


Article

# Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks

Yijing Li <sup>1</sup> , Ran Bi <sup>1,\*</sup>, Nan Jiang <sup>1</sup>, Fengqiu Li <sup>1</sup>, Mingsi Wang <sup>2</sup> and Xiangping Jing <sup>3</sup>

<sup>1</sup> China Academy of Information and Communications Technology (CAICT), Beijing 100191, China; liyijing@caict.ac.cn (Y.L.); jiangnan@caict.ac.cn (N.J.); lifengqiu@caict.ac.cn (F.L.)

<sup>2</sup> Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China; wangmingsi@iie.ac.cn

<sup>3</sup> China Information Technology Security Evaluation Center, Beijing 100085, China; xiangping\_jing@163.com

\* Correspondence: biran@caict.ac.cn

**Abstract:** With the rapid development of wireless communication technology, positioning technology, and modern smart devices, Internet of Vehicles (IoVs) smart vehicles have brought great convenience to human production and life. Meanwhile, privacy and security issues are becoming extremely serious, with serious consequences if sensitive data such as vehicle location and trip patterns are leaked. This paper focuses on the demands for vehicular network security, especially privacy protection and existing privacy-protection techniques, including common cryptography methods and cryptography-based advanced technologies. At the same time, this paper also analyzes the advantages and challenges of these technologies in protecting privacy and network security in the Internet of Vehicles, such as the challenges of computational resource requirements and security efficiency in the implementation process, as well as the complexity of realizing effective privacy protection in the interactions among different entities. Finally, this paper envisions the development of privacy-preserving application scenarios and the prospects for cryptography-based privacy-preserving technologies.

**Keywords:** vehicular network security; data protection; cryptography; IoVs; privacy preservation



**Citation:** 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>

Academic Editors: Hung-Yu Chien and Zbigniew Kotulski

Received: 8 May 2024

Revised: 30 May 2024

Accepted: 14 June 2024

Published: 17 June 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Definition

Rapid advancements in wireless communication, localization technologies, and smart devices have significantly increased research interest in vehicular networks (VNs), with a focus on crucial security and privacy issues. Privacy in VNs involves protecting personal and vehicle information from unauthorized access and misuse, which, if compromised, could lead to severe security problems [1].

A wide array of sensors, both internal and external to the vehicle, collect critical data that are essential for road safety and operational efficiency. If mishandled, these data can compromise individual privacy and safety, potentially disrupting social order. They include details such as vehicle tracking, driver identities, vehicle charging, operational status, and specifics like taxi order status and popular destinations. When shared with Location Service Providers (LSPs), these data could reveal sensitive information like exact locations, travel directions, and personal preferences, risking user anonymity [2–6].

The shift from fuel to electric vehicles has elevated the importance of charging data, exposing personal routines and mobility patterns that are relevant to urban planning and traffic management [7,8]. Additionally, vulnerabilities in these data could be exploited to manipulate traffic information, impacting the broader transportation system [9]. Protecting these data is crucial to guard against risks such as identity theft and the misuse of data for targeted advertising, which could undermine personal autonomy [10,11].

Research in this domain has expanded from a focus on network-related issues to include broader security and privacy concerns, integrating advanced cryptographic solutions

to protect vehicular networks. Numerous studies have explored the intricacies of these networks, proposing security protocols and assessing the effectiveness of privacy strategies across Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) platforms [10,12,13].

The following part begins by evaluating the different entities that need to be protected, ranging from user privacy to vehicle data and extending to manufacturers and service providers. In the discussion, standard cryptographic practices and advanced technology such as blockchain, federated learning, and differential privacy are reviewed. Each of these technologies is analyzed to understand their potential to protect privacy against a variety of threats, which are meticulously categorized into internal, external, and third-party risks. The challenges section explores the practical difficulties in implementing these techniques, recognizing the barriers to widespread adoption and the technical obstacles that may arise.

This paper aims to synthesize the insights gained from these discussions to provide a comprehensive understanding of how current practices can be developed and optimized. By mapping the interactions between these encryption methods and the types of data that they protect, we pave the way for a discussion that not only highlights the current state of privacy protection, but also points the way to the future.

