IJETIR
ISSN (Online) 2583-0554
IJETIR
Impact Factor: 5.731
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025

Ensuring Privacy in the 6G-Enabled Internet of Vehicles: A survey on current Solutions, Challenges, and Future Directions

Vijayalaxmi S Sadlapur and Nayana Hegde
Senior Grade Lecturer, Reva University, Bengaluru, India
Assistant Professor, Reva University, Bangaluru India
vijayalaxmis_12@rediffmail.com and nayana.srikanth@gmail.com

Abstract: *The Internet of Vehicles (IoV) has emerged as a transformative technology in Intelligent Transportation System (ITS), enabling seamless connectivity between vehicles, infrastructure, and devices. However, as IoV systems evolve, they face complex security and privacy challenges, especially in light of increasing connectivity, data sharing, and the integration of 6G networks. Existing security solutions, including blockchain-based schemes and authentication protocols, often struggle with scalability, resource efficiency and latency requirements. This survey systematically reviews the landscape of privacy-preserving and secure IoV solutions, assessing recent advancements in cryptographic techniques, decentralized trust management, and emerging quantum-resistant protocols. By identifying significant research gaps this paper highlights areas where future research can innovate to meet IoV's demanding security and privacy needs. The findings aim to guide the development of robust, adaptive solutions for secure, high-speed, and privacy-conscious IoV networks in an increasingly connected vehicular ecosystem.*

Keywords: Internet of Vehicles (IoV), Privacy-preserving solutions, Cryptographic techniques, Quantum-resistant protocols, Scalable frameworks

I. INTRODUCTION

To meet the large-scale and big-data demands in the mobility world, i.e., ITS, the conventional connected vehicles are evolving from V2X communication to IoV. V2X communication technology has evolved in three stages [1]. The first stage focused on ITS telematics. The second stage focused on advanced auxiliary driving. In the third stage, with the inclusion of 5G, V2X can support advanced

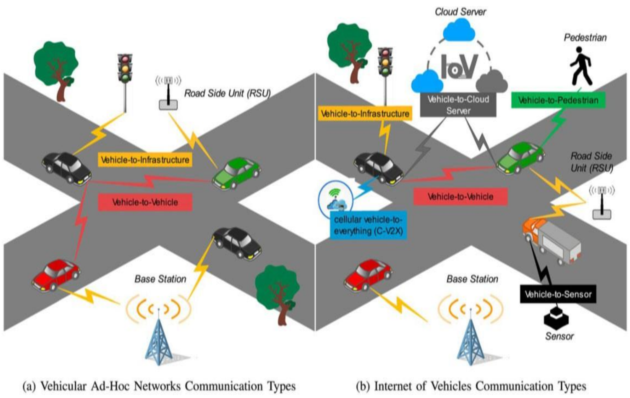

Figure 1 shows the comparison of communication types between IoV and VANETs [2]

automotive applications, resulting in IoV. IoV provides real-time network access for emerging automotive applications such as cooperative automatic driving and environmental perception, intelligent traffic control with the assistance of big data paradigm and cloud computing regime.

Table 1 The differences between VANET and IoV

Parameter	VANET	IoV
Goal	Improve traffic safety to avoid causalities and enhance traffic effectiveness	Enhance traffic safety, effectiveness and commercial infotainment for passengers to improve the driving experience
Communication types	V2V and V2I	V2V, V2R, V2I, V2S, and V2P
Network connectivity	Composed of singleton network architecture that restricts their use	Uses radio, Wi-Fi,4G/LTE and satellite networks
Decision making	Intelligent decisions are not possible	Intelligent decisions are possible based on AI, big data, and data mining computations
Cloud computing	Not supported due to unreliable Internet connectivity and limited data size	Supported due to the presence of vast real-time traffic information
Data size	Limited due to local information and non- collaboration	No limitation as a vast amount of data can be generated in real time

Table 2 The differences between IoV and SDV [3]

Aspect	Internet of Vehicles (IoV)	Software-Defined Vehicles (SDV)
Definition	A network of vehicles that communicate with each other, infrastructure, and devices	A vehicle where functionality is primarily driven and updated y software.
Focus	Communication and connectivity between vehicles and the environment	Vehicle functionality, control, and adaptability through software
Core Technology	Relies on V2X communication	Relies on embedded systems, cloud integration, software updates
Objective	Enable real-time communication for traffic management, safety, and navigation	Enhance flexibility, user experience, and functionality via software
Updates and Adaptation	Focus on enhancing network and communication protocols.	Enables OTA updates for vehicle features and bugs

The importance of researching the Internet of Vehicles (IoV) has increased due to recent developments in wireless communication technology. An important development in ITS, particularly with regard to wireless network technologies, is the IoV [4]. The swift expansion of open wireless networks has often led to privacy violations. In the context of the IoV, maintaining a secure connection and safeguarding privacy are essential elements. Every node in an IoV network sends messages to neighbouring nodes via a dedicated short-range communication (DSRC) protocol [5]. This novel idea in the IoV, aims to improve the capabilities of Vehicular Ad-Hoc Networks (VANETs) and make connection with the Internet of Things easier. Improved connection between automobiles and other infrastructure elements, including Road Side Units (RSU), buildings, and other objects, is made possible by the IoV. Vehicles using intelligent devices, such as wireless sensors on onboard units (OBU), can gather a substantial quantity of perceptual data. A growing number of businesses and organizations, such as Apple, Google, and Tesla, are methodically gathering and evaluating perceptual data in order to improve service offerings like intelligent guidance, energy management, and traffic monitoring [6].

