Privacy Protection Schemes in Internet of Vehicles (IoV): A Review and Analysis

Zheng Jiang[1], Fang-Fang Chua[2]*, Amy-Hui-Lan Lim[3]

[1,2,3]*Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia; E-mail: ffchua@mmu.edu.my*

Abstracts: Internet of Vehicles (IoV) refers to a dynamic network of vehicles where data exchange is a way of communication among them. Existing work focus on mitigating the data leakage and strengthening the privacy protection during data exchange among vehicles in IoV, specifically on the Safety Beacon Message (SBM) as it contains location and identity of the vehicles. Limited work reported on the design of privacy protection schemes explicitly for SBM, and the success case studies in implementation of privacy protection schemes in various types of IoV architectures. This paper aims to review past research on privacy protection schemes for SBM in IoV architectures and the challenges in pursuing similar research in current environment. Firstly, this paper discusses the privacy protection issues related to SBM that arise in the centralized IoV architectures. Next, decentralization and tamper- proof features of blockchain in IOV is introduced as the enhancement to the centralized IoV architectures. Then, privacy protection issues related to SBM in a blockchain-based IoV architecture will be discussed. Finally, this paper concludes with future direction of work in privacy protection schemes in blockchain- based IoV architecture.

Keywords: IoV, Internet of Vehicles, Privacy Protection Schemes, Safety Beacon Message, Blockchain.

1. INTRODUCTION

The growing acceptance and understanding of the Internet of Things (IoT) is driving the evolution of technology and the widespread adoption of IoT. This has led to a shift from traditional self-organizing vehicular networks to a more interconnected vehicle network. Intelligent Transportation Systems (ITS) has gained significant research focus and development in transportation (Qureshi et al., 2013). The Internet of Vehicles (IoV) is an interconnected network of vehicles that enables communication among vehicles and external systems, such as traffic control centers, to enhance transportation safety and efficiency. IoV applications include safety applications like collision evasion systems and emergency response systems, as well as non-safety applications like navigation and routing systems. Paid Information Collection (PIC) applications within IoV have emerged as a means to leverage data for service provision and optimization. However, privacy concerns hinder the sharing of personal and vehicle-related information. IoV encompasses various communication protocols and data exchange standards, such as Vehicle to Vehicle (V2V), Vehicle to Pedestrian (V2P), Vehicle to Infrastructure (V2I), and Vehicle to Network (V2N), collectively known as Vehicle to Everything (V2X) (Jeong et al., 2021). These networking modes are illustrated in Fig.1.

Fig. 1: Classification of V2X

In V2X engagement, a significant message type is the Safety Beacon Message (SBM). SBM serves as a communication protocol for ITS, aiming to enhance traffic safety and efficiency. It transmits specific traffic-related information to vehicles and devices, including roadway circumstances, vehicle operation status, traffic light signals, accident alerts, and street closure data. Through V2V or V2I communication, vehicles receive and interpret SBM to improve road conditions, traffic efficiency, and safety. SBM facilitates coordination and control among different vehicle types and traffic devices, supporting ITS progress and implementation. SBM utilizes distinct data formats and transmission protocols to ensure timely and accurate information exchange. It includes vehicle location, speed, acceleration, direction, braking status, road conditions, traffic flow, and safety-related details as shown in Fig.2. Identity and location data play a vital role in the IoV. Vehicle identity verification is crucial for V2V functionality and post-accident investigations. SBM provides location-based information, including the location of the vehicle (LV) and the location of SBM (LS). Precise location details enable high-quality V2V services and immediate recognition of traffic environment. SBM contributes to an integrated traffic management network, enhancing road safety and traffic efficiency. Its applications include traffic accident warnings and evasion, road traffic information services, and vehicle flow regulation (Li et al., 2018).

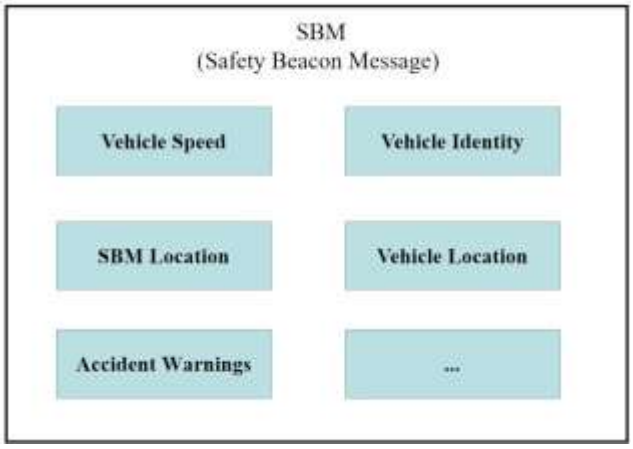

Fig. 2: Components of SBM

In recent years, IoV has experienced a shift towards a data-centered model due to the rapid evolution of intelligent terminals in vehicles. This evolution has created favorable conditions for IoV to collect user and vehicle data. However, relying solely on naturally uploaded data from users is insufficient to meet the data needs of IoV. To address this, the trend in IoV is moving towards PIC methods such as crowdsourcing and crowdsensing. Crowdsourcing involves conscious and active data collection by vehicles in response to crowdsourcing tasks published by the IoV backend (Lin et al., 2020). On the other hand, crowdsensing extends the concept by involving passive cooperation among vehicles without their awareness, forming a group concept among vehicles (Mei et al., 2020). Crowdsourcing applications do not require high vehicle density and involve targeted vehicles, while crowdsensing applications require high vehicle density, large amounts of data collection, and a certain degree of correlation. These PIC methods play a crucial role in collecting SBM in different IoV scenarios.