## 2. Current Privacy-Protection Methods

Figure 1 shows the entities that need to be protected in the context of IoVs privacy protection and the corresponding methods employed as presented in this paper.

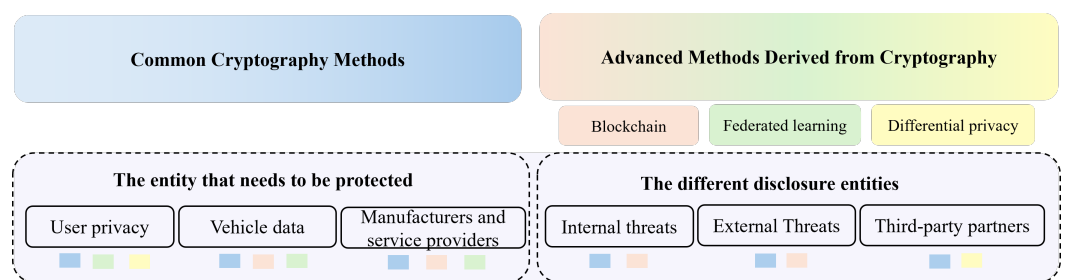


Figure 1. Structure of privacy-protection methods.

### 2.1. The Entity That Needs to Be Protected

In the context of vehicular networks, it is imperative to safeguard the interests and privacy of various entities, including users and vehicles, as well as manufacturers and service providers. Vehicular network systems must diligently uphold the privacy rights of vehicle owners and passengers. This encompasses the protection of sensitive data, including personally identifiable information, driving behavior records, and location details. Moreover, the technical data and performance metrics of the vehicle demand rigorous safeguards to prevent unauthorized access and misuse. These datasets may encompass vital information such as vehicle speed, route history, and fuel consumption, among others. In addition to these, manufacturers and service providers engaged in the realm of vehicular networks must take diligent measures to preserve their proprietary knowledge, trade secrets, and competitive advantages. Central to the concept of privacy protection in the vehicular network ecosystem is the unwavering commitment to shield the privacy and sensitive information of these stakeholders, thereby upholding their rights and ensuring the utmost data security.

#### 2.1.1. User Privacy Protection

In vehicular network systems, it is imperative to adhere to stringent data privacy practices. These entail obtaining explicit consent from users before embarking on the collection and processing of their personal data. Users must possess unequivocal clarity regarding the specific objectives for which their data will be collected and utilized. Vehicular network systems bear the responsibility of furnishing comprehensive and transparent information concerning their data-processing activities. This includes elucidating the

precise purposes for which the data will be employed, detailing the methodologies by which they will be processed, and specifying the duration of their storage. It is of paramount importance that users are granted effortless access to this information and that its content is readily comprehensible to facilitate informed decision-making regarding their personal data [14].

Whenever feasible, the processing and analysis of personal information collected by a vehicular network transpires within the confines of the vehicle itself, thereby affording users paramount control over their personal data. This approach serves to significantly curtail the transmission of data, consequently mitigating the risk of data leakage. For situations necessitating the transfer of data beyond the vehicle's confines, robust data-anonymization techniques are meticulously employed to systematically expunge or substitute personally identifiable information. This strategic deployment effectively precludes the identification of users [15]. Through meticulous de-identification, desensitization, and data-obfuscation methodologies, the processed data lose the capacity to directly or indirectly link to individual identities or their respective activities, thus fortifying the protection of individual privacy.

The spectrum of data-anonymization techniques encompasses various methods that are contingent upon the nature of the data and the requisite privacy thresholds. These methods span generalization, suppression, perturbation, noise addition, microclustering, and other pertinent techniques. The selection of the appropriate anonymization methods and parameterization is contingent upon the specific data types and the intricacies of the privacy requisites. Concurrently, rigorous authentication protocols are implemented to thwart unauthorized access, assiduously safeguarding user data from illicit interception or compromise.