One essential element of the IoV is privacy protection. Privacy protection is the blockchain-based architecture used by the IoV is intended to secure user data from unwanted access, guaranteeing privacy. The system complies with legal requirements and employs a number of privacy-preserving techniques. To preserve privacy, the IoV uses a technique called Authentication Key Agreement (AKA). Users use a shared secret key to expedite authentication procedures. Implementing a secret key to improve authentication procedures reduces the risk factor for IoV applications. User IDs, key values, and confidential information are all included in the secret key [7]. The AKA system protects user data against unwanted access, which improves the effectiveness and efficiency of the IoV. The blockchain technique points out flaws

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Impact Factor: 5.731
Volume 5, Issue 12, December 2025

in the authentication procedure and suggests fixes. Through engagement services, the blockchain method makes it easier to compute shared data while protecting against unwanted access for IoV applications. A privacy-preserving method based on the Deep Q- Network (DQN) algorithm is put into practice for IoV networks. The DQN method is used to identify traffic signals during the authentication process. These DQN algorithm gives users effective interaction capabilities while maintaining the protocol's integrity [8].

The current study on vehicular network attack identification utilizing digital twin technology does not adequately address the performance metrics of the 6G IoV network, such as detection rate, accuracy, and F1- score. The deployed solutions static paradigm is incompatible with 6G IoV networks. These networks diverse designs and the range of attack methods necessitate adaptable solutions. Moreover, they exhibit instability in a variety of datasets. A 15% discrepancy in performance outcomes, for instance, is revealed by comparing the performance findings from references across two datasets. The two datasets differed by around 25%, according on the performance findings of the random forest and decision tree methods shown in [13]. In the rapidly evolving 6G IoV space, the existing solutions are unreliable and inadequate for handling a range of threats. In 6G IoV situations, a better approach is needed to provide steady performance while dynamically detecting threats.

By combining environmental awareness, information sharing, and cooperative control mechanisms for vehicle operation and traffic management systems, the IoV improves road safety and traffic efficiency. The IoV with 6G capability has a lot of promise, but in order to realize its full potential, a number of issues need to be resolved [15]. The IoV presents serious security and privacy issues because of its intrinsic openness and dynamic nature. Attackers are able to carry out a variety of assaults that have the potential to interfere with the system's regular operation or reveal private data pertaining to automobiles. These assaults include, for instance, message linking, manipulation, and impersonation [11].

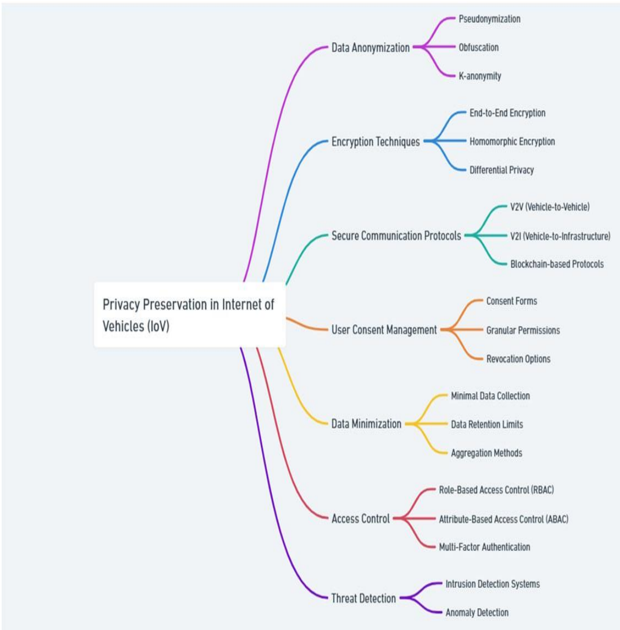

Figure 2 Mind map for privacy preserving in IoV

Figure 2 encompasses various techniques to ensure secure and confidential data handling for privacy preservation in the IoV . Data anonymization plays a key role in masking sensitive information. Techniques such as Pseudonymization modify data to prevent direct identification of individuals unless additional information is used. Obfuscation further protects information by making it difficult for unauthorized users to interpret, while K-anonymity ensures that data for any individual is indistinguishable from that of at least k other people, reducing re-identification risks.

Encryption techniques form the backbone of secure data transmission in IoV. End-to-End Encryption keeps data encrypted from sender to recipient, preventing unauthorized access. Homomorphic Encryption takes this further by allowing computations on encrypted data without the need for decryption, thus preserving privacy during data processing.

Differential Privacy adds controlled noise to data, enabling analysis without exposing specific details about individuals, which is crucial for privacy in aggregated data usage. For secure interactions between vehicles and infrastructure, Secure communication protocols are vital. V2V communication facilitates safe exchanges between vehicles, which is essential for cooperative driving and traffic safety. V2I protocols enable secure connections between vehicles and external infrastructure, supporting a wide range of applications like traffic management. Additionally, Blockchain-based protocols offer a decentralized and transparent approach to secure data exchanges, ensuring data integrity and enhancing trust among IoV stakeholders.

To empower users with control over their data, User consent management systems are implemented. Consent forms that explicitly gather user permission for data usage, ensuring transparency. Granular permissions allow users to specify the extent of data sharing, increasing trust in the system. Moreover, Revocation options give users the flexibility to withdraw their consent, enabling them to control data exposure over time.