This paper aims to comprehensively review and analyze privacy protection schemes in the context of IoV. The paper focuses primarily on the privacy issues related to SBM in IoV architectures, as SBM are critical due to their transmission of sensitive information such as location and vehicle identity. First, the paper will survey the existing research related to privacy protection schemes specifically designed for SBM. The analysis will include an evaluation of the strategies employed to mitigate data leakage and strengthen privacy during data exchange among vehicles. The paper will place particular emphasis on the limitations of these current approaches and the challenges encountered in their implementation. Next, the paper will delve into the privacy protection issues related to SBM that arise in centralized IoV architectures. An in-depth understanding of the vulnerabilities and potential threats in centralized systems will be provided, setting the groundwork for the subsequent discussion. The paper then transitions into an exploration of the decentralized and tamper-proof features of blockchain in IoV, positioning it as an enhancement to the traditional centralized IoV architectures. The advantages and obstacles

presented by blockchain technology in this context will be comprehensively explored.

2. PRIVACY PROTECTION ISSUES IN CENTRALIZED IOV ARCHITECTURES

2.1. Overview of Centralized IoV Architectures

The origins of IoV can be traced back to the 1960s. After several decades of evolution, the IoV structure has progressed through various generations. Fig. 3 delineates a centralized IoV architecture, primarily composed of elements like vehicles, On-Board Unit (OBU), Road Side Unit (RSU), Certification Authority (CA), and Cloud server. Interaction processes exist among these entities (Kanumalli et al., 2020). The vehicle, a mobile entity in IoV, is typically furnished with smart IoT devices for the detection and collection of SBM. Wireless communication in the vehicle can be classified into V2V and V2I, basedon the vehicle's communication target. V2V signifies inter-vehicle communication, while V2I denotes communication between vehicles and infrastructure like RSUs. The WAVE protocol stack developed by IEEE chiefly supports these wireless communication forms. OBUs are WAVE devices installed in a vehicle to facilitate vehicular communication. They're equipped with a resource instruction processor, user interface (like PC5), and special short-range communication protocols centered on IEEE 802.11p and Cellular Vehicle-to-Everything (C-V2X). OBUs' primary roles involve wireless access, self-organizing networking, geographic routing, network conflict management, data security, and IP mobility management. RSUs are stationary wireless devices positioned on road sides or specific spots. They also use short-range communication protocols centered on IEEE 802.11p and C-V2X to collect and transmit SBM shared by OBUs, thus expanding the IoV's range. RSUs offer secure application services, such as traffic accident alerts, and Internet connections for OBUs. CAs serve as trusted third-party entities. They can produce security parameters for all IoV participants, including identity, public key, private key etc., to safeguard the entire IoV system's security. Lastly, the cloud server is primarily utilized for centralized SBM processing. SBMs are uploaded to the RSU via the vehicle's OBU. Following several switching, gateway, and forwarding operations, these SBMs are accumulated and centrally processed in the cloud server.

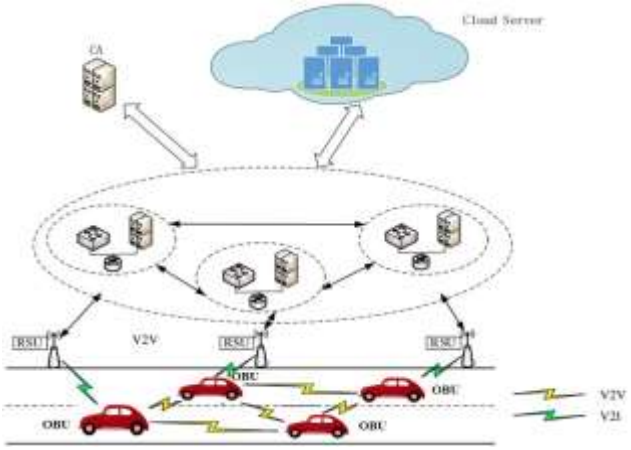

Fig. 3: Architecture of the Centralized IoV

2.2. Data Leakage and Privacy Concerns

The rapid surge in the quantity of IoV and the broadening of vehicle business applications' extent have enriched individuals with enhanced transportation services (Jiang et al., 2019). However, this paradigm shift introduces fresh dilemmas for the currently predominant centralized IoV structure. With the massive data environment, the data processed by IoV is experiencing an explosive growth (Jiang et al., 2018 & Hussain et al., 2018), raising formidable issues for the IoV's centralized model concerning system latency, bandwidth, cost, and notably security and privacy (Liao et al., 2017). In particular, privacy concerns arise from the prevalence of central bodies in the centralized IoV system. The inability of the centralized IoV architecture to fully ensure the trustworthiness of these central entities means that attacks on any central entity (such as a Certificate Authority, or a cloud server) and subsequent compromises could lead to serious data security risks, including data

tampering, inconsistency, and loss, thereby violating user privacy. Furthermore, with an immense data environment, the IoV's centralized architecture is susceptible to overload and bottleneck issues in the central entities, gravely hampering IoV system response time, potentially causing a single point of failure and paralysis, thereby escalating the risk of privacy breaches. In a centralized IoV setting, the central entities are presumed to be honest yet inquisitive, capable of functioning correctly but possibly interested in sensitive user information like identity and location data. This paper mainly considers central entities such as CA servers, Roadside Units, base stations, and other access points. By leveraging SBM, these central entities can effortlessly gain access to personal data, including user identity and location information. Moreover, with the motive of financial profit, central entities might leak some of this sensitive data to adversaries, who could then collate it with data gathered from other sources to mine a more holistic profile of a user, like their home address, family ties, occupation, and social status, leading to disruption in users' lives, economic detriment, and even threats topersonal safety.

