



Privacy-Preserving and Zero-Trust Vehicle Renting in VANETs: Secure Authentication, Driver Accountability, and Sybil Resistance

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). Privacy-Preserving and Zero-Trust Vehicle Renting in VANETs: Secure Authentication, Driver Accountability, and Sybil Resistance. International Journal of Creative and Open Research in Engineering and Management, 2(9), 1-9.
<https://doi.org/10.55041/ijcope.v2i9.221>

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.v2i9.221>

Abstract

Vehicular Ad Hoc Networks (VANETs) enable intelligent transportation services such as connected vehicle communication, vehicle sharing, and vehicle renting, but their open and dynamic communication environment creates significant security and privacy challenges. Vehicle-rental services require not only reliable authentication but also temporary authorization, protection of renter identity, resistance to Sybil attacks, and accountability in the event of misuse. This paper proposes a Privacy-Preserving and Zero-Trust Vehicle Renting Framework (PP-ZTVR) that integrates pseudonymous authentication, controlled pseudonym management, rental-session binding, zero-trust authorization, Sybil resistance, conditional driver accountability, continuous verification, and credential revocation. Unlike conventional authentication approaches in which successful authentication may establish persistent trust, the proposed framework separates authentication from authorization and evaluates access according to the current renter, vehicle, rental session, validity period, permissions, and revocation status. Controlled pseudonym issuance limits identity multiplication while preserving privacy during normal VANET communication. A protected accountability mechanism enables authorized identity resolution when serious security incidents occur. The framework also incorporates session-specific authorization tokens to prevent unauthorized vehicle access after rental

expiration or outside the assigned vehicle. A security and performance evaluation framework is developed using authentication latency, computational overhead, communication overhead, revocation delay, Sybil detection rate, false-positive rate, privacy protection, and scalability as key metrics. The proposed framework provides an integrated architecture for balancing privacy, accountability, authentication, and zero-trust access control in VANET-based vehicle-rental environments and provides a foundation for future implementation and quantitative evaluation in realistic vehicular network scenarios.

Keywords: Vehicular Ad Hoc Networks (VANETs); Privacy-Preserving Authentication; Zero-Trust Security; Vehicle Renting; Sybil Attack Resistance; Driver Accountability; Pseudonymous Authentication; Conditional Privacy; Rental-Session Authorization; Credential Revocation; Secure Vehicle Communication.

1. Introduction

Vehicular Ad Hoc Networks (VANETs) have become an important component of intelligent transportation systems because they enable communication among vehicles, roadside units (RSUs), edge servers, transportation infrastructure, and service providers. VANETs support applications such as collision avoidance, traffic management, intelligent



parking, vehicle sharing, vehicle renting, and cooperative driving. However, the open and highly dynamic nature of vehicular communication creates significant security and privacy challenges. Vehicles must be able to authenticate communicating entities and verify the integrity of received messages while preventing unauthorized parties from obtaining permanent information about vehicle owners and drivers.

Privacy-preserving authentication is particularly important because vehicular messages may contain information that can reveal a user's identity, location, travel route, and behavioural patterns. At the same time, excessive anonymity can create accountability problems. A malicious user may exploit anonymous or pseudonymous identities to disseminate false information, launch Sybil attacks, or misuse a rented vehicle without being identified. Therefore, an effective VANET security architecture must achieve a balance between privacy and accountability.

Vehicle-renting services introduce additional security requirements. Unlike a vehicle owner, a renter receives temporary authority to operate a particular vehicle for a predefined period. Consequently, successful registration or authentication of a renter should not automatically provide unrestricted access to all vehicles or all services. The system must determine whether the renter is authorized to operate a particular vehicle, whether the rental session is currently valid, whether the associated credential has been revoked, and whether the requested operation falls within the permissions granted by the rental agreement.

Recent research has specifically addressed these challenges. Akil, Martucci, and Hoepman proposed a non-interactive privacy-preserving Sybil-free authentication scheme for VANETs [1]. Their subsequent work investigated a secure and privacy-preserving authentication scheme based on a zero-trust approach to vehicle renting in VANETs [2]. Akil et al. also proposed a privacy-preserving approach to vehicle renting and driver accountability [3]. These studies provide a strong foundation for integrating privacy-preserving authentication, Sybil resistance, zero-trust principles, and driver accountability in vehicle-rental environments.