Data minimization is another essential aspect, focusing on reducing the amount of data collected to what is strictly necessary. Minimal data collection ensures only essential information is gathered, decreasing the risk of data misuse. Data retention limits set boundaries on how long data can be stored, which lowers the risk of privacy violations. Through Aggregation methods, data is combined in a way that preserves useful insights without exposing individual information, thus protecting privacy.

Access control mechanisms regulate who can access data, thereby safeguarding sensitive information. Role- Based Access Control (RBAC) restricts data access according to user roles, ensuring that only authorized personnel have access. Attribute-Based Access Control (ABAC) offers more nuanced control by determining access based on specific user attributes. To further secure access, Multi-Factor Authentication adds additional verification steps, reducing the likelihood of unauthorized entry into the system.

Lastly, Threat Detection is crucial for identifying and mitigating potential security threats. Intrusion detection Systems continuously monitor network activity to detect any unusual or unauthorized behaviour. Additionally, Anomaly detection methods identify deviations from normal patterns, which may indicate privacy breaches or malicious activities, enabling timely responses to protect the IoV ecosystem. Together, these privacy-preserving measures form a comprehensive framework that enhances user trust, ensures data security, and supports safe communication within the IoV, addressing privacy challenges in an increasingly connected vehicular environment.

A. Challenges

Scalability of Privacy-Preserving Mechanisms: With the exponential growth of connected vehicles, current privacy-preserving solutions often struggle to scale effectively. Many existing mechanisms, such as blockchain and cryptographic protocols, introduce significant computational and communication overheads, making them less feasible for large-scale IoV deployments.

• Balancing Privacy and Traceability: Ensuring user privacy while enabling traceability for accountability poses a challenge. Many privacy-preserving solutions rely on pseudonymization, yet it remains challenging to strike a balance where privacy is maintained, but malicious vehicles can still be identified by authorities when necessary.

• Resource Constraints in Vehicular Networks: IoV devices, including On Board Units (OBUs) and RSUs, are often resource-constrained in terms of processing power, memory, and energy. Implementing intensive privacy-preserving and security protocols can strain these limited resources, impacting the overall performance of the network.

• Real-Time Data Processing and Low Latency Requirements: IoV applications require quick response times to support real-time decision-making for safety-critical applications. Privacy-preserving mechanisms that involve high computational costs can lead to delays, which conflict with the low- latency demands of IoV systems, especially in 6G-enabled environments.

• Heterogeneity and Dynamic Topology of IoV: IoV networks are highly heterogeneous, consisting of various types of vehicles, sensors, and infrastructure. Additionally, the network topology is dynamic due to vehicle mobility, making it challenging to develop consistent, adaptive privacy-preserving mechanisms that cater to diverse devices and changing conditions.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Impact Factor: 5.731
Volume 5, Issue 12, December 2025

• Vulnerability to Emerging Cybersecurity Threats: IoV networks are susceptible to various cybersecurity attacks, including impersonation, modification, and message replay attacks. As quantum computing progresses, traditional cryptographic solutions may also become vulnerable, creating an urgent need for quantum-resistant privacy-preserving protocols to ensure long-term security.

• Data Sharing and Privacy Regulation Compliance: IoV systems often require the collection and sharing of sensitive data, such as location and personal information, raising concerns about compliance with privacy regulations like General Data Protection Regulation (GDPR). Designing privacy-preservingframeworks that align with regulatory requirements while maintaining functional efficiency in IoV systems remains a complex challenge.

These challenges underscore the need for innovative, resource-efficient, and scalable privacy-preserving solutions tailored to the unique demands of IoV environments.

B. Contribution

The motivation for this survey paper arises from the critical need to address security, privacy, and performance challenges within the IoV ecosystem. As IoV technology advances, enabling seamless interactions between vehicles and infrastructure, it also introduces significant vulnerabilities, particularly concerning identity privacy and secure data exchange in a highly dynamic and open wireless environment. While various privacy-preserving methods and security protocols, such as blockchain and AKA schemes, have been explored, existing solutions often face limitations like computational overhead, communication delays, and scalability issues. Moreover, the transition toward 6G networks intensifies these challenges, demanding more efficient, scalable, and adaptable approaches to manage the increased data traffic and heterogeneity in IoV systems. This survey aims to systematically analyse current advancements, identify gaps, and evaluate emerging technologies and methodologies that promise to enhance privacy, authentication, and network efficiency in IoV, ultimately guiding future research toward developing robust, real-time IoV security solutions.

• Comprehensive Analysis of Privacy-Preserving Security Solutions for IoV: This survey paper provides critical insights into the current landscape towards adaptability to 6G enabled IoV's privacy and security solutions through in-depth examination of existing privacy preserving security schemes.

• Identification of Gaps and Challenges in Privacy Preservation for IoV: The survey emphasizes the need for lightweight and privacy-focused security frameworks to ensure secure and efficient data exchange without compromising user anonymity, scalability, computational overhead, and adaptability in high- speed vehicular networks.

• Guidance for Future Research in Privacy-Preserving IoV Security: By considering the unique demands of 6G enabled IoV, this paper proposes avenues for integrating emerging technologies like edge intelligence and federated learning.