2.3. Overview of Privacy Protection in Centralized IoV

Reflecting upon the properties of blockchain such as decentralization, redundant data storage, collective upkeep, and resistance to modification (Peters et al., 2018 & Joy et al., 2017), it has been suggested by scientists to integrate it into IoV as an alternative to intermediary parties to boost data privacy and security (Dorri et al., 2017 & Luo et al., 2019). For instance, Sharma et al. (2017) put forward a blockchain-oriented distributed IoV structure primarily encompassing control nodes, miner nodes, vehicle management servers, and authentication bodies. The blockchain network is collaboratively deployed by the miner and control nodes. Whenever a new vehicle wants to join the IoV, both the vehicle management server and authentication entity collectively assign identity-related resources and load them onto the blockchain network for validation, facilitating a distributed identity data storage and safeguarding user's vehicle identity details. In Lei et al., (2017) proposal, blockchain is utilized to establish secure key management to enhance the security of key-based communication among vehicles within a diverse IoV. In a mixed IoV, vehicles might exist in varying network areas, each having a CA server. By installing blockchain across all CA server nodes, the dependency on entirely trusted CA servers for key management is eliminated. As per the proposal by Amoretti et al. (2018), location privacy leakage within the IoV is tackled using a blend of blockchain and k-anonymity. To ensure location privacy, anonymous shelter zones must be set up for the vehicle's real location. Each anonymous zone creation is deemed a transaction and is logged onto the blockchain. Hence, by documenting the historical trust data of k vehicles on the blockchain, the trustworthiness of vehicles within the anonymous zones can be elevated. Building these zones based on trust significantly enhances the vehicles' privacy protection level. To this point, the fusion of centralized IoV and blockchain technology has emerged as a significant area of study within the IoV domain.

3. Decentralization and Blockchain in IoV

With the rapid surge in the number of interconnected vehicles and the broadening range of vehicular applications, people are enjoying enhanced transportation services (Jiang et al., 2019). Nevertheless, this growth poses unique challenges to the traditional centralized IoV structures. Faced with vast data environments, the volume of data associated with IoV is rising dramatically (Jiang et al., 2018 & Hussain et al., 2018), exerting substantial strain on the centralized network with respect to system latency, bandwidth utilization, cost effectiveness, security measures, and privacy preservation (Liao et al., 2017). A particular area of concern is privacy breaches; the centralized network model creates privacy vulnerabilities due to an abundance of central entities. The centralized model fails to assure the absolute trustworthiness of these entities, meaning that an attack on a central entity (like a CA or cloud server) could lead to serious data security issues, including data tampering, inconsistency, and loss, leading to breaches in user privacy. Furthermore, in a massive data environment, centralized IoV are susceptible to overload and bottleneck problems in central entities, seriously undermining the network's response time and potentially leading to single-point failure and system paralysis, further escalating the risk of privacy leaks. Given the benefits of blockchain technology, such as decentralization, redundant storage, collectiveupkeep, and tamper-proofing (Peters et al., 2018 & Joy et al., 2017), researchers are actively investigatingthe integration of blockchain technology into IoV to replace intermediaries and enhance data security and privacy. Hence, the adoption of blockchain technology constitutes a key focal point of this paper.

3.1. Overview of Blockchain Technology

The conventional blockchain network is made up of distrustful, decentralized nodes (Novo et al., 2018), as depicted in Fig. 4. Each node actively participates in data management, data backup, and maintains a complete copy of the blockchain. The point at which a fresh block gains approval from the majority of nodes within the system (a figure that varies according to the consensus mechanisms in place), are inscribed into the blockchain by the miner. As a result, each node replicates the information of the newly added block. As a result, all nodes within the blockchain network collaboratively upkeep the data, thus securing its consistency and totality.

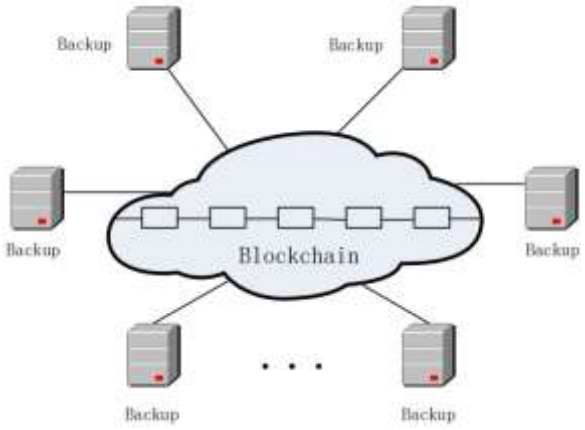

Fig. 4: Blockchain System

Blockchain possesses various unique advantages that make it a promising technology. One of its key benefits is its decentralized nature, operating on a peer-to-peer network model where each participating node is considered equal. The absence of central authority, thanks to its decentralized and distributed form, fosters trust among different components within the system. In the realm of blockchain technology, smart contracts (SCs) play a significant role. They are crucial components that facilitate the automation and execution of predefined actions based on predetermined conditions.

