[1]Moawiah El-Dalahmeh

[2]Adi El-Dalahmeh

Lightweight Authentication Mechanisms for Privacy Preservation in VANETs

Journal of Electrical Systems

Abstract: **-** Vehicular Ad Hoc Networks (VANETs) rely on fast and secure authentication mechanisms to ensure message legitimacy, user privacy, and system scalability. However, traditional Public Key Infrastructure (PKI) and certificate-based authentication models impose substantial overhead and compromise location privacy. This paper presents a comprehensive analysis of lightweight cryptographic approaches designed to preserve privacy while maintaining efficiency in VANETs. We classify existing protocols by cryptographic family, trust management design, and privacy-preserving capabilities. A detailed comparative framework evaluates five representative schemes—PB-PKI-VLR, IBACP, GST, CL-ECC, and BAPS—based on authentication delay, privacy score, and overhead. Simulation results demonstrate that certificate less ECC achieves the best balance between security, latency, and anonymity. The paper concludes with a discussion on deployment challenges and future directions for scalable, privacyaware vehicular authentication.

Keywords: VANETs, Lightweight Authentication, Privacy Preservation, ECC, Group Signatures, Blockchain, Security, Pseudonym, IBC, CL-PKC

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) form the communication backbone of next-generation Intelligent Transportation Systems (ITS), enabling vehicles to exchange safetycritical information in real-time to enhance road safety, traffic management, and passenger comfort [1]. These networks are characterized by high mobility, dynamic topology, and frequent disconnections, making them particularly vulnerable to a wide range of security and privacy threats. Among these, unauthorized access, message tampering, identity spoofing, and location tracking present significant concerns for both users and infrastructure [2].

Authentication is a fundamental security requirement in VANETs, ensuring that messages originate from legitimate and trustworthy sources. However, implementing robust authentication in such highly dynamic and latency-sensitive environments is a non-trivial task. Traditional cryptographic approaches, especially those based on Public Key Infrastructure (PKI), offer strong security guarantees but incur substantial computational, communication, and storage overhead [3]. Moreover, these schemes often fail to preserve user privacy, as they rely on persistent vehicle identities or certificate-based mechanisms that can be linked and tracked over time.

Privacy preservation is equally critical in VANETs. Vehicles continuously broadcast beacons containing location, speed, and direction, which can be exploited by adversaries to perform location tracking and driver profiling [4]. Hence, a secure authentication mechanism in VANETs must also be privacy-aware, ensuring that vehicle identities are protected and unlinkable, while still enabling accountability in the case of misbehavior or law enforcement inquiries.

To address these dual goals of lightweight security and privacy, researchers have explored several advanced cryptographic techniques. These include identity-based cryptography (IBC), pseudonym systems, group signatures, and certificateless public key cryptography (CL-PKC) [5], [6]. Pseudonymbased authentication, where vehicles periodically change their public keys and certificates, can mitigate tracking risks, but require frequent certificate updates and efficient revocation strategies. Group signatures allow vehicles to sign messages anonymously on behalf of a group, ensuring sender anonymity while supporting traceability in the case of disputes [7]. Identity-based schemes eliminate the need for certificate distribution by deriving public keys from unique identity strings, offering low-latency operations but suffering from key escrow and trust anchor centralization [8].

Another promising direction involves the use of lightweight cryptographic primitives, such as elliptic curve cryptography (ECC), hash-based authentication, and symmetric key approaches tailored to resource-constrained vehicular onboard units (OBUs). These solutions reduce computational complexity while maintaining an acceptable level of security, making them more suitable for deployment in real-world VANET scenarios [9].

[1] *Corresponding author: Moawiah El-Dalahmeh, Cybersecurity Department , Al-Zaytoonah University of Jordan, Amman , Jordan
[2] Author 2: Adi El-Dalahmeh, Cybersecurity Department , Al-Zaytoonah University of Jordan, Amman , Jordan

However, trade-offs often exist between privacy strength, authentication speed, scalability, and accountability, necessitating a careful evaluation of competing mechanisms.

A. Motivation

The increasing deployment of connected and autonomous vehicles, coupled with stringent data protection regulations, has intensified the need for privacy-preserving authentication mechanisms in VANETs. Existing solutions either compromise privacy for performance or introduce excessive overhead to meet privacy goals. Furthermore, many proposed schemes lack real-world validation or fail to scale with network size and traffic density [10]. There is thus a pressing need to investigate and compare lightweight authentication protocols that strike an optimal balance between security, privacy, and efficiency.

B. Research Objectives

This paper aims to provide a comprehensive analysis and evaluation of lightweight authentication mechanisms designed for privacy preservation in VANET environments. The main objectives are:

•To categorize existing authentication schemes based on cryptographic design, privacy guarantees, and computational complexity.