II. RELATED WORK

Recent advancements in 6G-enabled IoV have heightened concerns regarding data privacy and security [16], identify decentralized management as a primary challenge in the implementation of the IoV network architecture. The research paper outlines a decentralized trust management approach specifically designed for the IoV network. This method employs a fuzzy logic-based approach for the computation of direct trust levels. This method employs trustee nodes located within the transmission range of a trustor node. Reinforcement learning serves as an additional approach for evaluating trust, particularly in scenarios where the actions of the trustee are not immediately observable. The integration of fuzzy logic with reinforcement learning may lead to heightened processing overhead, especially in resource-constrained devices within vehicular networks. Additionally, regular exchanges of trust information among nodes could lead to increased communication expenses.

AKM-IoV [17] represents a lightweight authentication method and key management system specifically developed for an IoV environment utilizing fog computing technology. The three phases of authentication key management in the Internet of Vehicles (AKM-IoV) include the management of authentication keys between a vehicle and a fog server, between a fog server and RSU, and between a cloud server and a fog server. Each of the three steps incorporates mutual authentication, establishing a secure session that relies on a shared secret session key. The protocol necessitates multiple message exchanges and cryptographic procedures for key formation, potentially leading to increased communication and processing overhead. Additionally, vulnerabilities can arise if the process for adding additional nodes to the network is not executed properly.

Table 3 Comparison of performance and limitations of various privacy schemes

Ref	Method	Advantages	Disadvantages	Research Gap
[13]	SVeriFL	Integrity and correctness verification using BLS signatures. Privacy- preserving with CKKS homomorphic encryption. Ensures consistency of server responses across participants.	Potential computational overhead from BLS signatures and MPC. Approximation errors due to CKKS encryption.	Scalability in large-scale federated environments. Real-time performance impacts.
[17]	Blockchain and Collaborative Service-based Conditional Privacy-Preserving (BCS-CPP)	Reduces the need for public key certificate management through smart contracts. Eliminates key escrow issues with decentralized blockchain technology. Sustains minor computational and communication overhead regardless of user count. Maintains privacy during location-based service queries. Enhances collaborative efficiency within the IoV ecosystem.	Dependency on blockchain performance and scalability. Potential delays in transaction processing due to blockchain consensus mechanisms. Requires widespread adoption of blockchain technology within the IoV infrastructure for optimal functionality.	Further investigation is needed into the blockchain's ability to handle ultra- high transaction volumes typical in dense IoV environments. Exploration of the trade-offs between real- time responsiveness and privacy/securit y levels provided by blockchain technology. Need for robustness testing against novel attack vectors specific to IoV and blockchain integration.
[19]	Privacy-Preserving Multi-Modal Implicit Authentication Protocols	Uses password and behavior features for robust security; ensures privacy of behavior features.	Relies on consistent behavior feature collection; needs significant computational resources.	Needs more reliable behavior feature detection and scalability solutions.
[20]	Conditional Privacy-Preserving Authentication Scheme with Hierarchical Pseudonyms (CPAHP)	Protects vehicle identities and tracks, enables recovery of identities of malicious vehicles, supports batch verification for efficient message handling, integrates blockchain for smooth traffic data sharing.	Dependency on the reliability of the blockchain network, Potential complexity in managing hierarchical pseudonyms.	Needs optimization for managing pseudonyms and blockchain integration in ultra-dense IoV scenarios
[21]	Conditional Privacy-Preserving Authentication (CPPA) based on ECC	Uses ECC for strong security, incorporates batch verification via small exponent test to handle multiple messages efficiently, provides anonymous authentication using real identities transformed into anonymous ones.	Potentially complex implementatio n of ECC and management of anonymous identities, dependency on the robustness of the small exponent test for batch verification.	Optimization of the anonymous identity generation and management process, further reduction in computational overhead, and exploration of real-world application scalability.
[27]	ID-CPPA	Efficient authentication of high-volume vehicular communications using one- way hash functions.	Potential scalability issues in ultra- dense network scenarios.	Exploration of the scheme's performance in ultra-dense vehicular environments.

		Supports batch signature verification, reducing computational overhead. Security assured under the Inv-CDH problem in the ROM.	Dependency on the robustness of the bilinear map, which may affect performance under different network conditions.	Assessment of real-world implementatio n challenges and overhead beyond theoretical models.

The authors in reference [18] presented a dynamic spectrum sharing system for Internet-of-Things (IoT) networks utilizing blockchain technology. The process of spectrum sharing is represented through a double auction procedure, facilitating the exchange between the resource provider and the requester. This mechanism effectively aligns supply and demand, allowing for participation from both parties [19].

The authors in [20] proposed a resource-sharing architecture to manage dynamic resource-sharing scenarios. This design integrates a two-stage Stackelberg game with multi-agent deep reinforcement learning (MADRL) and blockchain technology. This study employs UAVs to function as the ABS, thereby enhancing MDs' financial advantage through the aggregation of energy and spectrum resources. The blockchain records resource-sharing transactions conducted by the MEC nodes upon achieving consensus through the PBFT-based proof-of-reputation (PoR) technique. Within the framework of autonomous resource slicing in the 5G RAN, the authors of [21] proposed a hierarchical resource trading system designed for peer-to-peer mobile virtual network operators (MVNOs) utilizing blockchain technology. This research employed a two-stage Stackelberg game framework to determine pricing and demand strategies involving a sole vendor and multiple buyers. Furthermore, [22] introduces a blockchain-based spectrum trading system designed for the autonomous creation and modification of slices between spectrum suppliers (infrastructure providers) and customers (MVNOs). This paper models the pricing and spectrum demand dynamics among infrastructure providers, seller MVNOs, and buyer MVNOs through a three-stage Stackelberg game framework. The initiatives discussed primarily targeted incentives for resource providers and requestors, lacking the development of incentive systems that effectively promote consensus nodes [23].