Security problems in connected distributed systems may also arise from unintended or covert communication channels. Akil, Mancini, and Venturi investigated multi-covert-channel attacks in cloud environments [4]. Although their work is not specifically focused on VANETs, it demonstrates the broader importance of considering communication leakage and unauthorized information channels in distributed security architectures.

The broader VANET literature has investigated authentication, privacy preservation, conditional privacy, certificateless cryptography, pseudonym-based authentication, Sybil resistance, revocation, blockchain, and lattice-based security. Manivannan et al. examined secure authentication and privacy-preserving techniques in VANETs [5], while Mundhe et al. presented a comprehensive survey of authentication and privacy-preserving schemes [6]. Sutradhar et al. investigated privacy-preserving authentication protocols for secure vehicular communication [7], and Nath and Choudhury examined privacy-preserving authentication requirements and protocols [8].

Several studies have developed specific cryptographic solutions. Ming proposed an efficient certificateless conditional privacy-preserving authentication scheme [9]. Dharminder and Mishra investigated lattice-based conditional privacy-preserving authentication [10]. De Sales et al. proposed a privacy-preserving authentication and Sybil-detection protocol [11], while Balaram and Pushpa investigated Sybil-resistant location privacy [12]. Ali et al. proposed an ECC-based conditional privacy-preserving authentication mechanism [13]. Mukherjee et al. investigated batch-verifiable lattice-based authentication [14], and Imghoure et al. studied ECDSA-based certificateless conditional privacy-preserving authentication [15].

Other studies have addressed conditional privacy, privacy-preserving authentication, physical security, pseudonym-based authentication, revocation, blockchain, and post-quantum security [16]–[24].

Despite these developments, an integrated architecture specifically addressing the complete vehicle-rental lifecycle remains an important research problem. A vehicle-rental system requires privacy-preserving authentication, temporary authorization, vehicle-specific access control, Sybil resistance, continuous verification, accountability, and revocation. These requirements are closely interconnected and cannot be adequately addressed by considering authentication alone.



Therefore, this paper proposes a Privacy-Preserving and Zero-Trust Vehicle Renting Framework (PP-ZTVR) for VANETs. The proposed framework integrates pseudonymous authentication, controlled pseudonym issuance, rental-session binding, zero-trust authorization, conditional accountability, Sybil resistance, continuous verification, and dynamic credential revocation.

The central research question is:

How can a VANET-based vehicle-rental system provide strong authentication and continuous zero-trust authorization while preserving renter privacy, preventing Sybil attacks, supporting conditional accountability, and enabling efficient credential revocation?

The proposed framework addresses this question by separating permanent identity from operational identity and authentication from authorization. The framework treats a rental session as a temporary security boundary and requires authorization to remain valid only for the specified renter, vehicle, time period, and set of permitted operations.

2. Literature Review

The security of VANETs has been extensively investigated because vehicles operate in a distributed, wireless, and highly dynamic environment. Conventional authentication mechanisms can establish whether a message originates from a legitimate entity, but they may reveal persistent identities and consequently enable tracking. Privacy-preserving authentication therefore attempts to allow vehicles to prove legitimacy without continuously revealing their permanent identities.

Manivannan et al. [5] reviewed secure authentication and privacy-preserving techniques in VANETs and identified authentication, confidentiality, integrity, privacy, and resistance to attacks as important requirements. Mundhe et al. [6] provided a comprehensive survey of VANET authentication and privacy-preserving schemes and highlighted the trade-off between security, privacy, computation, and communication overhead. Sutradhar et al. [7] examined privacy-preserving authentication protocols for secure vehicular communication, while Nath and Choudhury [8] discussed privacy-preserving authentication requirements in VANET environments.

