jena, M. C., Paul, T. & Jena, O. K. (2026). Privacy-Preserving Security in Vehicular Networks: A Review of Authentication, Vehicle Renting, and Driver Accountability. International Journal of Creative and Open Research in Engineering and Management, <i>02</i></i>(10), 1-9.  
<https://doi.org/10.55041/ijcope.v2i10.015>

## 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.v2i10.015>

## Abstract

Vehicular Ad Hoc Networks (VANETs) are an important component of intelligent transportation systems, enabling real-time communication among vehicles, roadside infrastructure, and transportation services. However, the open and highly dynamic nature of VANETs creates significant security and privacy challenges, including impersonation, Sybil attacks, identity disclosure, pseudonym misuse, unauthorized access, and difficulties in maintaining accountability. These challenges become more complex in vehicle-rental environments, where temporary drivers must be authenticated and authorized without unnecessarily exposing their permanent identities. This review presents a comprehensive analysis of 40 studies on secure and privacy-preserving vehicular communication, with particular emphasis on authentication, conditional privacy, pseudonym management, Sybil resistance, driver accountability, blockchain-assisted security, revocation, and zero-trust authentication. Four closely related studies on privacy-preserving Sybil-free authentication, secure vehicle renting using a zero-trust approach, privacy-preserving vehicle renting with driver accountability, and covert-channel security are examined as central contributions to the research domain. The review shows that conventional authentication mechanisms provide strong identity verification but may expose sensitive user information, whereas pseudonyms, anonymous credentials, conditional privacy-preserving authentication, and zero-knowledge techniques provide

stronger privacy while retaining controlled accountability. Blockchain-based and trust-management approaches further address distributed authentication and revocation but introduce additional computational, communication, and scalability considerations. The analysis identifies a significant research gap in integrating privacy-preserving rental authorization, Sybil resistance, temporary credential management, conditional accountability, efficient revocation, and zero-trust principles within a unified VANET framework. Future research should therefore focus on lightweight anonymous credentials, zero-knowledge-based authorization, rental-session-bound pseudonyms, privacy-preserving accountability, and scalable decentralized revocation mechanisms. Such an integrated approach can support secure and privacy-aware vehicle sharing and rental services while maintaining the authentication and accountability requirements of intelligent transportation systems.



## 1. Introduction

Vehicular Ad Hoc Networks (VANETs) enable vehicles to exchange information with neighboring vehicles, roadside infrastructure and other components of intelligent transportation systems. Such communication can support applications including collision avoidance, traffic management, emergency warning, cooperative driving and infotainment. Because decisions may depend on information received from other vehicles, establishing the authenticity and integrity of vehicular messages is a fundamental security requirement.

At the same time, vehicular communication exposes sensitive information. A vehicle's communication messages may reveal its identity, location, movement pattern, driving behavior and association with particular infrastructure. Consequently, a security mechanism that provides authentication by directly exposing the long-term identity of a vehicle can create significant privacy risks. Research on VANET security has therefore increasingly concentrated on conditional privacy-preserving authentication, where ordinary communication is anonymous or pseudonymous while an authorized entity can recover the real identity of a malicious participant when accountability is required [5]–[15].

Early authentication approaches mainly concentrated on establishing whether a message originated from a legitimate vehicle. Pseudonyms, group signatures, identity-based cryptography and certificateless mechanisms subsequently became important approaches for separating authentication from direct identity disclosure [6]–[18]. However, the deployment of large numbers of pseudonyms introduces storage, certificate-management and revocation challenges. Furthermore, malicious vehicles can exploit anonymous identities to launch Sybil attacks by creating or controlling multiple apparent identities [14], [25].

Blockchain-based approaches have subsequently been investigated to distribute authentication and revocation functions and reduce dependence on a centralized trusted authority [22], [23], [32]–[35]. Other studies have explored trust management, fog computing, batch verification and efficient revocation mechanisms to improve the scalability of vehicular security [17], [19], [28], [29], [36].

A particularly important development is the extension of VANET privacy research from ordinary vehicle communication to vehicle-rental scenarios. Vehicle renting changes the security model because the driver temporarily obtains access to a vehicle that may be owned by another party. Thus, the system must establish that the renter is authorized to use the vehicle while avoiding unnecessary disclosure of the renter's long-term identity. At the same time, the system should preserve accountability if the vehicle or communication credentials are abused.

Akil, Martucci and Hoepman addressed this problem through privacy-preserving vehicle-rental research. Their work on Sybil-free authentication considers privacy-preserving authentication while preventing users from creating multiple identities [1]. Their subsequent work introduced a secure and privacy-preserving authentication scheme using a zero-trust approach to vehicle renting, incorporating zero-knowledge proofs and delegatable anonymous credentials [2]. Related work considered privacy-preserving vehicle renting and driver accountability [3]. These studies are particularly relevant because they move the research problem beyond conventional VANET authentication toward temporary authorization, renter privacy and accountability.