[24] have developed a conceptual framework for Proof of AI (PoAI), which is an energy-efficient consensus method designed to ensure the security and decentralization of a blockchain system. The machine learning approach is utilized to achieve efficient leader election and to establish a unique dynamic block creation mechanism. [25] proposed a blockchain-assisted cross-domain protocol designed for communications within the industrial internet of things (IIoT). Their method, while distinctive to cross-domain applications, incurs significant computational and communication costs. This is because this method requires multiple read and write operations on the blockchain. proposed an improved method for cross-domain IIoT communications, differing from the approach. Conversely, the computational and transmission costs associated with this scheme remain significantly elevated. Xue et al. [21] have introduced a cross-domain protocol for medical consortiums. The protocol, while distinctive to cross-domain applications, remains vulnerable to distributed denial of service (DDoS) attacks. One protocol supports cross-domain V2V communications however, the computational and transmission overhead is significantly high.

[26] This document presents an effective certificateless aggregate signature method designed to protect privacy under specific circumstances. The proposed strategy reduces processing overhead and bandwidth resource utilization through the implementation of a full aggregation technique. The IoV system employs a pseudonym strategy to ensure the maintenance of conditional privacy. Within the framework of the random oracle model, we demonstrate that the proposed system is secure against Type-I and Type-II adversaries, contingent upon the computational Diffie-Hellman assumption. The computing cost, communication effectiveness, and security requirements of the proposed approach are evaluated in comparison to those of related research.

[27] PPIoV is presented as a solution that utilizes Blockchain technology and Federated Learning (FL) to enhance vehicle privacy within the Internet of Vehicles framework. Conventional machine learning methods are unsuitable for application in networked and highly dynamic systems such as the Internet of Vehicles, as they are designed to train on data that displays local features. Federated learning facilitates the training of a global model while ensuring the protection of privacy throughout the process. The methodology employed involves a system designed to assess the reliability of the

vehicles utilized in the federated learning training process. Additionally, PPIoV employs blockchain technology to establish trust among various communication nodes. The cloud utilizes local learned model updates from vehicles and fog nodes to enhance the global learned model, with transactions occurring on the blockchain.

[28] Develop a reliable platoon recommendation system that emphasizes privacy considerations. This essay presents several advantages in comparison to existing methodologies. The feedback report collection procedure does not disclose any personal information or the weight of member vehicles. The fog node and cloud service provider employ an iterative methodology to enhance the reputation of PH automobiles, considering the high- speed mobility and technical limitations of the vehicles, irrespective of member vehicle engagement. The proposed method meets the criteria for IoV security, as indicated by the security analysis. Several studies in 2024 [29-30] have addressed these challenges, proposing innovative solutions to enhance privacy in this domain. [31] critically examine the integration of joint communication and sensing (JCAS) in 6G networks, highlighting potential privacy breaches such as location tracking and identity disclosure. They propose an enhanced JCAS architecture incorporating additional network functions to manage sensing policies and consent information, aiming to align with privacy regulations like the GDPR. [32] introduce Zero-X, a blockchain-enabled open-set federated learning framework designed to detect zero-day attacks in IoV. By combining deep neural networks with open-set recognition and leveraging blockchain for decentralized federated learning, Zero- X aims to protect user privacy while effectively identifying novel threats. [33] propose QEPP, a Quantum Efficient Privacy Protection Protocol tailored for 6G-quantum IoV ecosystems. This protocol addresses the surge in user numbers and data volumes by ensuring network security and privacy protection, while also mitigating the challenges associated with inadequate cloud computing resources.

Table 4 Comparison of performance and limitations of various privacy schemes

Ref	Method	Advantages	Disadvantages
[34]	Blockchain- Based Privacy Framework	Ensures data immutability and transparency	High computational overhead
[35]	Federated Learning for Vehicular Networks	Decentralized data training reduces privacy risks	High communication cost
[36]	Differential Privacy Mechanism	Prevents leakage of sensitive data during data sharing	Trade-off between data utility and privacy
[37]	Homomorphic Encryption for Data Privacy	Allows secure data processing without decryption	Computationally intensive
[38]	Vehicular Edge Cloud Privacy Model	Reduces latency and increases local data processing	Vulnerable to edge attacks
[39]	Secure Multi- Party Computation	Ensures privacy- preserving collaborative computations	High latency and energy consumption
[40]	Anonymous Authentication Protocol	Ensuresprivacy through pseudonym-based user authentication	Pseudonym management complexity
[41]	Trusted Execution Environment (TEE)-Based Privacy	Isolates and secures data computation in IoT devices	Limited scalability due to hardware dependency
[42]	Lightweight Cryptography Scheme	Reduces computational overhead in resource- constrained environments	May compromise security levels
[43]	Privacy- Aware Traffic Management Protocol	Optimizes data sharing while preserving	High overhead in maintaining traffic-related privacy policies
[44]	AI-Powered Privacy Preservation Framework	Detects and mitigates privacy risks dynamically	Vulnerable to adversarial attacks
[45]	Conditional Privacy- Preserving Scheme	Provides privacy control based on user- defined conditions	Requires continuous user participation