#### 2.1.2. Vehicle Data Protection

Encryption plays a pivotal role in safeguarding data transmitted through vehicular network systems, encompassing communications across various domains, including Vehicle-to-Infrastructure communication, intra-vehicle systems, and interactions with cloud services. The application of encryption techniques serves as an effective deterrent against unauthorized access and the illicit extraction of sensitive information. The implementation of end-to-end encryption for vehicle data serves as a robust security measure to ensure the confidentiality and integrity of data during both the transmission and storage phases. Data-encryption technology is broadly classified into categories such as symmetric encryption, asymmetric encryption, and hybrid encryption, among others. The selection of the most fitting encryption algorithms and key management schemes hinges upon the specific application scenarios and security requisites in question.

Furthermore, the establishment of a stringent access control framework assumes paramount importance in guaranteeing that only authorized users or systems are granted access to vehicle data. This access control mechanism meticulously governs data access rights, encompassing aspects such as the authorized entities, modes of access, and permissible scope of access. This comprehensive approach effectively mitigates the risk of unauthorized data access or misuse. Data access control techniques span various models based on attributes, roles, policies, and environmental factors, to name a few. The judicious selection of the appropriate access control policies is contingent upon the particular data security levels and the intricacies of business requirements.

It is also essential to note that the General Data Protection Regulation (GDPR) [14] articulates the principle of data minimization, mandating vehicular network systems to exclusively collect and retain data that are pertinent to vehicle operation and safety, while prudently minimizing the collection of superfluous data. This imperative aligns with GDPR's commitment to enhancing data privacy and minimizing data exposure.

#### 2.1.3. Manufacturer and Service Provider Protection

Within the realm of vehicular networks, manufacturers and service providers are entrusted with the processing and storage of substantial volumes of data. This dataset

encompasses vehicle information, user profiles, road conditions, and more. Notably, this data repository often harbors sensitive information, spanning from personally identifiable user data to intricate vehicle specifications and performance metrics. Unauthorized access to such data by third parties poses significant risks, including the compromise of user privacy and the potential detriment to a company's core business interests [16,17].

To address these challenges, the adoption of a differential privacy algorithm has emerged as a viable strategy for devising data privacy-protection schemes that are tailored to the nuances of the Internet of Things (IoT). This approach mandates that raw data remain exclusively stored locally, with all statistical outputs furnished to data collectors meticulously safeguarded through differential privacy calculations [16].

Furthermore, the integration of blockchain technology has introduced revolutionary paradigms for data sharing and management. By providing decentralized, distributed, and tamper-proof solutions, blockchain augments the security and reliability of data exchange. However, it is imperative to underscore that, while blockchain offers inherent advantages, it does not inherently guarantee privacy and data confidentiality. Thus, solutions leveraging blockchain technology must adopt a holistic approach to encompass comprehensive user privacy-protection considerations [17].

## 2.2. The Method

Table 1 shows the two types of privacy-protection methods introduced in this paper: one is the common encryption method, and the other is the advanced encryption-based method that integrates encryption with the existing advanced technology.

**Table 1.** Methods of Cryptography-Based Privacy Protection.

Methods	Submethods	Papers
Common Cryptography Methods	-	[18–37]
Advanced Methods Derived from Cryptography	Blockchain Federated learning Differential privacy	[38–45] [46–50] [8,51–53]

### 2.2.1. Common Cryptography Methods

Cryptography plays a pervasive role in vehicular networks to bolster privacy protection by safeguarding the confidentiality, integrity, and availability of information, all while meticulously constraining unauthorized access [7]. Empirical evidence substantiates its notable efficacy in preserving the privacy of vehicle data across diverse applications, including, but not limited to, communication, transactions, and charging processes. As such, encryption emerges as a dependable choice for fortifying the security of vehicle data in multifarious scenarios.

Data encryption serves as the cornerstone for safeguarding sensitive information within a vehicular network. Its pivotal role encompasses the protection of both vehicle data and user privacy against passive attacks, while simultaneously curtailing unauthorized access to vehicle data. This encompassing encryption protection extends to diverse facets, including, but not limited to, inter-vehicle communication, Vehicle-to-Infrastructure communication, and the secure storage of data within vehicular systems.