The specific problem of vehicle renting introduces additional requirements beyond conventional VANET authentication. Akil et al. [3] investigated privacy-preserving vehicle renting together with driver accountability. This work is important because a vehicle-rental system must protect the renter's identity during normal operation while retaining the possibility of identifying a responsible party after a legitimate security investigation.

Akil et al. [2] further investigated secure and privacy-preserving authentication using a zero-trust approach to vehicle renting in VANETs. The zero-trust principle is particularly appropriate for rental services because authentication at the beginning of a rental should not result in permanent trust. Instead, access should depend on the validity of the current rental authorization, vehicle, time period, and security conditions.

Sybil attacks represent another major challenge. In a Sybil attack, one malicious participant creates or controls multiple identities and uses them to gain disproportionate influence within the network. Akil et al. [1] specifically investigated non-interactive privacy-preserving Sybil-free authentication in VANETs. De Sales et al. [11] also investigated privacy-preserving authentication combined with Sybil detection, while Balaram and Pushpa [12] examined Sybil-resistant location privacy. These studies demonstrate that privacy and Sybil resistance must be designed together rather than treated as completely independent objectives.

Certificateless cryptography provides another approach to vehicular authentication. Ming [9] proposed an efficient certificateless conditional privacy-preserving authentication scheme. Ali et al. [13] developed an ECC-based conditional privacy-preserving authentication mechanism, while Imghoure et al. [15] investigated ECDSA-based certificateless



conditional privacy-preserving authentication. These approaches demonstrate how cryptographic mechanisms can reduce certificate-management requirements while maintaining authentication and privacy.

Lattice-based cryptography has attracted increasing attention because of the potential threat posed by quantum computing. Dharminder and Mishra [10] proposed a lattice-based conditional privacy-preserving authentication mechanism. Mukherjee et al. [14] investigated batch-verifiable lattice-based authentication, while Nath and Choudhury [24] proposed lattice-based privacy-preserving mutual authentication. These studies provide a possible direction for developing future post-quantum versions of the proposed framework.

Credential revocation is another essential component of vehicular security. A credential that has been compromised or associated with malicious activity should no longer be accepted by vehicles or roadside infrastructure. Shen et al. [20] investigated scalable revocation in conditional privacy-preserving authentication. Blockchain-assisted authentication has also been explored as a mechanism for distributed security and audit management [21].

Other research has investigated conditional privacy-preserving authentication [16], privacy-preserving authentication schemes [17], physically secure authentication [18], pseudonym-based certificateless authentication [19], and enhanced privacy-preserving authentication [23]. These approaches collectively demonstrate the maturity of VANET security research, but they also show that security objectives are frequently addressed individually.

The literature therefore indicates a need for an integrated vehicle-rental security architecture. The proposed PP-ZTVR framework builds upon the direct vehicle-rental and zero-trust foundations of Akil et al. [1]–[3] and incorporates complementary concepts from the wider VANET security literature [5]–[24].

The principal research gap addressed in this paper is the integration of privacy-preserving authentication, zero-trust authorization, controlled pseudonyms, rental-session management, Sybil resistance, driver accountability, and revocation into a unified vehicle-rental architecture.

3. Proposed Privacy-Preserving and Zero-Trust Vehicle Renting Framework

The proposed Privacy-Preserving and Zero-Trust Vehicle Renting Framework, referred to as PP-ZTVR, is designed for VANET-based vehicle-rental environments. The framework considers the renter, rental service provider, vehicle, trusted authority, roadside or edge infrastructure, and accountability and revocation authority as the principal entities.

3.1 System architecture

The renter interacts with the Rental Service Provider to select and reserve a vehicle. The Trusted Authority manages permanent identities and cryptographic credentials but does not expose the renter's permanent identity during ordinary VANET communication. The Rental Service Provider creates a temporary rental authorization associated with a specific vehicle and rental period.

The vehicle contains an onboard security module responsible for verifying the renter's credential and rental authorization. RSUs or edge servers assist with message verification, security monitoring, and distribution of revocation information. The Accountability and Revocation Authority maintains the protected relationship between operational pseudonyms and permanent identities and performs identity resolution only under authorized conditions.