[47]	Quantum Cryptography for IoV	Provides high security using quantum keys	Implementation complexity and high cost
[47]	Decentralized Identity Management	Avoids centralized data storage, ensuring user privacy	Requires significant storage and network resources
[48]	Location Privacy Preservation Techniques	Protects user location information against tracking	Trade-offs between privacy and service quality
[49]	Privacy- Enhanced Vehicular Fog Computing	Improves data processing efficiency with privacy enhancements	Susceptible to fog node attacks
[50]	Biometric- Based Authentication	Provides robust and user-friendly privacy-preserving access	Risk of biometric data leakage
[51]	Privacy- Preserving Blockchain Consensus	Combines blockchain security with enhanced user privacy	High energy consumption
[52]	Cooperative Privacy Preservation Protocol	Ensures privacy through cooperation among vehicles	Vulnerable to insider attacks
[53]	AI-Driven Privacy Risk Assessment	Proactively identifies and addresses potential privacy risks	Relies on accurateand sufficient training data

A. Research gap

• Scalability of Privacy-Preserving Solutions: Current privacy-preserving mechanisms, such as blockchain and cryptographic protocols, often struggle to scale effectively for large, dynamic IoV networks. There is a need for lightweight and scalable solutions that maintain security and privacy as the number of connected vehicles grows.

• Efficient Balance Between Privacy and Accountability: Many solutions focus on privacy preservation, yet few provide an effective balance between maintaining user anonymity and enabling traceability when required, such as identifying malicious vehicles. Research is needed to develop frameworks that support conditional privacy without compromising accountability.

• Resource-Efficient Privacy Techniques for IoV Devices: IoV devices, such as onboard units (OBUs) and roadside units (RSUs), are typically limited in computational power, memory, and energy. Current solutions often overlook these constraints, highlighting a gap for resource-efficient privacy-preserving techniques specifically designed for IoV environments.

• Adaptability to High Mobility and Dynamic IoV Topologies: The constantly changing topology of IoV networks, due to high mobility, challenges the effectiveness of static privacy-preserving protocols. Research is needed to design adaptive security and privacy mechanisms that respond dynamically to the shifting network structure.

• Quantum-Resistant Privacy Protocols: As quantum computing advances, traditional cryptographic methods may become susceptible to attacks. Few existing IoV security solutions address this future risk, indicating a gap for developing quantum-resistant cryptographic techniques to ensure long-term privacy and security.

• Real-Time Processing of Privacy-Preserving Protocols: Privacy-preserving solutions that meet the low-latency requirements of real-time IoV applications are limited. There is a need for research focused on designing high-speed, privacy-preserving protocols that support real-time decision-making in IoV systems without causing delays.

• Integration of Privacy with Data Regulation Compliance: With increasing data privacy regulations, like GDPR, IoV systems face challenges in managing compliance while enabling effective data sharing. Current research lacks comprehensive frameworks that align privacy-preserving measures with regulatory requirements, indicating a gap for regulation-compliant privacy frameworks for IoV.

III. CONCLUSION

In conclusion, the IoV holds immense potential to revolutionize transportation by enabling secure, interconnected vehicular networks. However, as this technology advances, so do the challenges associated with ensuring privacy, security, and efficiency in IoV systems. This survey highlights the limitations of current privacy-preserving methods, such as scalability constraints, resource inefficiency, and adaptation issues in dynamic and high-speed IoV environments.

By systematically reviewing recent advances and identifying key research gaps, this paper emphasizes the need for innovative solutions that balance privacy with accountability, enhance real-time data processing, and integrate with evolving regulatory requirements. Addressing these gaps will require interdisciplinary research and the integration of emerging technologies, such as edge intelligence and quantum-resistant cryptography, to create resilient and scalable IoV systems. Ultimately, this survey aims to guide future developments in IoV, paving the way for robust, privacy-centric, and secure transportation networks.

ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for his unwavering guidance, invaluable insights, and encouragement throughout the research process. No funding is raised for this research.

REFERENCES

[1] Zhou, Haibo, et al. "Evolutionary V2X technologies toward the internet of vehicles: Challenges and opportunities." Proceedings of the IEEE 108.2 (2020): 308-323.
[2] Haddaji, Achref, Samiha Ayed, and Lamia Chaari Fourati. "IoV security and privacy survey: Issues, countermeasures, and challenges." The Journal of Supercomputing 80.15 (2024): 23018-23082.
[3] F. Pan et al., "Toward Software-Defined Vehicles: From Model-Based Engineering to Virtualization- Based Deployment," in IEEE Access, vol. 12, pp. 192127-192145, 2024, doi: 10.1109/ACCESS.2024.3512002.
[4] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, “A Comprehensive Survey on Authentication and Attack Detection Schemes That Threaten It in Vehicular Ad-Hoc Networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 12, pp. 13 573–13 602, 2023.
[5] R. Kumar, P. Kumar, A. Aljuhani, A. Jolfaei, A. N. Islam, and N. Mohammad, “Secure Data Dissemination Scheme for Digital Twin Empowered Vehicular Networks in Open RAN,” IEEE Transactions on Vehicular Technology, pp. 1–13, 2023.
[6] B. Lampe and W. Meng, “Intrusion Detection in the Automotive Domain: A Comprehensive Review,” IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2356–2426, 2023.
[7] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, “A Comprehensive Survey on Authentication and Attack Detection Schemes That Threaten It in Vehicular Ad-Hoc Networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 12, pp. 13 573–13 602, 2023.
[8] E. Batista, P. Lopez-Aguilar, and A. Solanas, “Smart health in the 6g era: Bringing security to future smart health services,” IEEE Communications Magazine, 2023.
[9] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, “Security and privacy for reconfigurable intelligent surface in 6g: A review of prospective applications and challenges,” IEEE Open Journal of the Communications Society, 2023.
[10] B. Mao, J. Liu, Y. Wu, and N. Kato, “Security and privacy on 6g network edge: A survey,” IEEE Communications Surveys & Tutorials, 2023
[11] M. M. Y. Al-Quraan, L. Mohjazi, L. Bariah, A. Centeno, A. Zoha, K. Arshad, K. Assaleh, S. Muhaidat,
[12] M. Debbah, and M. A. Imran, “Edge-native intelligence for 6g communications driven by federated learning: a survey of trends and challengesf,” IEEE Transactions on Emerging Topics in Computational Intelligence, 2023.
[13] Y. Liu, Y. Deng, A. Nallanathan, and J. Yuan, “Machine learning for 6g enhanced ultra-reliable and low-latency services,” IEEE Wireless Communications, vol. 30, no. 2, pp. 48–54, 2023.
[14] H. Gao, N. He, and T. Gao, “Sverifl: Successive verifiable federated learning with privacy-preserving,” Information Sciences, vol. 622, pp. 98–114, 2023.
[15] C. Lin, X. Huang, and D. He, “Ebcpa: Efficient blockchain-based conditional privacy-preserving authentication for vanets,” IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3,
pp. 1818–1832, 2023.