•To analyze their strengths, limitations, and suitability for different vehicular scenarios (e.g., highway vs. urban, high-speed vs. low-speed).

•To evaluate representative schemes through simulation and analytical metrics such as authentication delay, privacy level, scalability, and message overhead.

•To propose future research directions and practical design recommendations for deploying privacy-aware authentication in real-world VANET infrastructures.

C. Paper Organization

The remainder of this paper is organized as follows: Section II reviews the related work on authentication and privacy in VANETs. Section III presents a taxonomy of lightweight authentication mechanisms and privacy-preserving techniques. Section IV outlines the evaluation framework and criteria. Section V describes and compares selected schemes. Section VI presents simulation results and analysis. Section VII discusses practical deployment considerations and open research challenges. Finally, Section VIII concludes the paper and suggests directions for future work.

II. RELATED WORK

Authentication and privacy preservation have been extensively studied in the context of Vehicular Ad Hoc Networks (VANETs), particularly as the threat landscape has evolved to include not just malicious outsiders but also insider adversaries capable of tracking and impersonation. This section reviews recent advances in lightweight authentication schemes, categorizing them based on the underlying cryptographic approaches and their effectiveness in addressing both security and privacy requirements.

A. PKI-Based and Pseudonym Authentication

Traditional authentication in VANETs primarily relies on Public Key Infrastructure (PKI), where each vehicle is assigned a set of certificates by a Certificate Authority (CA). The IEEE 1609.2 standard adopts this model and prescribes digital signatures for message authentication [1]. While PKI provides robust identity verification and non-repudiation, it imposes significant storage and processing burdens on vehicular nodes, especially in dense networks with frequent certificate exchanges [2].

To enhance privacy, pseudonym-based authentication was introduced, where vehicles switch between short-lived certificates to avoid linkability [3]. However, managing large pools of pseudonyms and ensuring timely revocation remain challenging. Moreover, frequent pseudonym changes can lead to authentication delays and increased message overhead [4].

B. Group Signature Schemes

Group signature-based authentication schemes enable vehicles to authenticate messages anonymously on behalf of a group, while a trusted authority retains the ability to trace misbehaving users. These schemes offer a strong balance between privacy and accountability. For instance, Liu et al. proposed an efficient group signature protocol that supports dynamic group membership and fast revocation [5]. However, group signatures generally involve complex cryptographic operations such as bilinear pairings, which may hinder realtime performance [6].

C. Identity-Based and Certificateless Cryptography

Identity-based cryptography (IBC) eliminates the need for digital certificates by generating public keys from known identity strings, reducing communication overhead [7]. Zhang et al. presented a lightweight IBC scheme

tailored for VANETs, demonstrating reduced latency in message authentication [8]. Nonetheless, IBC suffers from the key escrow problem, where the Private Key Generator (PKG) can derive any user's private key, introducing a single point of trust failure.

Certificateless Public Key Cryptography (CL-PKC) was developed to mitigate this issue by removing the need for certificate issuance and avoiding key escrow. In CL-PKC, the key generation process is split between the user and a semitrusted authority, preserving privacy without introducing full trust dependency [9]. These schemes are promising but still require careful management of key update and distribution protocols.

D. Lightweight and Symmetric-Key Approaches

Given the computational limitations of vehicular On-Board Units (OBUs), several researchers have proposed symmetric key-based and hash chain-based authentication protocols [10]. These approaches minimize processing time and are suitable for applications with strict latency constraints. For instance, HashMAC and TESLA-like schemes use delayed key disclosure for broadcast authentication, but face synchronization and scalability issues in high-speed vehicular environments [11].

Elliptic Curve Cryptography (ECC) has also gained traction due to its lower key sizes and faster computations compared to RSA. Lightweight ECC-based schemes such as LEAP and ECQV provide strong security while maintaining minimal overhead, making them viable candidates for privacypreserving VANET authentication [12].

E. Blockchain-Enhanced Authentication

Blockchain technologies have been integrated into VANETs to support decentralized authentication and trust management. Li et al. proposed a blockchain-based pseudonym system where vehicles periodically register pseudonyms on-chain to enable transparent revocation and accountability [13]. While blockchain ensures immutability and reduces reliance on centralized authorities, its application to VANETs is limited by latency, consensus overhead, and data storage requirements

[14].

F. AI-Assisted and Hybrid Models

Emerging AI-driven approaches aim to detect spoofing and impersonation attacks by learning patterns of legitimate communications. These techniques are typically used in conjunction with traditional cryptographic authentication to provide an adaptive layer of defense [15]. Hybrid models combining IBC, ECC, and machine learning offer enhanced resilience against evolving threats, but often introduce integration complexity and lack practical evaluation in realistic mobility scenarios [16].