3.2. Overview of Privacy Protection Framework based on Blockchain-based IoV

The integration of blockchain technology into IoV can strengthen data integrity, improving data security and authenticity. Nonetheless, blockchain relies on several technology integrations, and it cannot directly assure security and privacy. Critical technologies such as contemporary cryptography, anonymity, and chain storage are instrumental in securing the block content and preserving the privacy of users. Considerable endeavours have been devoted to ensuring the privacy of blockchain-based IoV, in response to these challenges. A model is proposed by Lu et al. (2018) that employs an anonymous reputation system to halt the dissemination of counterfeit information and maintain vehicular privacy. The system constructs a privacy-focused trust management in IoV. A reputation assessment algorithm is employed to determine the trustworthiness of messages based on the reputation value assigned to a particular vehicle. To safeguard privacy and mitigate tracking attacks, the actual identities of vehicles engaging in V2I and V2V communications are substituted with pseudonyms.

Lei et al. (2017) have suggested a security framework supported by blockchain for ITS' heterogeneous network. The framework incorporates a novel key management scheme assisted by blockchain technology and a dynamic transaction collection scheme. This framework enhances the efficiency of distributed key management in heterogeneous networks, enabling faster processing and improved performance. The security managers (SMs) have an essential function of verifying and authenticating the key transmission process, after the central manager is removed. Kaur et al. (2019) have evaluated the flaws of current authentication mechanisms for cloud-based IoV. To address these flaws, the authors have presented a decentralized authentication and key exchange mechanism for vehicular fog computing scenarios, which employs blockchain and Elliptic Curve Cryptography

(ECC). Blockchain is used to maintain network information, while ECC ensures mutual authentication between vehicles and fog nodes, user anonymity, and reauthentication of participating vehicles. Noh et al. (2020) showcase a blockchain-supported connected vehicle message authentication scheme. The scheme offers anonymous and decentralized broadcast messages exchanged by connected vehicles, letting vehicles verify messages efficiently and in a distributed manner. Public key-based encryption and message authentication code technology are used for authentication. Xu et al. (2018) develop a secure model called Remote

Authentication Security Model(RASM) for remote authentication utilizing privacy-preserving blockchain for intelligent vehicles in V2X networks. Lastly, in order to offer efficient keyword search capability to users, Chen et al. (2019), introduce a unique, decentralized searchable encryption scheme that is intended for blockchain and cloud-based IoV applications. This encryption method, known as Blockchain-based Searchable Public-key Encryption scheme with Forward and Backward privacy(BSPEFB), allows data that is stored on devices such as cloud servers to be searched while ensuring user data security. To safeguard user privacy, the scheme incorporates forward and backward privacy measures. Forward privacy protects the security of future data after a key update, ensuring previously encrypted data remains secure and unaffected by the updated key. Backward privacy, on the other hand, defends the privacy of past data after a key update by preventing potential links between the updated key and historical data. The blockchain's decentralized nature that is implemented through SCs, helps to address single-point attacks and verify the correctness of returned results. This system model and workflow of BSPEFB are demonstrated in Fig. 5 of the paper. This scheme is vital in maintaining user data privacy, particularly in environments where encryption keys require regular updates to bolster security. The system is composed of four entities namely Cloud Server (CS), Blockchain Platform (BP), Data Owner (DO), and Data User (DU). The CS stores data and responds to user requests, while the BP maintains a blockchain network supporting SCs for search and data storage services. The DO shares data through the CS, and the DU paysfor these services. As illustrated in Fig. 5, the BSPEFB process involves five steps which are encrypting indexes, encrypting the database, searching keywords, accessing the data and matching the data with the keywords. This approach provides critical safeguards for user data privacy, particularly in contexts requiring regular updates of encryption keys to ensure security.

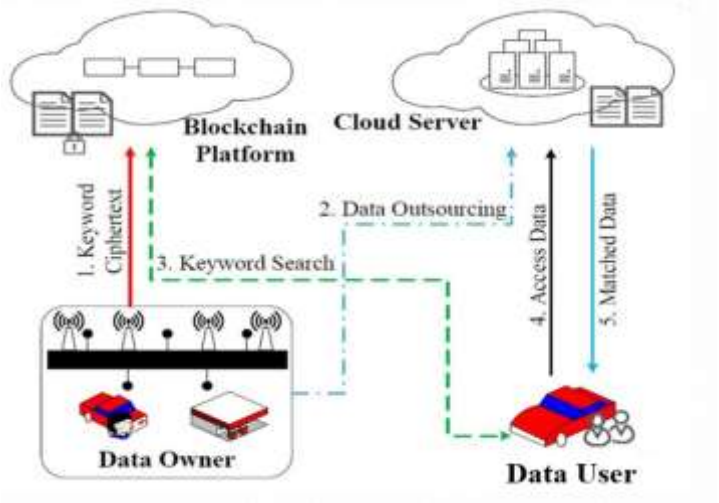

Fig. 5: System Model and Workflow of BSPEFB

3.3. Challenges of Privacy Protection in Blockchain-based IoV

Incorporating blockchain into IoV systems necessitates dealing with substantial data and transactions in an ever-changing vehicular setting. The current challenge lies in the application of blockchain technology to IoV, given its heavy reliance on huge data sets and mobility. Hence, the performance metrics of blockchain-based IoV are as vital as their security and privacy. These metrics include latency, power usage, throughput, and scalability. Various research aims at enhancing these metrics, particularly in relation to blockchain-supported IoV. For instance, a study by Sharma (2018) tackles the issue of excessive power consumption due to abundant transaction-related