The objective of this review is therefore to examine the development of privacy-preserving VANET authentication and identify how existing mechanisms address the specific requirements of secure vehicle renting. The review focuses on six major questions:

1. How have privacy-preserving authentication mechanisms evolved in VANETs?
2. How are pseudonyms and anonymous credentials used to protect vehicle and user identity?
3. How do existing schemes address Sybil attacks and malicious-user revocation?
4. How can accountability be achieved without eliminating privacy?
5. What role do blockchain, trust management and zero-knowledge mechanisms play?
6. What research gaps remain for secure and privacy-preserving vehicle-rental systems?



The remainder of the paper is organized into five major sections. Section 2 reviews the literature according to major technological themes. Section 3 analyzes privacy-preserving authentication mechanisms. Section 4 focuses on vehicle renting, Sybil resistance, accountability and zero-trust security. Section 5 provides a comparative analysis and identifies research gaps and future directions. Section 6 concludes the review.

## 2. Literature Review

### 2.1 Evolution of VANET Authentication

The earliest VANET security research established the need to protect vehicular communication against impersonation, message manipulation and unauthorized participation. Raya, Papadimitratos and Hubaux emphasized the importance of securing vehicular communications while preserving the privacy of legitimate participants [40]. Subsequent work introduced increasingly sophisticated authentication mechanisms designed specifically for the highly dynamic VANET environment.

Traditional public-key infrastructures provide a straightforward mechanism for authenticating vehicles, but direct use of long-term certificates can allow vehicles to be tracked. Consequently, pseudonym-based authentication became a major research direction. Sun et al. proposed an efficient pseudonymous authentication mechanism designed to preserve privacy in vehicular communication [6]. Other approaches employed identity-based cryptography, anonymous credentials, group signatures and certificateless authentication [5], [7]–[13].

Conditional privacy became an important design objective. Under conditional privacy, an ordinary observer should not be able to determine the real identity of a communicating vehicle, while an authorized entity should retain the ability to identify a malicious participant. This creates a balance between anonymity and accountability.

He et al. developed an identity-based conditional privacy-preserving authentication scheme for VANETs [5]. Azees et al. proposed efficient anonymous authentication with conditional privacy preservation [10]. Other schemes subsequently investigated batch authentication, lightweight cryptography and efficient certificate management [8], [13], [15], [17].

The literature therefore shows a gradual transformation from simple identity authentication toward a multi-objective security model involving authentication, anonymity, unlinkability, traceability and revocation.

### 2.2 Pseudonym-Based Privacy Preservation

Pseudonyms replace a vehicle's long-term identity with temporary identifiers. When pseudonyms are changed appropriately, an external observer has greater difficulty linking messages to the same vehicle.

Sun et al. investigated pseudonymous authentication with strong privacy preservation [6]. Other research developed pseudonym-based certificateless authentication mechanisms to avoid some limitations associated with conventional certificate management [21]. The pseudonym-based certificateless approach combines pseudonyms with certificateless signatures and provides mechanisms for vehicle revocation and identity tracing [21].

Pseudonym systems, however, create a fundamental trade-off. Increasing the frequency of pseudonym changes may improve unlinkability, but it also increases credential-management requirements. If pseudonyms are centrally issued and stored, the system may require substantial storage and communication resources. Large-scale revocation also becomes difficult.

Qi et al. investigated privacy-preserving authentication together with pseudonym revocation and used mechanisms such as compressed revocation information to improve efficiency [11]. Scalable revocation was further studied through efficient key-update mechanisms, reducing the computational burden associated with revoking malicious vehicles [28].



Thus, pseudonyms provide an important privacy mechanism but do not independently solve the complete security problem. A practical system must additionally control pseudonym issuance, prevent identity multiplication, support revocation and preserve accountability.

### 2.3 Conditional Privacy and Accountability

Conditional privacy represents a central concept in VANET security. The objective is not unrestricted anonymity. Instead, legitimate vehicles should communicate without exposing their permanent identities, while authorized investigation should remain possible when malicious behavior occurs.

The literature contains several approaches for implementing this principle. Identity-based schemes can associate pseudonymous credentials with an underlying identity managed by a trusted authority [5]. Group-signature approaches can allow members to authenticate anonymously while supporting controlled identity opening. Pseudonym-based systems can allow authorized entities to associate pseudonyms with registered vehicles [10], [11].

However, the centralized authority introduces another challenge. If the trusted authority becomes compromised, overloaded or overly powerful, the privacy guarantees of the entire system can be weakened. Su et al. specifically examined approaches for reducing dependency on the trusted authority and proposed a privacy-preserving mechanism that limits the information visible to the authority [20].

This issue is particularly important in vehicle-rental environments. A rental service provider may know the real identity of a renter for contractual purposes, while VANET communication does not necessarily require the vehicle's surrounding participants to know that identity. Therefore, the rental ecosystem should distinguish between contractual identity and communication identity.

### 2.4 Sybil Attacks in VANETs

A Sybil attack occurs when a malicious participant presents multiple identities in order to appear as multiple independent entities. In VANETs, this threat can have particularly serious consequences because traffic decisions may depend on the apparent number of vehicles reporting an event.