[16] Y. Yigit, I. Panitsas, L. Maglaras, L. Tassiulas, and B. Canberk, “CyberTwin: Digital Twin-Boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks,” in ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, June 2024, pp. 2167–2172.
[17] Y. Yigit, C. Chrysoulas, G. Yurdakul, L. Maglaras, and B. Canberk, “Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks,” in 2023 IEEE Globecom Workshops (GC Wkshps), Kuala Lumpur, Malaysia, December 2023, pp. 178–183.
[18] Z. Zeng, Q. Zhou, K. Wei, N. Yang and C. Tang, "BCS-CPP: A Blockchain and Collaborative Service- Based Conditional Privacy-Preserving Scheme for Internet of Vehicles," in IEEE Transactions on Intelligent Vehicles, vol. 9, no. 2, pp. 4130-4144, Feb. 2024, doi: 10.1109/TIV.2023.3327364.
[19] J. Liu et al., "CPAHP: Conditional Privacy-Preserving Authentication Scheme With Hierarchical Pseudonym for 5G-Enabled IoV," in IEEE Transactions on Vehicular Technology, vol. 72, no. 7, pp. 8929-8940, July 2023, doi: 10.1109/TVT.2023.3246466.
[20] P.-S. Xie, X.-J. Pan, H. Wang, J.-L. Wang, T. Feng, , and Y. Yan, “Conditional privacy-preserving authentication scheme for iov based on ecc,” International Journal of Network Security, vol. 24, no. 3,pp. 501–510, 2022.
[21] Y. Xia, H. Yuan, J. Qin, Q. Yuan, and J. Zhao, “An efficient anonymous identity authentication based on cp-abe and consortium blockchain for iov,” in 2023 4th International Conference on Electronic Communication and Artificial Intelligence (ICECAI), 2023, pp. 10–17.
[22] H. Sikarwar and D. Das, “A novel mac-based authentication scheme (nomas) for internet of vehicles (iov),” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 5, pp. 4904–4916, 2023.
[23] D. Mohammed Sharif, H. Beitollahi, and M. Fazeli, “Detection of application-layer ddos attacks produced by various freely accessible toolkits using machine learning,” IEEE Access, vol. 11, pp. 51 810–51 819, 2023.
[24] G. S. Rawat, K. Singh, N. I. Arshad, K. Hadidi, and A. Ahmadian, “A lightweight authentication scheme with privacy preservation for vehicular networks,” Computers and Electrical Engineering, vol. 100, p. 108016, 2022.
[25] C. Maurya and V. K. Chaurasiya, “Efficient anonymous batch authentication scheme with conditional privacy in the internet of vehicles (iov) applications,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 9, pp. 9670–9683, 2023.
[26] I. Ali and F. Li, “An efficient conditional privacy-preserving authentication scheme for vehicle-to- infrastructure communication in vanets,” Vehicular Communications, vol. 22, p. 100228, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221420961930275X
[27] M. A. Al Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang and J. Ma, "Two-Factor Privacy-Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks," in IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14253-14266, 15 April15, 2024, doi: 10.1109/JIOT.2023.3340259.
[28] S. Dass et al., "A Privacy-Preserving Architecture for Joint Communication and Sensing in 6G Networks," Proceedings of the 2024 IEEE Global Communications Conference (GLOBECOM), 2024. [Online]. Available: https://arxiv.org/abs/2405.01742.
[29] A. Korba, M. Amara, and B. Chikhaoui, "Zero-X: A Blockchain-Enabled Open-Set Federated Learning Framework for IoV Privacy," 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2024. [Online]. Available: https://arxiv.org/abs/2407.02969.
[30] Y. Ren et al., "QEPP: Quantum Efficient Privacy Protection Protocol for 6G-Quantum IoV Ecosystems," IEEE Transactions on Quantum Communications, vol. 10, no. 3, pp. 112–126, Mar. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10221729.
[31] M. Huang and Z. Chen, "A Trust-Based Privacy Management Framework for 6G IoV," IEEE Transactions on Vehicular Technology, vol. 73, no. 1, pp. 315–328, Jan. 2024.
[32] K. Sun et al., "Dynamic Data Anonymization Techniques for Privacy in 6G IoV," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 2, pp. 203–217, Feb. 2024.
[33] W. Jiang, J. Tao and Z. Guan, "A Trusted Data Privacy Computing Method for Vehicular Ad Hoc Networks Based on Homomorphic Encryption and DAG Blockchain," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3492031.