communications between updating vehicles and blockchain networks. This paper presents a distributed clustering approach that ideally regulates the volume of transactions, leading to significant energy savings. The performance of this method is thoroughly analyzed and compared to conventional methods, resulting in a 40.16% decrease in power usage and an 82.06% reduction in transaction volumes. Liu et al. (2019) propose a performance optimization framework for blockchain-assisted IoV, utilizing deep reinforcement learning (DRL) technology to manage scalability problems and process the voluminous data produced by vehicles. This framework aims at maximizing transaction throughput and considering three essential blockchain characteristics which are decentralization, security, and latency. The study firstly offers a method for assessing blockchain performance quantitatively. It then employs DRL technology to enhance performance by choosing block creators and adjusting block size and interval time based on the dynamic distribution of vehicles.

Beyond performance difficulties, existing studies on blockchain-powered IoV predominantly focus on a single-chain model. This presents hurdles in securing and efficiently storing vast amounts of SBM, which can lead to breaches of privacy. Wang et al. (2021) offer a comprehensive view of blockchain's potential applications in IoV, such as identifying vehicles, sharing data, fostering collaboration, and managing traffic. Nonetheless, this comes with an array of challenges, including performance constraints like latency and throughput, which can hinder real-time capabilities and the scalability of IoV applications. Despite blockchain's innate security, risks such as 51% attacks and SC vulnerabilities can possibly undermine the safety and dependability of IoV systems. Furthermore, it is crucial to safeguard personal privacy information in IoV, such as the identity and location of vehicle owners, necessitating the application of suitable privacy protection measures. These hurdles highlight the need to tackle performance, security, and privacy issues in blockchain-driven IoV systems to maintain their efficacy and reliability. Alternatively, Jia et al. (2021) have suggested a dynamic key management algorithm for a smart building energy management system that leverages wireless sensor networks and blockchain. The algorithm employs blockchain to deliver distributed key management services, boosting the system's security and trustworthiness. However, the setup cost and complexity of the algorithm are heightened due to the creation of a blockchain network and the assignment of public-private key pairs to each node, complicates its widespread adoption. In another research, Lahiri et al. (2020) introduce a trustworthy framework for IoV, utilizing blockchain and edge computing. This framework is designed to increase the security, trust, and user privacy of the IoV system, facilitating automated transactions and data sharing, minimizing manual interference and enhancing system efficiency and scalability. Even though this trustworthy framework partially solves security and user privacy issues, significant performance problems emerge when handling a huge number of SBM. To conclude, Table 1 provides a summarization and discussion of these research topics and current issues.

Table 1 Summary of the existing work of the blockchain-based IoV architecture

Source	Description	Methods	Limitations
(Wang et al., 2021)	To propose a blockchain-based distributed IoV architecture	Multiple Mechanisms Compared	The application of blockchain inIoV is the traditional single- chain model, which lacks the security and efficiency to deal with massive data. Lack of a blockchain-based integrated framework to managethe privacy protection of SBM in IoV applications.
(Jia et al., 2021)	To use Blockchainfor Secure Key Management	Framework of a blockchain-based dynamic key management scheme	
(Lahiri et al., 2020)	Combined with blockchain and k- anonymity, it solves the location privacy leakage problem of IoV	Combine blockchain and edge computing	

4. PRIVACY PROTECTION ISSUES FOR SBM

4.1. Challenges in Protecting SBM Privacy

As the technology of IoV becomes more mature, attention is increasingly turning towards privacy protection, especially concerning the privacy of SBM, a persisting challenge. SBM are messages vehicles broadcast to nearby entities to facilitate the exchange of safety-related information, a critical function of IoV. These messages contain sensitive information, such as speed, location, and direction. The main challenges of SBM privacy protection fall into three main categorie namely anonymity, data security, and infrastructure limitations. Anonymity in the context of IoV's is essential because SBM revolves around the fact that each vehicle regularly broadcasts messages containing potentially sensitive information, such as current location, speed, and direction. While this function is fundamental to IoV, enabling vehicle awareness to avoid collisions or other dangers, the regular broadcast could permit adversaries to track specific vehicles, violating the privacy of the vehicle owner. To mitigate this, pseudonym change strategies are often employed, where vehicles regularly alter the identifiers used when sending SBM. The timing and coordination of these changes are crucial as they can provide information to track vehicles. Data security is a significant concern as SBM carry crucial safety-related data that needs protection from unauthorized access. A malicious entity gaining access to these messages could misuse this information for nefarious purposes, such as planning thefts or robberies. Additionally, malicious entities might inject false information into the system, causing confusion and potentially accidents. Ensuring the integrity and confidentiality of SBM is challenging. Techniques like encryption and digital signatures can be used to secure access to SBM and verify message authenticity, but managing the keys used for these purposes presents its own challenges. Infrastructure limitations are also a major concern. Real-time or near-real- time processing and communication of SBM is required for effective IoV operations. This requirement means that delays introduced by security measures such as encryption or digital signatures must be minimized. Traditional heavy encryption methods may not be feasible due to excessive delays. Lightweight encryption methods can be used to reduce this delay, but they typically offer less security than heavier encryption methods. Additionally, the infrastructure must handle a large number of SBM, necessitating significant bandwidth and processing power, whether in the vehicles themselves or the supporting infrastructure. Balancing efficiency and security are major challenges in this area. Mitigating these challenges requires a blend of technological and policy interventions. Techniques like pseudonym change strategies, data encryption, and secure multi-party computation can help ensure SBM privacy. Simultaneously, strict policies and regulations can act as deterrents to potential privacy breaches.