The architecture can be represented as:

Renter → Trusted Authority → Pseudonymous Credential

Renter → Rental Service Provider → Rental Authorization



Rental Authorization → Vehicle

Vehicle ↔ RSU/Edge Server ↔ VANET

Security Incident → Accountability Authority → Identity Resolution

The architecture deliberately separates normal operational communication from identity-resolution functions.

3.2 Privacy-preserving registration

During initial registration, the renter's permanent identity is verified by the Trusted Authority. After successful verification, the authority generates a protected cryptographic credential and one or more pseudonymous identities.

A pseudonymous identity can be represented in Word-compatible notation as:

$$\text{PID} = \text{H}(\text{Identity} + \text{Random Value} + \text{Validity Period})$$

where PID represents the pseudonymous identity and H represents a secure cryptographic hash function.

The relationship between the permanent identity and the pseudonym is securely maintained by the Trusted Authority. Other VANET participants use the pseudonym rather than the permanent identity.

This arrangement provides conditional privacy. During ordinary communication, the renter operates through a pseudonym. If a serious security incident occurs and the required authorization is obtained, the accountability authority can resolve the pseudonym to the corresponding registered identity.

3.3 Controlled pseudonym management

Pseudonymity must be controlled because unlimited pseudonym generation could facilitate Sybil attacks. The proposed framework therefore issues a controlled set of pseudonyms to each legitimate renter.

The pseudonym set can be represented as:

$$P = \{\text{PID1}, \text{PID2}, \text{PID3}, \dots, \text{PIDn}\}$$

Each pseudonym is associated with a validity period and cryptographic key. The Trusted Authority controls issuance and revocation.

The purpose is not to prevent legitimate privacy-preserving identity changes but to prevent a single participant from obtaining an unlimited number of simultaneously active identities.

The proposed approach therefore establishes a relationship between:

Permanent Identity → Controlled Pseudonyms → Rental Session

This relationship provides privacy while maintaining accountability and Sybil resistance.

3.4 Vehicle registration

Vehicles are also registered with the Trusted Authority. Each vehicle receives a cryptographic identity and operational credentials. Similar to renter identities, vehicle identifiers can be represented using temporary or pseudonymous identifiers.



A vehicle pseudonym can be represented as:

$$\text{VPID} = H(\text{Vehicle Identity} + \text{Random Value} + \text{Validity Period})$$

The use of vehicle pseudonyms reduces unnecessary disclosure of permanent vehicle information during ordinary communication.

3.5 Rental request and session creation

After selecting a vehicle, the renter submits a rental request to the Rental Service Provider. The request contains the renter's pseudonymous identity, selected vehicle, requested rental duration, and authentication proof.

The service provider verifies the renter credential, credential validity, revocation status, vehicle availability, and applicable rental conditions.

After successful verification, a unique rental-session identifier is generated:

$$\text{Session ID} = H(\text{Pseudonym} + \text{Vehicle Pseudonym} + \text{Start Time} + \text{End Time})$$

The rental session binds the renter to a particular vehicle and a particular time interval.

This binding is important because a legitimate renter should not automatically be authorized to use every vehicle simply because the renter possesses a valid account.

3.6 Rental authorization token

The Rental Service Provider generates a digitally signed authorization token containing the session identifier, renter pseudonym, vehicle pseudonym, start time, end time, and authorized operations.

The token can be represented as:

$$\text{Rental Token} = \text{Digital Signature}(\text{Session ID} + \text{Renter Pseudonym} + \text{Vehicle Pseudonym} + \text{Start Time} + \text{End Time} + \text{Permissions})$$

The token is transmitted securely to the vehicle.

The vehicle verifies the signature and confirms that the token corresponds to the current vehicle and rental session.

3.7 Zero-trust authorization

The central security principle of PP-ZTVR is that successful authentication does not establish permanent trust.

The vehicle evaluates authorization using multiple conditions:

$$\text{Authorization} = \text{Credential Valid AND Rental Token Valid AND Session Valid AND Not Revoked AND Context Valid}$$

If any of these conditions fails, access is rejected or restricted.