For example, if one malicious vehicle creates several pseudonymous identities and uses them to report the same false event, neighboring vehicles may interpret the multiple messages as independent evidence. Consequently, anonymity mechanisms must not inadvertently provide unlimited identity creation capability.

Akil et al. directly addressed this issue through a non-interactive privacy-preserving Sybil-free authentication scheme [1]. This work is highly relevant because it demonstrates that privacy and Sybil resistance do not necessarily have to be treated as mutually exclusive objectives. Instead, a system can attempt to prove that a participant possesses the necessary authorization without unnecessarily exposing the participant's permanent identity.

Trajectory-based authentication has also been investigated as a mechanism for detecting or limiting Sybil behavior [14]. Other authentication systems rely on controlled pseudonym generation, credential management and trusted infrastructure to limit the number of identities associated with a legitimate participant.

A major research challenge therefore lies in designing credentials that provide unlinkability during normal operation while simultaneously preventing one participant from obtaining unlimited valid identities.

### 2.5 Blockchain-Based Authentication

Blockchain technology has been investigated as a mechanism for distributing authentication information and reducing reliance on a single centralized authority. Blockchain-based schemes can maintain tamper-resistant records of certificates, pseudonyms, revocation information or trust relationships [22], [23], [32]–[35].



Feng et al. proposed a blockchain-assisted privacy-preserving authentication system for VANETs [34]. Other work introduced blockchain-based conditional privacy-preserving authentication [22], [23]. Blockchain mechanisms can improve transparency and resistance to unilateral manipulation, but they also introduce computational, communication and latency costs.

The scalability issue is particularly important because VANETs may generate a large number of authentication events. If every vehicular message requires interaction with a blockchain network, the resulting latency may be unsuitable for safety-critical applications.

Recent approaches have therefore investigated lightweight blockchain participation, cross-domain authentication and alternative mechanisms for efficient revocation [32], [33]. Blockchain can be particularly useful for vehicle-rental systems when it is employed selectively—for example, to maintain authorization or revocation state rather than to process every safety message.

## **2.6 Trust Management and Distributed Authentication**

Authentication establishes whether a participant possesses a valid credential, but it does not necessarily establish whether the participant is behaving correctly. This distinction motivates trust-management approaches.

Trust-based VANET schemes attempt to evaluate participant behavior using communication history, message consistency or contextual information [29], [36]. Trust can complement cryptographic authentication by identifying participants that repeatedly generate false or suspicious information.

However, trust mechanisms must themselves preserve privacy. If detailed behavioral histories are associated permanently with a driver's identity, the system may create a new privacy risk. Therefore, future architectures should consider privacy-preserving reputation and trust mechanisms in which behavioral evidence can be evaluated without exposing unnecessary personal information.

## **2.7 Anonymous Authentication and Lightweight Mechanisms**

Vehicular systems have strict latency requirements. Authentication mechanisms must therefore be sufficiently efficient to support large numbers of vehicles and frequent message exchanges.

Batch authentication has been explored to allow multiple signatures or messages to be verified more efficiently [8], [15]. Lightweight conditional privacy-preserving mechanisms have also been proposed [13]. Other research has focused on reducing bilinear pairing operations, certificate-management overhead and communication rounds [17], [20], [28].

The literature demonstrates that there is no single universally optimal cryptographic mechanism. A scheme suitable for routine safety messages may not be directly suitable for rental authorization. Rental authorization can tolerate a more sophisticated initial authentication process because it is performed less frequently than safety-message verification. This observation creates an opportunity to use different security layers for different functions.

## **3. Privacy-Preserving Authentication for Vehicle Renting**

### **3.1 Why Vehicle Renting Changes the Security Problem**

Conventional VANET authentication generally assumes that the vehicle and its registered owner are closely related. Vehicle renting breaks this assumption.

In a rental scenario, at least four identities may exist:

- vehicle owner;



- rental service provider;
- temporary renter or driver;
- VANET communication identity.

These identities should not necessarily be exposed to one another during every communication event.

For example, a neighboring vehicle does not need to know the renter's name simply to verify that an emergency warning originated from a legitimate participant. Similarly, a rental service may need to know the renter's contractual identity without exposing that identity to other vehicles.

Therefore, vehicle-rental security requires separation between identity, authentication and authorization.

### 3.2 Privacy-Preserving Vehicle Renting

Akil et al. proposed a privacy-preserving approach to vehicle renting and driver accountability in VANETs [3]. This contribution extends VANET privacy beyond conventional vehicle authentication by considering the relationship between a rental user and a vehicle.

The problem becomes more complex because the vehicle's communication credentials may need to change when the renter changes. A credential issued to the permanent owner should not automatically imply that the owner is responsible for every message generated during a rental period.

This motivates session-oriented authorization. A rental credential can be associated with:

- a particular vehicle;
- a specific renter;
- a defined rental period;
- a set of permitted functions;
- a controlled pseudonym;
- a revocation status.

Such binding can provide a stronger relationship between authorization and accountability while avoiding disclosure of the renter's identity during ordinary communication.