[34] S. Eghtessad, T. Hasanli, R. Huynh, K. Workneh, M. I. Ibrahem and M. M. Fouda, "A Survey on Privacy Preservation Methods in Future Vehicular Networks," 2023 11th International Conference on Information and Communication Technology (ICoICT), Melaka, Malaysia, 2023, pp. 319-325, doi: 10.1109/ICoICT58202.2023.10262771.

[35] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," Foundations and Trends in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014, doi: 10.1561/0400000042.

[36] Li, Y.; Bi, R.; Jiang, N.; Li, F.; Wang, M.; Jing, X. Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks. Electronics 2024, 13, 2372. https://doi.org/10.3390/electronics13122372

[37] Adhiarja, Asher and Farrell, Noor D. and Asher, Benjamin, Cyber Security and Privacy Preservation Protocols in VANET (July 1, 2023). Available at SSRN: https://ssrn.com/abstract=4507559 or http://dx.doi.org/10.2139/ssrn.4507559

[38] Ebrahimi, Masoud & Marksteiner, Stefan & Nickovic, Dejan & Bloem, Roderick & Schögler, David & Eisner, Philipp & Sprung, Samuel & Schober, Thomas & Chlup, Sebastian & Schmittner, Christoph & König, Sandra. (2023). A Systematic Approach to Automotive Security. 10.48550/arXiv.2303.02894.

[39] Meuser, T., Ojo, O.T., Bischoff, D., Fernández Anta, A., Stavrakakis, I., Steinmetz, R. (2021). Hide Me: Enabling Location Privacy in Heterogeneous Vehicular Networks. In: Georgiou, C., Majumdar, R. (eds) Networked Systems. NETYS 2020. Lecture Notes in Computer Science(), vol 12129. Springer,

[40] Amro, Belal. (2018). Protecting Privacy in VANETs Using Mix Zones with Virtual Pseudonym Change. International Journal of Network Security & Its Applications. 10. 10.5121/ijnsa.2018.10102.

[41] W. Jiang, J. Tao and Z. Guan, "A Trusted Data Privacy Computing Method for Vehicular Ad Hoc Networks Based on Homomorphic Encryption and DAG Blockchain," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3492031.

[42] Li, Y.; Bi, R.; Jiang, N.; Li, F.; Wang, M.; Jing, X. Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks. Electronics 2024, 13, 2372. https://doi.org/10.3390/electronics13122372.

[43] Aditya Kumar Singh, Jyoti Grover, and Sumita Mishra. 2023. Integration of Blockchain in VANET Using gRPC for Privacy Preservation of Vehicles. SN Comput. Sci. 5, 1 (Nov 2023). https://doi.org/10.1007/s42979-023-02438-0

[44] Huang Lu and Jie Li. 2016. Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey. Wirel. Commun. Mob. Comput. 16, 6 (April 2016), 643–655. https://doi.org/10.1002/wcm.2558

[45] J. Cui, Y. Cai, S. Yang and Y. Zhang, "A Survey on Privacy-preserving Schemes for Vehicular Ad Hoc Networks," 2021 IEEE 15th International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China, 2021, pp. 129-134, doi: 10.1109/ASID52932.2021.9651711.

[46] S. Eghtessad, T. Hasanli, R. Huynh, K. Workneh, M. I. Ibrahem and M. M. Fouda, "A Survey on Privacy Preservation Methods in Future Vehicular Networks," 2023 11th International Conference on Information and Communication Technology (ICoICT), Melaka, Malaysia, 2023, pp. 319-325, doi: 10.1109/ICoICT58202.2023.10262771.

[47] D. Zheng, C. Jing, R. Guo, S. Gao and L. Wang, "A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs," in IEEE Access, vol. 7, pp. 117716- 117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

[48] Malik, Nisha & Nanda, Priyadarsi & Arora, Arushi & He, Xiangjian & Puthal, Deepak. (2018). Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks. 674-679. 10.1109/TrustCom/BigDataSE.2018.00099.

[49] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," in IEEE Access, vol. 6, pp. 45655-45664, 2018, doi: 10.1109/ACCESS.2018.2864189.

[50] Z. Qi and W. Chen, "Location Privacy Protection of IoV based on Blockchain and K-anonymity Technology," 2023 6th International Conference on Electronics Technology (ICET), Chengdu, China, 2023, pp. 15-21, doi: 10.1109/ICET58434.2023.10211967.

[51] Z. Xia, L. Zeng, K. Gu, C. Su, H. Hu and K. Long, "Secure and Lightweight Vehicular Privacy Preservation Scheme Under Fog Computing-Based IoVs," in IEEE Transactions on Intelligent Vehicles, vol. 9, no. 2, pp. 4115-4129, Feb. 2024, doi: 10.1109/TIV.2023.3303312.
[52] Zheng, T., Wu, J. & Li, G. IoV data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing. J Cloud Comp 12, 99 (2023). https://doi.org/10.1186/s13677-023-00478-8