For example, a renter may possess a valid permanent account but have no current rental authorization. Similarly, a renter may have a valid rental authorization for Vehicle A but not for Vehicle B. A rental authorization may also become invalid when the rental period expires.

This creates a direct relationship between authorization and the current rental context.



3.8 Continuous verification

Traditional authentication models may authenticate a user once and then maintain trust for the remainder of a session. The proposed framework instead supports continuous or event-driven verification.

Verification can occur when the vehicle is unlocked, when the vehicle is started, when a sensitive operation is requested, periodically during a long rental, or when suspicious behaviour is detected.

This approach is consistent with the zero-trust principle because the system continuously evaluates whether the current conditions justify access.

3.9 Sybil resistance

The proposed Sybil-resistance mechanism combines controlled pseudonym issuance with rental-session binding and behavioural monitoring.

A malicious user attempting to generate many independent identities is limited by the controlled pseudonym policy. Furthermore, pseudonyms are linked to valid rental sessions, making it difficult to use a large collection of pseudonyms simultaneously for unauthorized vehicle access.

The edge infrastructure can also examine suspicious behaviour such as simultaneous conflicting locations, incompatible rental sessions, excessive message generation, or inconsistent identity usage.

A conceptual Sybil suspicion score can be represented as:

Sybil Suspicion Score = $w_1 \times \text{Location Conflict} + w_2 \times \text{Time Conflict} + w_3 \times \text{Session Conflict} + w_4 \times \text{Credential Conflict}$

where the weighting factors represent the relative contribution of each indicator.

A high suspicion level can trigger additional verification or temporary restriction.

3.10 Driver accountability

The framework does not provide unrestricted anonymity. Instead, it implements conditional accountability.

During normal operation:

Pseudonym $\rightarrow$ VANET Communication

During an authorized investigation:

Pseudonym $\rightarrow$ Accountability Authority $\rightarrow$ Registered Identity

Identity resolution should require an authorized security event, such as serious misuse of the vehicle, repeated malicious activity, unauthorized access, or significant network attacks.

This architecture protects the renter from unnecessary identity disclosure while preserving the ability to investigate serious incidents.



3.11 Credential revocation

Credential revocation is integrated into the authorization process. A credential can be revoked when it is compromised, misused, expired, or associated with malicious activity.

The vehicle therefore checks both credential validity and revocation status before granting sensitive access.

The resulting authorization relationship is:

Valid Credential + Valid Rental Token + Valid Session + Non-Revoked Status = Authorized Access

If any condition fails, access is denied.

4. Security Analysis and Performance Evaluation

The security of the proposed PP-ZTVR framework is evaluated against major threats affecting privacy-preserving VANET-based vehicle-rental systems.

An impersonation attack occurs when an adversary attempts to act as a legitimate renter or vehicle. PP-ZTVR requires possession of the appropriate cryptographic credential and verification of the corresponding rental authorization. Therefore, knowledge of a pseudonym alone does not provide sufficient authorization.

Replay attacks are addressed through the use of timestamps, nonces, session identifiers, and cryptographic signatures. A received message is accepted only if its temporal information is valid and its cryptographic verification succeeds. A previously used nonce or expired session should be rejected.

A man-in-the-middle attacker may attempt to intercept or modify communication between the renter and vehicle. Cryptographic authentication and integrity protection prevent an attacker from successfully modifying signed information without detection.

Credential theft is addressed through rental-session binding. Even if an attacker obtains some credential information, the attacker should not automatically gain unlimited access because the authorization token is associated with a specific vehicle, session, time period, and set of permissions.

Unauthorized vehicle access is controlled through the rental token. A valid registered identity alone is insufficient to start or operate a vehicle when no valid rental authorization exists.

Expired-rental attacks are addressed through time-limited authorization. If the current time exceeds the rental end time, the authorization token becomes invalid.

Sybil attacks are addressed through controlled pseudonym issuance, identity binding, rental-session association, and behavioural monitoring. The framework does not attempt to eliminate pseudonyms because doing so would reduce privacy. Instead, it controls the number and validity of operational identities.