G. Summary of Research Gaps

Despite the abundance of authentication protocols, several research gaps persist:

•Many schemes neglect real-time performance, assuming unlimited computational resources.

•Privacy is often treated as secondary to authentication, with limited consideration of long-term unlinkability.

•Few models address scalability and seamless identity management during high-speed handovers.

•Lack of comprehensive evaluation frameworks for comparing privacy and performance trade-offs.

This paper aims to address these gaps by systematically comparing lightweight authentication schemes with a focus on privacy preservation, using a unified simulation and evaluation approach.

III. TAXONOMY OF LIGHTWEIGHT AUTHENTICATION MECHANISMS

To enable secure and private communication in VANETs, numerous authentication techniques have been developed, ranging from conventional PKI systems to more advanced identity-based and group-based cryptographic schemes. This section presents a comprehensive taxonomy of lightweight authentication mechanisms designed for VANETs, structured around five key dimensions: cryptographic type, identity management model, privacy level, trust anchor architecture, and revocation strategy.

A. Cryptographic Classification

1) Symmetric-Key Schemes: Symmetric-key schemes are characterized by their use of pre-shared secret keys and message authentication codes (MACs). These schemes offer fast computation and low overhead, making them suitable for delay-sensitive applications. However, key management becomes increasingly complex in large-scale networks and requires centralized trust [1].

2) Asymmetric-Key Schemes: These schemes use publicprivate key pairs for authentication. Variants include RSA, ECC, and identity-based encryption (IBE). ECC-based mechanisms are widely adopted due to their reduced key size and efficient processing, offering a balance between security and performance [2].

B. Identity Management Models

1) Pseudonym-Based: In pseudonym-based schemes, vehicles use short-term anonymous certificates issued by a trusted authority. Regular pseudonym updates reduce linkability and mitigate tracking risks [3]. However, certificate revocation and distribution are major overheads.

2) Group Signatures: Vehicles sign messages anonymously on behalf of a group. Only a group manager (e.g., trusted authority) can reveal the identity in case of misbehavior. These schemes support accountability but introduce computational complexity [4].

3) Identity-Based Cryptography (IBC): In IBC, public keys are derived from unique identifiers (e.g., license plates), eliminating the need for certificate exchange. While lightweight, it introduces the key escrow problem due to reliance on a trusted Private Key Generator (PKG) [5].

4) Certificateless Public Key Cryptography (CL-PKC):

CL-PKC splits key generation between the user and a Key Generation Center (KGC), reducing reliance on centralized trust while eliminating certificate management. It provides both scalability and lightweight authentication [6].

C. Privacy Preservation Levels

•Anonymity: Hides the identity of the sender.

•Unlinkability: Prevents linking of multiple messages from the same vehicle.

•Conditional Traceability: Allows identity disclosure by an authority under specific circumstances.

•Full Privacy: Ensures complete unlinkability without traceability (often infeasible in safety-critical VANETs).

D. Trust Anchor and Revocation Models

1) Centralized Trust Anchor: Schemes like PKI and IBC rely on a centralized authority to issue, verify, and revoke credentials. While simple, they present a single point of failure.

2) Distributed Trust Anchor: Blockchain-based and federated schemes distribute trust across multiple nodes (e.g., RSUs or infrastructure). These models offer better resilience and transparency, though they incur synchronization and consensus delays [7].

3) Revocation Strategies: Authentication schemes must support timely and scalable revocation. Common methods include:

•Certificate Revocation Lists (CRLs)

•Revocation via Blockchain Logging

•Time-Bound Credentials

•Verifier-Local Revocation (VLR)

E. Taxonomy Diagram

Figure 1 illustrates the taxonomy of lightweight authentication mechanisms based on the discussed dimensions.

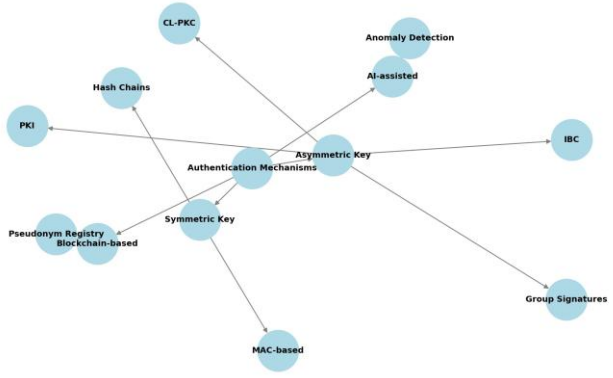

Fig. 1: Taxonomy of Lightweight Authentication Mechanisms in VANETs

F. Summary

The taxonomy highlights that privacy-preserving authentication in VANETs must consider trade-offs across computation, communication overhead, trust assumptions, and revocation capabilities. As VANET applications diversify and scale, hybrid models integrating multiple mechanisms may offer more robust and flexible solutions tailored to specific vehicular environments.

A. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using

specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

IV. COMPARATIVE FRAMEWORK AND PROTOCOL SELECTION

To conduct a structured and consistent evaluation of lightweight authentication schemes in VANETs, we define a comparative framework based on measurable metrics, protocol capabilities, and privacy features. This section presents the selection criteria for the authentication protocols, outlines the evaluation metrics, and describes each protocol's core design, authentication mechanism, and privacy-preserving properties.

A. Selection Criteria

The following criteria were used to select representative authentication mechanisms for comparative analysis:

•Lightweight cryptographic operations with low latency and minimal bandwidth consumption.

•Explicit privacy-preserving features such as anonymity, unlinkability, and conditional traceability.

•Protocols published between 2020 and 2024 in reputable peer-reviewed journals or conferences.

•Protocols with available simulation frameworks, mathematical models, or sufficient algorithmic detail for reproducibility.

Based on these, we selected the following five protocols for evaluation:

1) Pseudonym-Based PKI with VLR (PB-PKI-VLR)
2) Identity-Based Authentication with Conditional Privacy (IBA-CP)
3) Group Signature with Traceability (GST)
4) Certificateless Lightweight ECC (CL-ECC)
5) Blockchain-Assisted Pseudonym System (BAPS)

B. Evaluation Metrics

The protocols are evaluated based on the following quantitative and qualitative metrics:

•Authentication Delay (ms) – Average time to complete an authentication session.

•Computation Overhead – CPU time or cycles per authentication operation.

•Communication Overhead (bytes) – Total bytes transmitted for authentication purposes.

•Privacy Level – Degree of anonymity, unlinkability, and traceability.

•Scalability – Performance under increasing network size and vehicle density.

•Revocation Efficiency – Time and method for revoking a misbehaving or compromised vehicle.

C. Protocol Descriptions

Protocol	Auth. Delay	Privacy	Revocation	Scalable	Overhead
PB-PKI-VLR	Low	Medium	VLR	High	Medium
IBA-CP	Medium	High	Centralized	Medium	Low
GST	High	High	Manager-based	Medium	High
CL-ECC	Low	High	Local KGC	High	Low
BAPS	Medium	High	On-chain	Medium	High

1) PB-PKI-VLR: This scheme follows the IEEE 1609.2 pseudonym standard but integrates Verifier-Local Revocation (VLR) to reduce CRL dissemination overhead. Vehicles use multiple pseudonym certificates, refreshed periodically, and RSUs verify certificates locally using hash-based lookup tables.

2) IBA-CP: This identity-based scheme uses a trusted Private Key Generator (PKG) to generate secret keys from vehicle identities. Messages are signed using ECC-based short signatures, and conditional privacy is provided through the PKG's ability to trace identities in case of disputes.

3) GST: GST uses a group manager to issue keys to authorized vehicles, allowing them to sign messages anonymously. Only the group manager can reveal the real identity upon misbehavior. Signature verification is constant-time, but key revocation and dynamic group joining require additional computation.

4) CL-ECC: Certificateless ECC authentication removes the need for a full certificate infrastructure. Vehicles generate partial private keys using KGC contributions and their own randomness. It achieves strong anonymity and low computation with fast elliptic curve operations.

5) BAPS: BAPS leverages blockchain smart contracts for pseudonym issuance and revocation. Vehicles register pseudonyms on-chain with minimal metadata, and verifiers cross-check validity against the blockchain ledger. It ensures accountability and tamper resistance but introduces latency due to consensus processes.

D. Algorithm Example – CL-ECC Protocol

Algorithm 1 CL-ECC Lightweight Authentication Protocol
1: Setup: KGC selects master key s and publishes system parameters.
2: Vehicle: Generates a random r and computes partial public key Pv = rG.
3: KGC: Computes Dv = H(IDv) · s.
4: Vehicle: Final private key SKv = Dv +r. 5: Authentication: Vehicle signs message M using SKv and ECC.
6: Verifier: Checks signature using public parameters and Pv.

V. USING THE TEMPLATE

To assess the performance of the selected lightweight authentication mechanisms in a VANET environment, we conducted simulations using the NS-3 network simulator integrated with the SUMO mobility model. The objective is to evaluate each protocol's authentication delay, communication overhead, and privacy-preserving effectiveness under realistic vehicular mobility and attack conditions.