### 3.3 Zero-Trust Authentication for Vehicle Renting

The zero-trust approach proposed by Akil, Martucci and Hoepman represents an important evolution in VANET security research [2]. Rather than assuming that successful initial authentication establishes permanent trust, the approach treats authorization as something that must be explicitly established and verified.

The work incorporates zero-knowledge proofs and delegatable anonymous credentials [2]. These technologies are relevant because they allow a participant to demonstrate possession of an appropriate credential without necessarily revealing all information contained in that credential.

This is particularly suitable for vehicle rental. A renter may need to prove:

- that the renter is authorized to use the vehicle;
- that the authorization is currently valid;
- that the credential has not been revoked;
- that the renter possesses the required permissions;

without necessarily disclosing the renter's complete identity to every VANET participant.



This principle represents a significant conceptual shift from identity-centric security toward claim-based authorization.

### 3.4 Delegatable Anonymous Credentials

Anonymous credentials allow users to demonstrate authorization without directly revealing identifying information. Delegatable credentials further allow an authorized entity to derive or delegate a restricted authorization to another participant.

In a rental environment, this creates a natural hierarchy:

Rental provider → authorized renter → temporary VANET credential.

The rental provider can issue a credential containing appropriate restrictions without transferring unnecessary information to other VANET participants.

The approach is particularly useful when rental permissions vary. For example, a credential can be restricted according to rental duration, vehicle category or permitted operations.

### 3.5 Zero-Knowledge Proofs

Zero-knowledge proofs provide a cryptographic mechanism through which one participant can prove knowledge of a secret or possession of a valid credential without revealing the underlying secret.

Their relevance to vehicle renting is significant. Instead of communicating a driver's complete identity, a vehicle or VANET infrastructure can verify a statement such as:

"The current participant possesses a valid rental authorization for this vehicle and this authorization has not expired."

The verifier does not necessarily need to learn the renter's complete identity.

The zero-trust vehicle-rental scheme proposed by Akil et al. specifically incorporates zero-knowledge proofs for this purpose [2]. This represents a promising direction because it aligns authentication with the principle of minimum information disclosure.

## 4. Comparative Analysis

Table 1 summarizes the major security objectives addressed by the reviewed literature.

**Table 1. Major security objectives in the reviewed literature**

| Security objective        | Representative references   | Main approach                                                         |
|---------------------------|-----------------------------|-----------------------------------------------------------------------|
| Vehicle authentication    | [5], [6], [8], [10]         | Public-key, identity-based and anonymous authentication               |
| Conditional privacy       | [5], [10], [13], [21], [25] | Pseudonyms, anonymous credentials and conditional identity resolution |
| Pseudonym management      | [6], [11], [21], [28]       | Dynamic pseudonyms and efficient revocation                           |
| Sybil resistance          | [1], [14], [25]             | Controlled identity generation and Sybil-resistant credentials        |
| Driver accountability     | [3]                         | Privacy-preserving identity resolution                                |
| Vehicle-rental privacy    | [2], [3]                    | Anonymous credentials and rental-specific authorization               |
| Zero-trust authentication | [2]                         | Continuous/explicit authorization and zero-knowledge mechanisms       |



|                           |                              |                                                         |
|---------------------------|------------------------------|---------------------------------------------------------|
| Blockchain authentication | [22], [23], [32]–[35]        | Distributed authentication and revocation               |
| Trust management          | [29], [36]                   | Behavioral and reputation-based mechanisms              |
| Efficient revocation      | [11], [12], [28], [32], [33] | CRLs, key updates and blockchain-assisted mechanisms    |
| Batch verification        | [8], [13], [15], [28]        | Aggregated or batch cryptographic verification          |
| Reduced TA dependency     | [20]                         | Privacy-preserving interaction with trusted authorities |

The comparison shows that individual mechanisms generally address specific security dimensions. However, relatively few approaches simultaneously consider privacy, Sybil resistance, rental authorization and driver accountability.

**Table 2. Comparison of major authentication approaches**

| Approach                         | Privacy         | Accountability                                 | Sybil resistance                               | Revocation | Main limitation                                                         |
|----------------------------------|-----------------|------------------------------------------------|------------------------------------------------|------------|-------------------------------------------------------------------------|
| Conventional PKI                 | Low to moderate | High                                           | Moderate                                       | High       | Identity exposure and certificate management                            |
| Pseudonym authentication         | High            | Moderate                                       | Limited unless controlled                      | Moderate   | Pseudonym management                                                    |
| Group signatures                 | High            | High                                           | Moderate                                       | Complex    | Computational and revocation overhead                                   |
| Identity-based CPPA              | High            | High                                           | Moderate                                       | Moderate   | Trusted-authority dependency                                            |
| Certificateless authentication   | High            | High                                           | Moderate                                       | High       | Key-management complexity                                               |
| Blockchain authentication        | High            | High                                           | Potentially high                               | High       | Latency and blockchain overhead                                         |
| Trust-based authentication       | Variable        | Moderate                                       | Potentially high                               | Moderate   | Trust computation and privacy concerns                                  |
| Anonymous credentials            | Very high       | High if traceability exists                    | High when issuance is controlled               | High       | Credential-management complexity                                        |
| Zero-knowledge authentication    | Very high       | High if accountability is separately supported | High when combined with controlled credentials | High       | Proof-generation and verification overhead                              |
| Zero-trust rental authentication | Very high       | High                                           | High                                           | High       | Requires integrated credential, rental and authorization infrastructure |

#### 4.1 Analysis of the Four Compulsory Contributions

The four compulsory references occupy different but complementary positions in the research landscape.