4.2. Existing Privacy Protection Schemes for SBM in Blockchain-based IoV

Table 2 provides a summary of the privacy concerns in PIC applications' SBM collection due to incorporating data such as user location, identity, and other information. Numerous studies on privacy protection in IoV have been conducted (Vergara-Laurens et al., 2016 & Abu Alsheikh et al., 2017), resulting in an array of proposed privacy safeguard mechanisms, including those based on anonymity, obfuscation, fuzziness, and cryptography. However, these mechanisms fail to account for the interrelation between time, space, and data. Personal and local sensing data need to be disclosed to others in a single PIC application to create valuable insights and services, consequently leading to privacy concerns. Gao et al. (2022) have introduced a unique trajectory obfuscation algorithm, proficient at concealing user location information whilst ensuring data quality and task completion rates. The algorithm dissects the user's trajectory into several segments, creating fake trajectory segments within each that are combined with the real ones to deter attackers from pinpointing the user's actual location. However, trajectory obfuscation can potentially disrupt the data's accuracy and completeness due to the potential interference or noise from the fake trajectory segments. Zhang et al. (2021) suggest employing geometric range query technology to convert the task recommendation procedure into a process of locating suitable participants within a geometric range to secure user location privacy. The algorithm initially transmutes user location information into discrete grid points, then transforms the task range into grid point ranges. Following this, it leverages geometric range query technology to search for appropriate participants within the grid point range, circumventing the direct revelation of user location information. Privacy protection strategies like introducing noise to query results and controlling query frequency are also utilized. However, the process of transmuting user location and task range into grid points can generate some discretization errors, resulting in less accurate recommendations. Also, geometric range queries demand significant computational resources and time, which might negatively impact application performance and response time. Qian et al. (2021) propose an optimal task allocation algorithm that strikes a balance between location privacy protection and service quality assurance in

vehicle-based crowdsensing networks. The algorithm views participants and tasks in the sensing network as a bipartite graph, with participants' location privacy and service quality as optimization objectives and constraints respectively. The algorithm employs linear programming techniques to optimize the objective function and constraints, therebyachieving the optimal task allocation algorithm that fulfills location privacy and service quality requirements. Nonetheless, the algorithm only emphasizes location privacy protection and overlooks other privacy protection types such as identity and behavioral privacy.

Table 2 Summary of the privacy concerns in PIC applications' SBM collection

Source	Description	Methods	Limitations
(Gao et al., 2022)	To propose a differential location privacy-preservingalgorithm based on trajectory obfuscation	Differential privacy	Over-reliance on third-party security entities, such as CA Data loss caused by suppressing or obfuscating location data uploads
(Zhang etal., 2021)	To propose the location privacy-preserving task recommendation (PPTR) schemes with geometric range query in mobile crowdsensing without the trusted database owner	Geometric rangequery	
(Qian et al., 2021)	To use the differential privacy algorithm to preserve location privacy ofthe vehicle and submit it to IoV applications	Differential privacy	

The act of uploading SBM usually incorporates information like vehicle identification, velocity, location, and the content of the request. However, in this data-intensive era, the significance of identity and location information is paramount, and privacy concerns are mounting among users who don't want their personal information compromised. As a result, safeguarding the privacy of vehicle identity and location during SBM upload has become critical. A summary of some research on privacy protection during SBM upload can be found in Table 3. Su et al. (2019) develop an innovative privacy-securing authentication algorithm for Vehicle-to-Grid (V2G) networks, utilizing a blend of encryption technology and zero-knowledge proof to shield user privacy and verify user identity.

Despite the high security and low computational expense of the algorithm, it requires users and vehicles to implement specific hardware and software, possibly raising the cost and difficulty of implementation, hence affecting its practicality. Wang et al. (2020) have proposed a Vehicular Ad Hoc Network (VANET) identity verification algorithm based on combined conditional privacy. The algorithm merges identity-based encryption and anonymous authentication methods and employs conditional privacy to guard user location privacy. However, for this algorithm to be implemented successfully, all vehicles must pre-obtain CA signatures, which may prove challenging and costly in large-scale VANET deployments. A privacy-securing cooperative localization algorithm is proposed by Chandra Shit et al. (2022), targeting the enhancement of vehicle positioning accuracy and privacy protection using vehicle edge computing infrastructure. The algorithm employs vehicle cooperation for improved localization accuracy and utilizes anonymous certificates and obfuscation techniques for location privacy. Despite the algorithm's efficacy in providing highly precise vehicle localization and preserving location privacy, it requires vehicle cooperation, which can be influenced by the vehicle count and their cooperative intent