Tracking attacks are mitigated through temporary pseudonymous identities. Since the renter's permanent identity is not continuously transmitted, ordinary VANET participants have less direct ability to associate every message with a permanent individual.



Conditional accountability addresses the opposite problem. If a malicious renter abuses the system, the authorized accountability authority can investigate the associated pseudonym and, subject to appropriate authorization, recover the registered identity.

The framework can therefore be evaluated according to authentication security, privacy preservation, Sybil resistance, accountability, revocation, computation, communication overhead, and scalability.

4.1 Authentication performance

Authentication latency can be calculated as:

Authentication Latency = Request Processing Time + Verification Time + Response Time

The latency should be measured in milliseconds for different vehicle densities and authentication loads.

4.2 Computational overhead

Computational overhead should include the number and execution time of cryptographic operations, including hash calculations, signature generation, signature verification, key generation, encryption, and decryption.

The total computation time can be represented as:

Total Computation Time = Hash Time + Signing Time + Verification Time + Key Processing Time

The actual values should be obtained experimentally rather than assumed.

4.3 Communication overhead

Communication overhead represents the amount of data exchanged during authentication and rental authorization.

Communication Overhead = Total Size of Security Messages

The evaluation should include registration, authentication, rental authorization, session renewal, revocation, and accountability operations.

4.4 Revocation performance

Revocation delay is an important metric because a compromised credential should not remain active for an extended period.

Revocation Delay = Detection Time + Revocation Processing Time + Distribution Time

The proposed architecture should be evaluated under both individual and large-scale revocation scenarios.

4.5 Privacy performance

Privacy evaluation should examine whether an external observer can associate multiple pseudonymous messages with the same permanent renter.

The analysis should consider:

- resistance to direct identity disclosure;
- resistance to long-term tracking;



- protection of rental information;
- separation of operational and permanent identities;
- controlled identity resolution.

4.6 Sybil-detection performance

Sybil detection should be evaluated using detection rate and false-positive rate.

Sybil Detection Rate = Detected Sybil Identities / Actual Sybil Identities $\times$ 100

False Positive Rate = Legitimate Users Incorrectly Classified as Malicious / Total Legitimate Users $\times$ 100

The framework should be tested under different attack intensities.

4.7 Scalability evaluation

The proposed architecture should be evaluated with increasing numbers of vehicles and simultaneous rental sessions. A suitable experimental design could consider 100, 250, 500, 750, and 1000 vehicles, together with different numbers of concurrent authentication requests.

The simulation can be implemented using SUMO for vehicle mobility and Veins or NS-3 for communication and security-protocol evaluation. Cryptographic operations can be implemented using a suitable security library.

Table 1 presents the principal evaluation dimensions.

Table 1. Proposed performance evaluation parameters

Parameter	Measurement
Authentication latency	Milliseconds
Authentication success rate	Percentage
Computation overhead	Milliseconds or number of cryptographic operations
Communication overhead	Bytes
Revocation delay	Milliseconds
Sybil detection rate	Percentage
False-positive rate	Percentage
Privacy protection	Identity-linkability analysis
Scalability	Performance with increasing vehicles
Rental-session validation	Successful/failed authorization

The experimental results should be reported after implementation and should not be replaced by assumed numerical values.

5. Discussion and Conclusion

The proposed PP-ZTVR framework integrates several security concepts that are usually investigated independently. The most direct foundations are provided by the work of Akil et al. on Sybil-free privacy-preserving authentication [1], zero-trust vehicle renting [2], and privacy-preserving vehicle renting with driver accountability [3]. These works establish the core relationship between privacy, vehicle renting, authentication, accountability, and zero trust. The work of Akil et al.



on covert channels [4] further highlights the importance of controlling unintended communication and information leakage in distributed environments.

The wider VANET literature provides complementary mechanisms. Privacy-preserving authentication studies [5]–[8] establish the importance of protecting user identity while maintaining authentication. Certificateless and ECC-based schemes [9], [13], [15] provide mechanisms for efficient authentication. Sybil-resistant approaches [11], [12] address malicious identity multiplication. Lattice-based schemes [10], [14], [24] provide a potential direction for post-quantum security. Revocation and blockchain approaches [20], [21] support credential lifecycle and distributed security management.