Akil et al. [1] concentrate on privacy-preserving Sybil-free authentication. The principal contribution is the combination of privacy protection with resistance to multiple-identity abuse.

Akil et al. [2] extend the security problem to vehicle renting and introduce a zero-trust approach using zero-knowledge proofs and delegatable anonymous credentials. This moves the research focus from vehicle-level authentication toward dynamic authorization.



Akil et al. [3] specifically investigate privacy-preserving vehicle renting and driver accountability. The contribution is important because rental arrangements require responsibility to be associated with the appropriate temporary user rather than automatically with the permanent vehicle owner.

Akil, Mancini and Venturi [4] examine multi-covert-channel attacks in cloud environments. Although this work is not directly focused on VANETs, it contributes to the broader security context by demonstrating the importance of considering information leakage and covert communication channels in distributed computing environments.

Together, these four works provide a foundation for viewing vehicular security as a broader privacy and accountability problem rather than simply a message-authentication problem.

## **5. Research Gaps**

### **5.1 Lack of Unified Vehicle-Rental Security Models**

Most VANET authentication studies assume permanent or semi-permanent association between a vehicle and its credentials. Rental scenarios introduce temporary users, changing authorization and multiple stakeholders.

A comprehensive framework should explicitly represent the relationships among vehicle owner, rental provider, renter, vehicle and VANET infrastructure.

### **5.2 Privacy and Accountability Remain Difficult to Balance**

Complete anonymity can make malicious-user investigation difficult, whereas unrestricted identity disclosure undermines privacy.

Conditional accountability provides a potential solution, but identity resolution should be strongly controlled. Future systems should specify:

- who can resolve an identity;
- under what conditions resolution is permitted;
- what evidence is required;
- how identity-resolution requests are audited;
- how misuse of the resolution capability is prevented.

### **5.3 Sybil Resistance Requires Controlled Credential Issuance**

Dynamic pseudonyms improve privacy but can create opportunities for identity multiplication.

The work in [1] demonstrates the importance of explicitly addressing Sybil resistance. Future rental systems should bind the number and validity of pseudonymous credentials to an underlying authorization without revealing that underlying identity during normal communication.

### **5.4 Trusted Authority Dependency**

A significant portion of VANET authentication research relies on a trusted authority. However, excessive dependence on a centralized authority can introduce availability, privacy and security concerns [20].

Future systems should consider distributed or privacy-preserving authority interaction. Blockchain may assist in selected functions, but complete dependence on blockchain for real-time safety communication could create unnecessary latency.



## 5.5 Revocation Scalability

Revocation is one of the most persistent problems in privacy-preserving VANET authentication. Large certificate-revocation lists can impose substantial storage and verification costs. Recent work has investigated compressed revocation information, efficient key updates and blockchain-based approaches [11], [28], [32]–[35].

Rental environments introduce an additional dimension because authorization may expire naturally at the end of a rental period. Therefore, time-bounded credentials could reduce the need for explicit revocation in some circumstances.

## 5.6 Authentication Does Not Equal Authorization

Traditional VANET authentication primarily answers:

"Is this participant legitimate?"

A vehicle-rental system must additionally answer:

"Is this participant authorized to use this particular vehicle for this particular purpose at this particular time?"

The distinction is fundamental. Authentication can establish credential validity, while authorization should determine whether the current action is permitted.

The zero-trust approach in [2] provides an important basis for this separation.

## 5.7 Limited Integration of Context

Future systems could incorporate contextual authorization based on:

- rental duration;
- geographic region;
- vehicle type;
- communication service;
- emergency status;
- driver authorization;
- credential validity;
- revocation state.

However, context should be used carefully because excessive context collection can itself become a privacy threat.

## 6. Future Research Directions

### 6.1 Privacy-Preserving Zero-Trust Architecture

A future architecture should combine zero-trust principles with anonymous credentials. Every authorization request should be evaluated based on the current security context rather than assuming that previous authentication creates permanent trust.

A possible architecture consists of:

Vehicle → Anonymous Credential → Zero-Knowledge Proof → Authorization Engine → VANET Service

The vehicle demonstrates eligibility without revealing unnecessary identity information.



## 6.2 Rental-Session-Bound Credentials

Rental credentials should be explicitly associated with a rental session. The credential can contain cryptographic commitments to:

- vehicle identity;
- rental session;
- authorization period;
- permitted operations;
- credential status.

This prevents an authorization obtained for one rental session from being reused indefinitely.

## 6.3 Sybil-Resistant Anonymous Credentials

The concepts developed in [1] and [2] can be combined by constructing credentials that provide both anonymity and controlled uniqueness.