Table 3 Research on privacy protection before SBM upload

Source	Description	Methods	Limitations
(Su et al. 2019)	To propose a lightweight privacy-preserving authentication scheme thatdoes not use bilinear pairings	A novel privacy-preserving authentication scheme for IoV networks	Most algorithm can onlyprotect a single private information of the vehicle's identity or location Most privacy protection schemes

(Wang et al. 2020)	To propose a mixed- condition privacy- preserving authenticationprotocol based on PKI certificate and identity signature	Based on the PKI certificate systemand the anonymous identity signature mechanism	rely too much ontrusted third-party entities Most of the algorithms can't solve the problem before SBM data upload toblockchain
(Chandra Shitet al., 2022)	To proposed a location- based dynamic pseudonymtransformation privacy protection mechanism to protect user identity privacy	Privacy protection method based on pseudonym	

5. FUTURE DIRECTIONS AND RESEARCH CHALLENGES

In the evolving landscape of blockchain-based IoV, future research needs to focus on strengthening privacy protection schemes, especially for SBM. Firstly, there is a need for more explicit design and development of privacy schemes dedicated to SBM, considering the sensitivity of the content and their role in IoV architectures. Secondly, different privacy protection algorithms have their own limitations due to their specific focus. However, combining multiple privacy protection algorithms to comprehensively address privacy issues is a highly worthwhile direction to explore. For instance, combining differential privacy and homomorphic encryption is an excellent example. Differential privacy protects individual privacy by adding noise to the data. By combining it with homomorphic encryption, computations can be performed on encrypted data, enabling secure processing of sensitive information while preserving privacy. This combination ensures privacy maintenance during data aggregation and analysis processes inthe IoV environment. Thirdly, exploring the potential enhancements offered by decentralization and tamper-proof features of blockchain can be introduced to existing IoV architectures. Lastly, in addition to addressing privacy protection issues through technological means, the development of robust policies and regulations is urgently needed to guide privacy protection in an increasingly decentralized IoV environment. These research directions are crucial in ensuring the secure and effective operation of the IoV while protecting user privacy.

CONCLUSION

IoV is a rapidly evolving domain where data interchange, specifically SBM, plays a crucial role in facilitating vehicle communication. However, this study highlights the complex challenge of ensuring privacy in these data transactions. While existing research has primarily focused on reducing data exposure and strengthening privacy protection, there has been limited attention given to customizing privacy protection mechanisms specifically for SBM and their practical implementation across various IoV frameworks. By conducting a comprehensive review of prior studies, this paper identifies key privacyprotection issues associated with SBM in centralized IoV systems. In this context, integrating blockchain technology with centralized IoV shows significant potential due to its decentralized nature and immutable characteristics. Nevertheless, it is essential to acknowledge that blockchain-based IoV also presents unique privacy challenges. Thus, addressing these challenges becomes imperative for advancing privacy protection methods in IoV, particularly within a blockchain-oriented IoV architecture. In addition to technological advancements and innovations, the development of comprehensive policies and regulations is crucial. By doing so, it can collectively pave the way for a trusted and privacy preserving IoV that benefits all stakeholders involved.

REFERENCES

[1] Abu Alsheikh, M., Jiao, Y., Niyato, D., Wang, P., Leong, D., & Han, Z. (2017). The Accuracy- Privacy Tradeoff of Mobile Crowdsensing. arXiv e-prints, arXiv-1702.

[2] Amoretti, M., Brambilla, G., Medioli, F., & Zanichelli, F. (2018, July). Blockchain-based proof of location. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 146-153). IEEE.

[3] Chandra Shit, R., Sharma, S., Watters, P., Yelamarthi, K., Pradhan, B., Davison, R., ... & Puthal, D. (2022). Privacy-preserving cooperative localization in vehicular edge computing infrastructure. Concurrency and Computation: Practice and Experience, 34(14), e5827.

[4] Chen, B., Wu, L., Wang, H., Zhou, L., & He, D. (2019). A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6), 5813-5825.

[5] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In Proceedings of the second international conference on Internet-of-Things design and implementation (pp. 173-178).

[6] Gao, Z., Huang, Y., Zheng, L., Lu, H., Wu, B., & Zhang, J. (2022). Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing. IEEE Transactions on Industrial Informatics, 18(9), 6290-6299.

[7] Hussain, R., Kim, D., Son, J., Lee, J., Kerrache, C. A., Benslimane, A., & Oh, H. (2018). Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds. IEEE Internet of Things Journal, 5(4), 2441-2448.

[8] Jeong, H. H., Shen, Y. C., Jeong, J. P., & Oh, T. T. (2021). A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications. Vehicular Communications, 31, 100349.

[9] Jam, F. A., Singh, S. K. G., Ng, B., & Aziz, N. (2016). Effects of Uncertainty Avoidance on Leadership Styles in Malaysian Culture, , International Journal of Advance Business and Economics Research, 14(8), 7029-7045.

[10] Jia, C., Ding, H., Zhang, C., & Zhang, X. (2021). Design of a dynamic key management plan for intelligent building energy management system based on wireless sensor network and blockchain technology. Alexandria Engineering Journal, 60(1), 337-346.