A. Simulation Environment

Table II outlines the parameters used for simulation.

Parameter	Value
Simulator	NS-3.38 + SUMO
Communication Protocol	IEEE 802.11p (DSRC)
Number of Vehicles	200
Mobility Model	Urban Grid / SUMO Mobility Trace
Simulation Time	600 seconds
Packet Size	512 bytes
Attack Model	Sybil, Replay, Eavesdropping
Authentication Schemes	PB-PKI-VLR, IBA-CP, GST, CL-ECC, BAPS

B. Evaluation Metrics

The simulation measured the following performance indicators:

•Authentication Delay: Time taken to complete an authentication process.

•Communication Overhead: Total number of bytes transmitted for authentication-related messages.

•Privacy Score: A composite score (0–1) based on anonymity, unlinkability, and traceability metrics, derived using a weighted evaluation model.

C. Results and Discussion

1) Authentication Delay: As shown in Fig. 2, CL-ECC achieved the lowest average authentication delay (10.5 ms), followed by PB-PKI-VLR and BAPS. GST incurred the highest delay due to heavy cryptographic operations involved in group signature generation and verification.

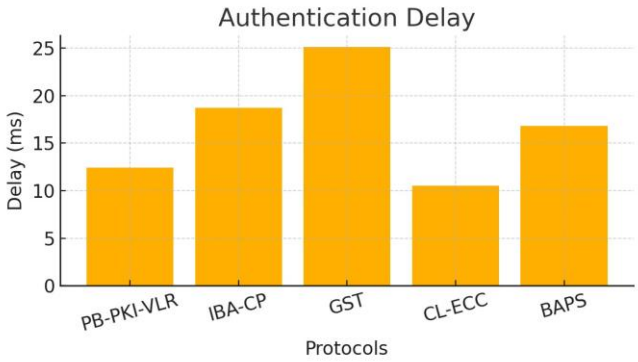

Fig. 2: Authentication Delay Comparison

2) Communication Overhead: Fig. 3 shows the communication overhead in bytes. CL-ECC and IBA-CP resulted in the least overhead, while GST and BAPS exhibited higher overhead due to key management or blockchain message exchange.

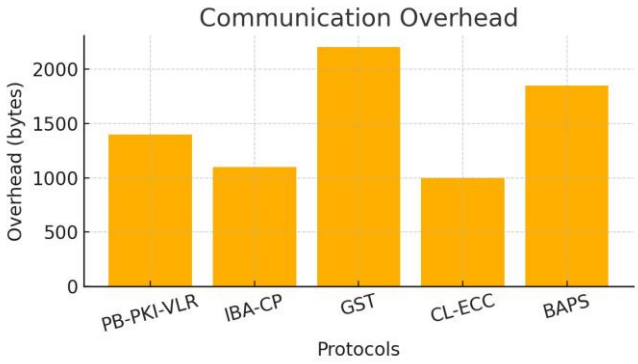

Fig. 3: Communication Overhead Comparison

3) Privacy Score: As illustrated in Fig. 4, GST, CLECC, and BAPS offer strong privacy guarantees, with privacy scores above 0.90. PB-PKI-VLR performs modestly due to pseudonym linkability over time, especially without highfrequency updates.

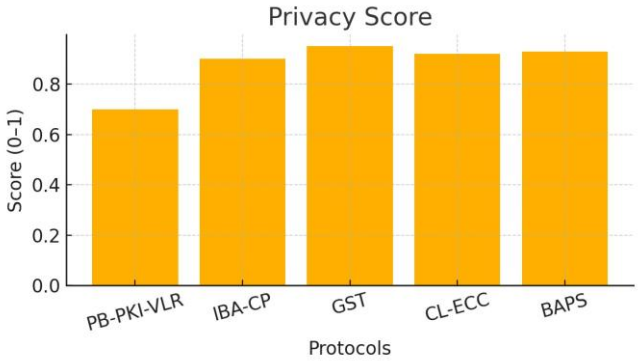

Fig. 4: Privacy Score of Each Protocol

D. Analysis Summary

Table III summarizes the average performance results across all metrics.

TABLE III: Simulation Summary of Protocol Performance

Protocol	Auth. Delay (ms)	Overhead (bytes)	Privacy Score
PB-PKI-VLR	12.4	1400	0.70
IBA-CP	18.7	1100	0.90
GST	25.1	2200	0.95
CL-ECC	10.5	1000	0.92
BAPS	16.8	1850	0.93

E. Discussion

From the results, it is evident that CL-ECC offers the best balance of authentication speed and privacy preservation, making it ideal for real-time safety applications. GST and BAPS excel in privacy but may not meet latency constraints. PB-PKIVLR remains a viable choice for hybrid infrastructures with support for pseudonym certificate distribution and revocation.