A user should be able to generate multiple pseudonyms over time for privacy but should not be able to create multiple simultaneously valid identities for the same security context.

## 6.4 Selective Disclosure

Future systems should adopt selective-disclosure principles in which only the minimum information required for a transaction is disclosed.

For example, a system might verify that:

- the renter is authorized;
- the rental has not expired;
- the vehicle is permitted;
- the credential has not been revoked;

without disclosing the renter's name.

## 6.5 Blockchain-Assisted Revocation Rather Than Blockchain-Dependent Communication

Blockchain should preferably be used for functions where its immutable and distributed properties provide a clear benefit, such as:

- credential status;
- revocation;
- audit records;
- inter-organizational authorization;
- dispute resolution.

Safety messages should not necessarily require blockchain confirmation for every transmission.

## 6.6 Privacy-Preserving Driver Accountability

Accountability mechanisms should be activated only under clearly defined conditions. An authorized investigator may be permitted to resolve a pseudonymous credential following a verified security incident.



A future system should therefore distinguish:

Normal communication → anonymous

Security investigation → conditionally identifiable

Unauthorized identity resolution → prevented and auditable

### **6.7 Lightweight Cryptographic Implementation**

Although zero-knowledge proofs and anonymous credentials provide strong privacy properties, computational and communication overhead must be considered. Future research should investigate lightweight proof systems and hardware-assisted cryptographic operations suitable for automotive platforms.

### **6.8 Integration with 5G/6G and Edge Computing**

Future intelligent transportation systems will increasingly rely on edge computing and advanced cellular connectivity. Rental authorization and credential verification could be delegated to edge nodes while preserving end-to-end privacy.

However, edge nodes should not automatically receive the renter's permanent identity. Privacy-preserving edge authorization therefore represents another important research direction.

### **6.9 Standardized Security and Evaluation Metrics**

Future studies should evaluate schemes using a common set of metrics:

- authentication latency;
- proof-generation time;
- verification time;
- communication overhead;
- storage requirements;
- pseudonym generation cost;
- revocation latency;
- Sybil-resistance capability;
- unlinkability;
- traceability;
- false-positive and false-negative rates;
- scalability;
- rental-session establishment time.

A standardized evaluation framework would make comparisons among proposed VANET authentication schemes more meaningful.

## **7. Proposed Conceptual Framework for Secure Vehicle Renting**

Based on the reviewed literature, a comprehensive privacy-preserving vehicle-rental architecture can be organized into seven logical layers.

### **Layer 1: Registration**

The renter and vehicle are registered with an appropriate authority or rental provider. The renter's real identity is maintained separately from the VANET communication identity.



## **Layer 2: Credential Issuance**

The rental provider issues an anonymous or pseudonymous rental credential containing the necessary authorization attributes.

## **Layer 3: Rental Session Establishment**

A cryptographic association is created between the renter, vehicle and rental session. The association is time-limited.

## **Layer 4: Privacy-Preserving Authentication**

The renter demonstrates possession of a valid credential without directly exposing the permanent identity.

## **Layer 5: Zero-Trust Authorization**

Each sensitive operation is evaluated against the current authorization state. Previous successful authentication does not automatically imply unrestricted future access.

## **Layer 6: Sybil Protection**

The system ensures that a renter cannot create unlimited simultaneously valid identities. Controlled pseudonym issuance and cryptographic uniqueness mechanisms can be employed.

## **Layer 7: Conditional Accountability**

If a serious security violation occurs, an authorized entity can resolve the relevant credential subject to predefined rules and evidence requirements.

This architecture combines the major concepts identified throughout the literature and particularly reflects the research direction represented by [1]–[3].

## **8. Discussion**

The reviewed literature demonstrates that VANET authentication has evolved considerably. Early research focused mainly on secure message authentication and vehicular PKI [40]. Privacy-preserving approaches subsequently introduced pseudonyms, identity-based cryptography and anonymous authentication [5]–[10]. Later studies concentrated on revocation, batch verification, reduced trusted-authority dependence and improved scalability [11]–[21], [28].

Blockchain introduced another direction by distributing authentication and revocation information [22], [23], [32]–[35]. Trust-management research extended security beyond cryptographic identity toward behavioral assessment [29], [36].

However, vehicle renting creates a distinct security problem. A renter is neither simply an anonymous VANET participant nor necessarily the permanent identity associated with the vehicle. The security system must therefore distinguish among ownership, temporary authorization, communication identity and accountability.

The contributions of Akil et al. [1]–[3] are particularly important in this context. The Sybil-free authentication work [1] addresses the risk that privacy mechanisms can be exploited to create multiple identities. The vehicle-rental and accountability work [3] addresses the relationship between temporary drivers and privacy-preserving communication. The zero-trust rental authentication work [2] extends these concepts through anonymous credentials and zero-knowledge mechanisms.



These contributions suggest that future VANET security should increasingly move from "authenticate the vehicle" toward "authenticate the authorization claim while protecting the participant's identity."