[11] Jiang, D., Wang, Y., Lv, Z., Qi, S., & Singh, S. (2019). Big data analysis based network behavior insight of cellular networks for industry 4.0 applications. IEEE Transactions on Industrial Informatics, 16(2), 1310-1320.

[12] Jiang, D., Huo, L., & Song, H. (2018). Rethinking behaviors and activities of base stations in mobile cellular networks based on big data analysis. IEEE Transactions on Network Science and Engineering, 7(1), 80-90.

[13] Joy, J., Cusack, G., & Gerla, M. (2017, October). Poster: time analysis of the feasibility of vehicular blocktrees. In Proceedings of the 3rd Workshop on Experiences with the Design and Implementation of Smart Objects (pp. 25-26).

[14] Kanumalli, S. S., Ch, A., & Sri, P. (2020). Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. International Journal of Advanced Computer Science and Applications, 11(1).

[15] Kaur, K., Garg, S., Kaddoum, G., Gagnon, F., & Ahmed, S. H. (2019, May). Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In 2019 IEEE International conference on communications workshops (ICC workshops) (pp. 1-6). IEEE.

[16] Lahiri, P. K., Das, D., Mansoor, W., Banerjee, S., & Chatterjee, P. (2020, December). A trustworthy blockchain based framework for impregnable IoV in edge computing. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 26-31). IEEE.

[17] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[18] Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., & Ye, H. (2018). Significant permission identification for machine-learning-based android malware detection. IEEE Transactions on Industrial Informatics, 14(7), 3216-3225.

[19] Li, H., Pei, L., Liao, D., Zhang, M., Xu, D., & Wang, X. (2020). Achieving privacy protection for crowdsourcing application in edge-assistant vehicular networking. Telecommunication Systems, 75, 1-14.

[20] Chang, L.-C. . (2023). The Experimentation Act and its Practice of Autonomous Vehicles in Taiwan. International Journal of Membrane Science and Technology, 10(3), 1404-1408. https://doi.org/10.15379/ijmst.v10i3.1720

[21] Liao, D., Sun, G., Zhang, M., Chang, V., & Li, H. (2017, July). Towards location and trajectory privacy preservation in 5G vehicular social network. In 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (Vol. 2, pp. 63-69). IEEE.

[22] Lin, H., Garg, S., Hu, J., Kaddoum, G., Peng, M., & Hossain, M. S. (2020). Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(6), 3755-3764.

[23] Liu, M., Teng, Y., Yu, F. R., Leung, V. C., & Song, M. (2019, May). Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[24] Lu, Z., Liu, W., Wang, Q., Qu, G., & Liu, Z. (2018). A privacy-preserving trust model based on blockchain for VANETs. Ieee Access, 6, 45655-45664.

[25] Luo, B., Li, X., Weng, J., Guo, J., & Ma, J. (2019). Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Transactions on Vehicular Technology, 69(2), 2034-2048.

[26] Mei, Q., Gül, M., & Shirzad-Ghaleroudkhani, N. (2020). Towards smart cities: crowdsensing-based monitoring of transportation infrastructure using in-traffic vehicles. Journal of Civil Structural Health Monitoring, 10(4), 653-665.

[27] Noh, J., Jeon, S., & Cho, S. (2020). Distributed blockchain-based message authentication scheme for connected vehicles. Electronics, 9(1), 74.

[28] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE internet of things journal, 5(2), 1184-1195.

[29] Peters, D., Wetzlich, J., Thiel, F., & Seifert, J. P. (2018, May). Blockchain applications for legal metrology. In 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) (pp. 1-6). IEEE.

[30] Qian, Y., Ma, Y., Chen, J., Wu, D., Tian, D., & Hwang, K. (2021). Optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4367-4375.

[31] Qureshi, K., & Abdullah, H. (2013). A Survey on Intelligent Transportation Systems. Middle-East Journal of Scientific Research, 15, 629–642.

[32] Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. Journal of information processing systems, 13(1), 184- 195.

[33] Sharma, V. (2018). An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). IEEE Communications Letters, 23(2), 246-249.

[34] Su, Y., Shen, G., & Zhang, M. (2019). A novel privacy-preserving authentication scheme for V2G networks. IEEE Systems Journal, 14(2), 1963-1971.

[35] Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2016). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. IEEE Internet of Things Journal, 4(4), 855-869.

[36] Wang, C., Cheng, X., Li, J., He, Y., & Xiao, K. (2021). A survey: applications of blockchain in the internet of vehicles. EURASIP Journal on wireless communications and networking, 2021, 1-16.

[37] Wang, S., Mao, K., Zhan, F., & Liu, D. (2020). Hybrid conditional privacy-preserving authentication scheme for VANETs. Peer-to-Peer Networking and Applications, 13, 1600-1615.

[38] Xu, C., Liu, H., Li, P., & Wang, P. (2018). A remote attestation security model based on privacy- preserving blockchain for V2X. Ieee Access, 6, 67809-67818.

[39] Zhang, C., Zhu, L., Xu, C., Ni, J., Huang, C., & Shen, X. (2021). Location privacy-preserving task recommendation with geometric range query in mobile crowdsensing. IEEE Transactions on Mobile Computing, 21(12), 4410-4425.

DOI: https://doi.org/10.15379/ijmst.v10i1.1818