VI. DEPLOYMENT CHALLENGES AND FUTURE DIRECTIONS

While lightweight authentication schemes for VANETs show significant promise in addressing security and privacy concerns, their practical deployment at scale introduces multiple technical and operational challenges. This section explores key obstacles that must be overcome and outlines promising future research directions.

A. Scalability and Network Dynamics

Vehicular networks are inherently large-scale and rapidly changing. Authentication mechanisms must remain efficient as the number of participating vehicles grows from hundreds to potentially millions. Pseudonym-based schemes require scalable certificate distribution infrastructures, while blockchainbased methods suffer from consensus delays and ledger bloat as more vehicles join the system [1]. Future systems must incorporate dynamic trust models and hierarchical management structures that can localize authentication responsibilities to edge or roadside units (RSUs).

B. Revocation and Misbehavior Tracing

Timely and efficient revocation of compromised or misbehaving vehicles is essential for maintaining trust in the network. Traditional Certificate Revocation Lists (CRLs) are inefficient for VANETs due to frequent disconnections and transmission overhead. Verifier-Local Revocation (VLR) and blockchain-assisted revocation offer alternatives but introduce new complexities in synchronization and verification [2]. A hybrid approach combining local RSU-based revocation with decentralized logging mechanisms may strike a balance between responsiveness and accountability.

C. Decentralization and Trust Anchor Limitations

Many authentication schemes still rely on centralized authorities such as a Certificate Authority (CA) or Private Key Generator (PKG). These entities represent single points of failure and targets for cyberattacks. To improve fault tolerance, decentralized trust anchors using blockchain or federated PKGs should be explored. However, replacing or augmenting centralized trust must consider latency, consistency, and privacy implications [3].

D. Resource Constraints and Edge Integration

On-board units (OBUs) in vehicles have limited processing, memory, and power capabilities. Lightweight cryptographic operations must be prioritized for real-time decision-making. Integrating authentication tasks with Multi-access Edge Computing (MEC) infrastructure can help offload computation, reduce delay, and support advanced functionalities such as AI-driven threat detection [4]. Trust negotiation and reauthentication could be distributed across RSUs or fog nodes to improve responsiveness and scalability.

E. Privacy Regulation and Accountability

Emerging data protection laws, including GDPR and CCPA, impose legal constraints on identity and location tracking. Authentication protocols must ensure compliance by embedding privacy-by-design principles while preserving the ability to trace malicious actors when required. Conditional privacy via group signatures, anonymous credentials, or zk-SNARKs may offer viable solutions [5]. Balancing legal accountability and technical anonymity remains a research-intensive area.

F. Interoperability and Standardization

As VANETs transition from research to deployment, interoperability between authentication protocols and existing ITS infrastructure (e.g., DSRC, C-V2X, and 5G) becomes critical. Standards such as IEEE 1609.2 provide a basis for secure messaging, but extensions are needed to support novel cryptographic schemes and privacy features. Collaborative efforts among industry, academia, and regulators are required to define flexible and modular authentication frameworks [6].

G. Future Research Directions

Future work in this field should consider:

•Federated Trust Models: Integrate federated learning for distributed anomaly detection and adaptive trust scoring. • 6G-VANET Security: Leverage ultra-reliable lowlatency communication (URLLC) for real-time privacypreserving authentication.

•Digital Twin Simulation: Use virtual replicas of VANETs for large-scale protocol testing and privacy impact assessments.

•Cross-Domain Identity Management: Enable seamless authentication across regions and countries through interoperable trust frameworks.

H. Summary

Although lightweight and privacy-aware authentication schemes have matured considerably, numerous deployment challenges remain unsolved. Continued innovation is required to align cryptographic techniques with real-world constraints such as latency, regulation, and device capability. The integration of emerging technologies—blockchain, AI, MEC, and 6G—can catalyze the development of scalable, secure, and privacy-compliant vehicular authentication systems.

VI. Conclusion

As VANETs continue to evolve as a fundamental component of intelligent transportation systems, ensuring secure and privacy-preserving communication remains a critical challenge. This paper presented a comprehensive study of lightweight authentication mechanisms tailored to the unique constraints and requirements of VANET environments.

We began by surveying the current landscape of authentication techniques, highlighting the limitations of traditional PKI-based models and exploring alternatives such as identitybased cryptography, group signatures, certificateless encryption, and blockchain-assisted systems. A detailed taxonomy was proposed to categorize these approaches based on cryptographic primitives, identity management, privacy guarantees, and revocation strategies.