This distinction is especially important for shared mobility. As vehicle ownership becomes increasingly separated from vehicle use through rental, leasing, car sharing and mobility-as-a-service platforms, identity-centric security architectures may become less suitable.

The literature also suggests that privacy should not be treated as a secondary feature. Privacy must be integrated into the authentication architecture from the beginning. Pseudonymization, anonymous credentials, zero-knowledge proofs and selective disclosure can provide different mechanisms for minimizing identity exposure.

At the same time, privacy mechanisms must not eliminate accountability. A secure architecture should provide controlled identity resolution under predefined conditions. Such a design allows normal users to communicate privately while enabling investigation of serious misuse.

## 9. Conclusion

This review analyzed 40 studies addressing authentication, privacy, Sybil resistance, revocation, trust management, blockchain and secure vehicle communication in VANETs, with particular emphasis on privacy-preserving vehicle renting.

The literature demonstrates a clear evolution from conventional vehicle authentication toward conditional privacy-preserving authentication and more sophisticated identity-management mechanisms. Pseudonyms provide an important basis for unlinkability, while identity-based, certificateless and anonymous authentication mechanisms improve the balance between authentication and privacy. Blockchain-based systems provide potential solutions for distributed authentication and revocation, while trust-management mechanisms can supplement cryptographic authentication with behavioral evaluation.

The most significant research development for vehicle-rental environments is the movement toward privacy-preserving authorization rather than simple vehicle authentication. The compulsory works by Akil, Martucci, Hoepman and collaborators [1]–[3] demonstrate this transition through Sybil-free authentication, privacy-preserving vehicle renting, driver accountability, zero-trust authorization, zero-knowledge proofs and delegatable anonymous credentials.

The review identifies several unresolved challenges, including controlled pseudonym issuance, scalable revocation, reduced trusted-authority dependency, privacy-preserving accountability and the integration of authentication with temporary rental authorization. A promising future architecture should therefore combine anonymous credentials, zero-knowledge proofs, controlled pseudonyms, zero-trust authorization, conditional accountability and efficient revocation.

Ultimately, the security requirements of future intelligent transportation systems will extend beyond proving that a vehicle is legitimate. Secure mobility systems must also determine whether a participant is authorized to perform a particular action while minimizing unnecessary disclosure of identity. Privacy-preserving zero-trust vehicle renting represents an important research direction toward achieving this objective.

## 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] 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
- [6] Sun, Y., Lu, R., Lin, X., Shen, X., & Su, J. (2010). An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Transactions on Vehicular Technology*, 59(7), 3589–3603. DOI: 10.1109/TVT.2010.2051468
- [7] Wang, S., & Yao, N. (2017). LIAP: A local identity-based anonymous message authentication protocol in VANETs. *Computer Communications*, 112, 154–164. DOI: 10.1016/j.comcom.2017.09.005
- [8] Jiang, S., Zhu, X., & Wang, L. (2016). An efficient anonymous batch authentication scheme based on HMAC for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 17(8), 2193–2204. DOI: 10.1109/TITS.2016.2517603
- [9] Cui, J., Zhang, J., Zhong, H., & Xu, Y. (2017). SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter. *IEEE Transactions on Vehicular Technology*, 66(11), 10283–10295. DOI: 10.1109/TVT.2017.2718101
- [10] Azees, M., Vijayakumar, P., & Deborah, L. J. (2017). EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 18(9), 2467–2476. DOI: 10.1109/TITS.2016.2634623
- [11] Qi, J., & Gao, T. (2020). A privacy-preserving authentication and pseudonym revocation scheme for VANETs. *IEEE Access*, 8, 177693–177707. DOI: 10.1109/ACCESS.2020.3027718
- [12] Simplicio, M. A., Jr., Cominetti, E. L., Patil, H. K., Ricardini, J. E., Ferraz, L. T. D., & Silva, M. V. M. (2021). Privacy-preserving certificate linkage/revocation in VANETs without linkage authorities. *IEEE Transactions on Intelligent Transportation Systems*, 22(6), 3326–3336. DOI: 10.1109/TITS.2020.2981907
- [13] Wei, L., Cui, J., Xu, Y., Cheng, J., & Zhong, H. (2021). Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs. *IEEE Transactions on Information Forensics and Security*, 16, 1681–1695. DOI: 10.1109/TIFS.2020.3040876
- [14] Li, J., Song, Z., Li, Y., Cao, C., & He, Y. (2021). Trajectory as an identity: Privacy-preserving and Sybil-resistant authentication for Internet of Vehicles. *Security and Communication Networks*, 2021, 8251697. DOI: 10.1155/2021/8251697
- [15] 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
- [16] Ali, I., Lawrence, T., Anyembe, A. A., & Li, F. (2020). An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs. *IEEE Transactions on Vehicular Technology*, 69(10), 11266–11280. DOI: 10.1109/TVT.2020.3008781