The principal contribution of PP-ZTVR is therefore architectural integration. The framework treats a vehicle-rental transaction as a temporary and context-dependent security relationship rather than as a permanent trust relationship.

The distinction between authentication and authorization is particularly important. Authentication determines whether the renter possesses a legitimate credential, whereas authorization determines whether the renter is currently permitted to perform a particular operation on a particular vehicle. Thus:

Legitimate Renter $\neq$ Automatically Authorized Renter

The proposed architecture expresses authorization through the combination of renter identity, vehicle identity, rental session, time, permissions, and revocation status.

Privacy and accountability are also treated as complementary objectives. During normal operation, the renter communicates using a pseudonym. When a serious security event occurs, the authorized accountability authority can resolve the pseudonym to the registered identity. This provides a mechanism for investigation without requiring permanent identity disclosure during routine VANET communication.

Similarly, privacy and Sybil resistance are balanced through controlled pseudonymity. The system allows pseudonyms for privacy but controls their issuance, validity, and association with rental sessions. This avoids the two extremes of permanent identity exposure and unrestricted anonymous identity creation.

The zero-trust approach is particularly suitable for vehicle renting because rental authorization is temporary. A renter may be authorized to operate one vehicle during a specific time period but should not automatically receive access to another vehicle or continue accessing the same vehicle after the rental period expires. PP-ZTVR therefore continuously or periodically evaluates the validity of the current authorization.

The proposed framework has several limitations. It assumes the availability of trusted infrastructure for identity registration and credential management. The accountability authority must be strongly protected because compromise of identity-resolution information could have serious privacy consequences. Continuous verification may increase computational and communication overhead, and behavioural Sybil detection may produce false positives under unusual traffic conditions. These limitations require experimental evaluation.

Future research should implement the framework in a realistic VANET simulation environment and compare it quantitatively with existing privacy-preserving authentication and vehicle-rental protocols. SUMO can be used to generate realistic vehicle mobility, while Veins or NS-3 can be used to model VANET communication. Formal verification using security-analysis tools can further investigate resistance against impersonation, replay, man-in-the-middle, Sybil, and unauthorized-access attacks. Post-quantum extensions using lattice-based cryptography can also be investigated using the approaches reported in [10], [14], and [24]. Blockchain can optionally be incorporated for distributed audit and revocation management [21].

In conclusion, secure vehicle renting in VANETs requires more than conventional authentication. The system must simultaneously protect renter privacy, prevent fraudulent identity multiplication, provide temporary vehicle-specific



authorization, maintain accountability, and revoke compromised credentials. The proposed Privacy-Preserving and Zero-Trust Vehicle Renting Framework addresses these requirements by integrating pseudonymous authentication, controlled identity management, rental-session binding, zero-trust authorization, Sybil resistance, conditional accountability, continuous verification, and revocation.

The framework provides a conceptual basis for developing secure VANET-based vehicle-rental services and can be extended to vehicle sharing, autonomous vehicle fleets, mobility-as-a-service platforms, and other connected transportation applications.

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. <https://doi.org/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. <https://doi.org/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: 18th IFIP WG 9.2, 9.6/11.7, 11.6 International Summer School, Privacy and Identity 2023, Revised Selected Papers, pp. 192–210. Springer. https://doi.org/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 Proceedings of the 6th International Conference on Software Defined Systems (SDS 2019), pp. 160–165. IEEE. <https://doi.org/10.1109/SDS.2019.8768563>
- [5] Manivannan, D., Moni, S. S., & Zeadally, S. (2020). Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). Vehicular Communications, 25, 100247. <https://doi.org/10.1016/j.vehcom.2020.100247>
- [6] Mundhe, P., Verma, S., & Venkatesan, S. (2021). A comprehensive survey on authentication and privacy-preserving schemes in VANETs. Computer Science Review, 41, 100411. <https://doi.org/10.1016/j.cosrev.2021.100411>
- [7] 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. <https://doi.org/10.1016/j.comcom.2024.02.024>
- [8] Nath, H. J., & Choudhury, H. (2023). Privacy-preserving authentication protocols in VANET. SN Computer Science, 4, 589. <https://doi.org/10.1007/s42979-023-02122-3>
- [9] Ming, Y. (2019). Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. Mobile Information Systems, 2019, 7593138. <https://doi.org/10.1155/2019/7593138>
- [10] Dharminder, D., & Mishra, D. (2020). LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication. Transactions on Emerging Telecommunications Technologies, 31, e3810. <https://doi.org/10.1002/ett.3810>
- [11] de Sales, T. B. M., Perkusich, A., de Sales, L. M., de Almeida, H. O., Soares, G., & de Sales, M. (2016). ASAP-V: A privacy-preserving authentication and Sybil detection protocol for VANETs. Information Sciences, 372, 208–224. <https://doi.org/10.1016/j.ins.2016.08.024>