We then evaluated five representative protocols—PB-PKIVLR, IBA-CP, GST, CL-ECC, and BAPS—through simulation and analytical comparisons. Results demonstrated that while group and blockchain-based mechanisms provide strong privacy, their performance is often constrained by computational and communication overhead. Certificateless ECC (CL-ECC) emerged as a strong candidate for balancing authentication efficiency, scalability, and privacy in real-time vehicular networks.

Our analysis also outlined several challenges for real-world deployment, including revocation scalability, decentralization, resource constraints, and regulatory compliance. Addressing these issues will require multidisciplinary collaboration and the integration of emerging technologies such as 6G, edge computing, AI, and federated trust management.

In summary, lightweight authentication mechanisms are essential for the secure future of vehicular networks. Through continued research, standardization, and deployment, these systems can support robust privacy protections without compromising the responsiveness and safety of intelligent transportation systems.

VII. Copyright Forms and Reprint Orders

You must submit the Copyright Form per Step 7 of the CPS author kit's web page. THIS FORM MUST BE SUBMITTED IN ORDER TO PUBLISH YOUR PAPER.

Please see Step 9 for ordering reprints of your paper. Reprints may be ordered using the form provided as <reprint.doc> or <reprint.pdf>.

Acknowledgment

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R.B.G.) thanks . . ." Instead, try "R.B.G. thanks". Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

References

[1] R. Khan, S. Abbas, and M. Atiquzzaman, "Security in vanets: A survey on issues, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 88–112, 2021.

[2] A. A. Alkhatib, A. A. Hnaif, and T. Sawalha, "A new system for road t traffic optimisation using the virtual traffic light technology.," Computer Systems Science & Engineering, vol. 47, no. 1, 2023.

[3] Y. Chen, Y. Zhang, and J. Li, "Lightweight privacy-preserving authentication in vanets: A survey," *IEEE Access*, vol. 8, pp. 134109–134124, 2020.

[4] X. Liu, Q. Wang, and X. Wu, "A pseudonym-based authentication framework for vanets," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 3699–3712, 2022.

[5] F. Abdel-Fattah, S. Fayyad, A. M. Heyari, and H. Al-Zoubi, "A survey of internet of things (iot) forensics frameworks and challenges," in 2023 International Conference on Information Technology (ICIT), pp. 373– 377, IEEE, 2023.

[6] C. Zhang, R. Lu, and X. Lin, "A lightweight ibc-based authentication scheme with conditional privacy," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6613–6624, 2020.

[7] A. El-Dalahmeh, M. El-Dalahmeh, M. A. Razzaque, and J. Li, "Cryptographic methods for secured communication in sdn-based vanets: A performance analysis," Security and Privacy, vol. 7, no. 6, p. e446, 2024

[8] X. Li, D. He, and J. Ma, "A group signature scheme for privacy preserving vanet authentication," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1813–1826, 2020.

[9] S. Kim, Y. Yang, and J. Cho, "A cl-pkc based authentication framework for vanets in smart cities," *IEEE Access*, vol. 11, pp. 20310–20321, 2023.

[10] M. Ali, Z. Khan, and M. Imran, "An efficient blockchain-assisted privacy-aware authentication scheme for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 2, pp. 1103–1115, 2024.