- [17] Kang, J., Lin, D., Jiang, W., & Bertino, E. (2018). Highly efficient randomized authentication in VANETs. *Pervasive and Mobile Computing*, 44, 31–44. DOI: 10.1016/j.pmcj.2018.01.004
- [18] Agustina, E. R., & Hakim, A. R. (2017). Secure VANET protocol using hierarchical pseudonyms with blind signature. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE. DOI: 10.1109/TSSA.2017.8272919
- [19] Nath, H. J., & Choudhury, H. (2022). A privacy-preserving mutual authentication scheme for group communication in VANET. *Computer Communications*, 192, 357–372. DOI: 10.1016/j.comcom.2022.06.024
- [20] Su, H., Dong, S., Wang, N., & Zhang, T. (2024). An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs. *Vehicular Communications*, 45, 100727. DOI: 10.1016/j.vehcom.2024.100727
- [21] Qi, J., et al. (2022). A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs. *Vehicular Communications*, 38, 100535. DOI: 10.1016/j.vehcom.2022.100535
- [22] Yang, Y., Wei, L., Wu, J., Long, C., & Li, B. (2022). A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network. *IEEE Internet of Things Journal*, 9(11), 8078–8090. DOI: 10.1109/JIOT.2021.3107443
- [23] Lin, C., Huang, X., He, D., et al. (2022). EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs. *IEEE Transactions on Dependable and Secure Computing*. DOI: 10.1109/TDSC.2022.3164740
- [24] Khan, S., Raza, A., & Hwang, S. O. (2022). An enhanced privacy preserving, secure and efficient authentication protocol for VANET. *Computers, Materials & Continua*, 71(2), 3703–3719. DOI: 10.32604/cmc.2022.023476
- [25] Al-Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2021). SE-CPPA: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *Sensors*, 21(24), 8206. DOI: 10.3390/s21248206
- [26] Cahyadi, E. F., & Hwang, M.-S. (2021). An improved efficient anonymous authentication with conditional privacy-preserving scheme for VANETs. *PLOS ONE*, 16(9), e0257044. DOI: 10.1371/journal.pone.0257044
- [27] Shim, K.-A. (2023). Security analysis of conditional privacy-preserving authentication schemes for VANETs. *IEEE Access*, 11, 33956–33963. DOI: 10.1109/ACCESS.2023.3263738
- [28] Wang, Y., et al. (2022). An efficient conditional privacy-preserving authentication scheme with scalable revocation for VANETs. *Journal of Systems Architecture*, 133, 102764. DOI: 10.1016/j.sysarc.2022.102764
- [29] Zhang, S., Liu, Y., Xiao, Y., & He, R. (2022). A trust based adaptive privacy preserving authentication scheme for VANETs. *Vehicular Communications*, 37, 100516. DOI: 10.1016/j.vehcom.2022.100516
- [30] Gan, Y., Xie, X., & Liu, Y. (2024). A privacy-preserving V2I fast authentication scheme in VANETs. *Electronics*, 13(12), 2369. DOI: 10.3390/electronics13122369
- [31] Verma, G. K., Chamola, V., Tiwari, A., Kumar, N., Mishra, D., Rana, S., & Barnawi, A. (2025). Escrow-free and efficient dynamic anonymous privacy-preserving batch verifiable authentication scheme for VANETs. *Ad Hoc Networks*, 166, 103670. DOI: 10.1016/j.adhoc.2024.103670
- [32] DBCPCA: Double-layer blockchain-assisted conditional privacy-preserving cross-domain authentication for VANETs. (2024). *Ad Hoc Networks*, 163, 103600. DOI: 10.1016/j.adhoc.2024.103600



- [33] Lu, X., & Guo, X. (2025). A double-layer blockchain-assisted conditional privacy-preserving authentication and emergency reporting scheme for VANETs. *Peer-to-Peer Networking and Applications*, 18, 271. DOI: 10.1007/s12083-025-02095-5
- [34] 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
- [35] Han, M., Liu, S., Ma, S., & Wan, A. (2020). Anonymous-authentication scheme based on fog computing for VANET. *PLOS ONE*, 15(2), e0228319. DOI: 10.1371/journal.pone.0228319
- [36] Mahmood, A., Zhang, W. E., Sheng, Q. Z., Siddiqui, S. A., & Aljubairy, A. (2019). Trust management for software-defined heterogeneous vehicular ad hoc networks. In *Security, Privacy and Trust in the IoT Environment* (pp. 203–226). Springer.
- [37] Zhu, X., Jiang, S., Wang, L., & Li, H. (2014). Efficient privacy-preserving authentication for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 63, 907–919. DOI: 10.1109/TVT.2013.2294032
- [38] Zhang, C., Lin, X., Lu, R., & Ho, P.-H. (2008). RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In *2008 IEEE International Conference on Communications (ICC)* (pp. 1451–1457). IEEE. DOI: 10.1109/ICC.2008.281
- [39] Fan, C.-I., Huang, C.-N., & Hwang, J.-J. (2008). Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks. In *Proceedings of the 2008 ACM Symposium on Applied Computing*. ACM. DOI: 10.1145/1506270.1506372
- [40] Raya, M., Papadimitratos, P., & Hubaux, J.-P. (2006). Securing vehicular communications. *IEEE Wireless Communications*, 13(5), 8–15. DOI: 10.1109/WC-M.2006.250352