- [12] Balaram, A., & Pushpa, S. (2018). Sybil attack resistant location privacy in VANET. *International Journal of Information and Communication Technology*, 13(4), 389–406. <https://doi.org/10.1504/IJICT.2018.095025>
- [13] Ali, I., Chen, Y., Ullah, N., Kumar, R., & He, W. (2021). An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. *IEEE Transactions on Vehicular Technology*, 70, 1278–1291. <https://doi.org/10.1109/TVT.2021.3050399>
- [14] Mukherjee, S., Gupta, D. S., & Biswas, G. P. (2019). An efficient and batch verifiable conditional privacy-preserving authentication scheme for VANETs using lattice. *Computing*, 101, 1763–1788. <https://doi.org/10.1007/s00607-018-0689-3>
- [15] Imghoure, A., El-Yahyaoui, A., & Omary, F. (2022). ECDSA-based certificateless conditional privacy-preserving authentication scheme in vehicular ad hoc network. *Vehicular Communications*, 37, 100504. <https://doi.org/10.1016/j.vehcom.2022.100504>
- [16] Xiong, W., Wang, R., Wang, Y., Zhou, F., & Luo, X. (2021). CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs. *IEEE Transactions on Vehicular Technology*, 70, 3456–3468. <https://doi.org/10.1109/TVT.2021.3064337>
- [17] Jegadeesan, S., et al. (2020). PPAS: Privacy preserving authentication scheme for vehicular ad-hoc network. *International Journal of Grid and Distributed Computing*, 13(1).
- [18] Aghabagherloo, A., Delavar, M., Mohajeri, J., Salmasizadeh, M., & Preneel, B. (2022). An efficient and physically secure privacy-preserving authentication scheme for Vehicular Ad-hoc NETWORKS (VANETs). *IEEE Access*. <https://doi.org/10.1109/ACCESS.2022.3203580>
- [19] Qi, J., Gao, T., Deng, X., & Zhao, C. (2022). A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs. *Vehicular Communications*, 38, 100535. <https://doi.org/10.1016/j.vehcom.2022.100535>
- [20] Shen, L., Wang, L., Zhang, K., Li, J., & Chen, K. (2022). An efficient conditional privacy-preserving authentication scheme with scalable revocation for VANETs. *Journal of Systems Architecture*, 133, 102764. <https://doi.org/10.1016/j.sysarc.2022.102764>
- [21] Xia, F., Shi, Q., Xie, Q., & Liu, L. (2021). An efficient privacy-preserving authentication model based on blockchain for VANETs. *Journal of Systems Architecture*, 117, 102158. <https://doi.org/10.1016/j.sysarc.2021.102158>
- [22] Zhang, J., Zhen, W., & Xu, M. (2013). An efficient privacy-preserving authentication protocol in VANETs. In *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 272–277. IEEE. <https://doi.org/10.1109/MSN.2013.31>
- [23] 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. <https://doi.org/10.32604/cmc.2022.023476>
- [24] Nath, H. J., & Choudhury, H. (2024). LbPV: Lattice-based privacy-preserving mutual authentication scheme for VANET. *Computers & Electrical Engineering*, 120, 109765. <https://doi.org/10.1016/j.compeleceng.2024.109765>