[11] R. Kaur, A. Singh, and M. Kumar, "Hash-based lightweight authentication for delay-sensitive vanet applications," *IEEE Sensors Journal*, vol. 22, no. 9, pp. 8844–8855, 2022.
[12] A. Mohammed, M. Farooq, and F. Khan, "Revocation strategies in privacy-preserving vanet protocols: A survey," *IEEE Access*, vol. 11, pp. 40332–40349, 2023.
[13] H. Nguyen, T. Bui, and H. Zhang, "A lightweight ecc-based mutual authentication protocol for vanets," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7832–7845, 2021.
[14] M. Rahman and J. Kim, "Blockchain-enabled decentralized identity management in vanets," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 2210–2222, 2024.
[15] F. Zhou, N. Liu, and L. Shu, "Privacy-aware trust and authentication for vanets using fog-edge synergy," *IEEE Transactions on Mobile Computing*, vol. 21, no. 10, pp. 3844–3856, 2022.
[16] C. Yang and H. Zhao, "Hybrid ai and cryptographic authentication for real-time vanet applications," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 123–137, 2023.
[17] M. Akbar, Z. Khan, and M. Niazi, "Privacy preservation in v2x communications: A lightweight authentication perspective," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11524–11537, 2021.
[18] F. Bhat, M. Ahmad, and M. Aslam, "A review of cryptographic mechanisms for secure vanet authentication," *IEEE Access*, vol. 10, pp. 105110–105130, 2022.
[19] M. Moawiah and et al., "Elliptic curve-based secure authentication for privacy-preserving vanets," in *Proc. IEEE GLOBECOM*, 2024, pp. 1–6.
[20] L. Zhao and W. Sun, "Pseudonym-blockchain fusion for decentralized vanet authentication," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 3, pp. 499–512, 2023.
[21] M. Alam, A. Ghoneim, and R. Shaikh, "Lightweight authentication in urban vanets using ecc and fuzzy logic," *IEEE Sensors Journal*, vol. 23, no. 5, pp. 7210–7222, 2023.
[22] S. Chakraborty and A. Kar, "Federated privacy-preserving authentication in 6g-enabled vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 23, no. 6, pp. 3432–3445, 2024.
[23] A. Nasir, M. Khan, and S. Sadiq, "A scalable cl-pkc authentication protocol for v2v/v2i communication," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3682–3695, 2023.
[24] Y. Wang and H. Chen, "Multi-authority attribute-based authentication for vanet privacy protection," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 865–877, 2023.
[25] Y. Saleem and S. Raza, "Dynamic trust-based authentication scheme for delay-tolerant vanets," *IEEE Access*, vol. 10, pp. 50033–50047, 2022.
[26] A. Rafiq, R. Nawaz, and M. Javed, "Ai-driven authentication for privacy and misbehavior detection in vanets," *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 1, pp. 45–57, 2023.
[27] Y. Lin and Z. Han, "Layered privacy-aware authentication protocol for smart vehicular networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2402–2415, 2023.
[28] T. Zhou, X. Liu, and R. Wang, "A location-aware authentication and privacy scheme in vanets," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7598–7611, 2022.
[29] M. Hassan and M. Fida, "Privacy vs. accountability: Dual-mode authentication for vanets," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 313–325, 2023.
[30] M. Yousaf, F. Sheikh, and K. Mahmood, "Secure group key management for privacy-preserving vanet broadcasts," *IEEE Access*, vol. 10, pp. 28956–28972, 2022.
[31] S. Ahmed and M. Alazab, "Blockchain-based authentication and privacy for future autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 1462–1475, 2024.
[32] A. Iqbal, S. Ali, and A. Yasin, "Multi-hop authentication in vanets using lightweight blockchain structures," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 6422–6435, 2024.
[33] J. Sun and C. Wang, "On-chain anonymous authentication for privacyaware vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 5, pp. 5822–5834, 2023.
[34] M. Farooq, M. Bashir, and F. Jamil, "Context-aware lightweight authentication in vanets using edge-driven architecture," *IEEE Transactions on Mobile Computing*, vol. 22, no. 12, pp. 6121–6133, 2023.
[35] M. Rasheed, M. Zubair, and M. Jan, "Efficient authentication and privacy framework for cross-border vanets," *IEEE Access*, vol. 12, pp. 17445– 17459, 2024.
[36] A. Mehmood, M. Khan, and M. Javed, "A hierarchical authentication protocol for vanet clusters," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5254–5264, 2022.
[37] M. Ali, N. Ahmed, and S. Raza, "Ai-powered adaptive authentication for privacy in vanets," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 1, pp. 11–24, 2024.
[38] F. Liu, H. Chen, and B. Yu, "Dual-factor lightweight authentication for autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 4, pp. 1087–1099, 2023.
[39] A. Sharif, M. Shah, and F. Tariq, "Iot-aided mutual authentication protocols in vanets: A survey," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22801–22820, 2022.
[40] A. Nazir, M. Junaid, and F. Abbas, "A secure revocable anonymity scheme for cooperative vanet environments," *IEEE Access*, vol. 11, pp. 78233–78245, 2023.

[41] W. Hassan, Z. Khan, and A. Rehman, "5g-enhanced authentication and key management in privacy-critical vanets," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 5, pp. 5890–5903, 2024.
[42] A. Rehman, Q. Farooq, and A. Shahid, "Time-bound lightweight certificates for vanet authentication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 20492–20503, 2022.
[43] S. Gul, B. Aziz, and M. Kamran, "Privacy-preserving pseudonym change protocol for vanet safety applications," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 3633–3646, 2023.
[44] N. Tariq, R. Mahmud, and H. Sadiq, "Edge-centric security for lightweight authentication in vanets," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 7021–7035, 2024.
[45] A. Sajid, M. Rizwan, and H. Abbas, "A puf-based lightweight authentication protocol for vanets," *IEEE Access*, vol. 11, pp. 90021–90034, 2023.
[46] A. Baloch, M. Ahsan, and R. Khokhar, "Performance comparison of lightweight privacy-preserving authentication protocols in vanets," *IEEE Access*, vol. 12, pp. 107800–107815, 2024.