In the context of the Internet of Vehicles (IoVs), Homomorphic Encryption (HE) is heralded as a transformative technology that ensures data privacy during processing and analysis. This encryption method allows for direct computations on encrypted data, with results remaining encrypted until decrypted by the data owner. Such features make HE particularly suitable for protecting vehicle privacy in sensitive areas like driver behavior analysis, vehicle tracking, and V2X (Vehicle-to-Everything) communications. In V2X scenarios, HE secures transmitted data against unauthorized access and ensures that information remains private, even if intercepted [18]. The concept of fully homomorphic encryption, which remained an unresolved challenge in cryptography for many years, was

finally cracked by Gentry in 2009, who introduced the first fully homomorphic encryption scheme, enabling the evaluation of arbitrary circuits on encrypted data [20]. Subsequently, various HE schemes have been developed. Initially, these schemes were largely impractical; however, recent advancements in implementation techniques and a deeper understanding of potential applications have begun to shift this perspective. Recent versions of the Simple Encrypted Arithmetic Library (SEAL), developed by Microsoft Research, have enhanced core functionalities to improve practicality [19]. Despite its power, HE was once deemed too inefficient for practical use. Yet, performance has significantly evolved from Gentry's original model, with multiple robust libraries now supporting HE schemes and protocols, demonstrating notable performance and contributing to ongoing standardization efforts [21].

Additionally, several protocols and standards have been developed to enhance security in vehicular communications. The MACsec protocol, defined under IEEE 802.1AE standard [22], offers Authenticated Encryption, ensuring confidentiality, integrity, and authenticity of data on Automotive Ethernet using the Galois/Counter Mode (GCM) [23] of the Advanced Encryption Standard (AES) [24]. It operates at the Data Link layer of the ISO/OSI model, meeting the demands for high data rates and performance, particularly when integrated with hardware accelerators [25]. The IEEE 1609 [26] family of standards facilitates Wireless Access in Vehicular Environments (WAVE), creating uniform communication interfaces across automotive manufacturers. This includes defining secure architectures and standardized services that support secure V2V and V2I communications, crucial for applications such as vehicle safety, automated tolling, and traffic management. Specifically, IEEE 1609.2 [27] focuses on Security Services for Applications and Management Messages, detailing secure message formats, encryption methods, and the guidelines for secure message exchanges. TLS/DTLS protocols, initially prevalent in securing internet communications, are now increasingly applied in in-vehicle networks to encrypt communications between in-vehicle servers and vehicles [28]. CANcrypt secures Controller Area Networks by facilitating secure device authentication and encrypted communications, utilizing a dynamic key updating mechanism [29]. Trusted Platform Modules (TPMs), commonly used in computing environments for secure storage of encryption keys and certificates, are also adapted for vehicular use to safeguard sensitive data.

To further augment privacy protection, a selective sharing scheme (S2PD) is advanced in [30] for the purpose of facilitating sensitive data sharing within vehicle social networks. Within this architectural framework, users possess the capability to upload encrypted data along with corresponding encryption keys. Authorized users are subsequently empowered to employ these keys for secure data retrieval and decryption. In [31], an independent hybrid zone scheme is introduced with the primary objective of preserving the sensitive location information of vehicles. This model delineates a pseudonym scheme tailored to vehicular networks, encompassing both authentication and pseudonym models.

Furthermore, ref. [32] delves into the investigation of secure transmission strategies for multiple-input signal-output (MISO) vehicular relay networks. These strategies are devised to shield infrastructure nodes from potential jamming and eavesdropping attacks originating from vehicles situated outside the protected zone. The study furnishes optimized transmission schemes for two distinct scenarios: one emphasizing message confidentiality preservation while ensuring desired transmission rates, and the other focusing on enhancing average confidentiality while taking throughput into account. In the pursuit of expediting the key establishment process in 5G Vehicular Ad Hoc Networks (VANETs), ref. [33] proposes an efficient physical layer key extraction method. This method capitalizes on the received signal capacity to generate keys characterized by high bit generation rates and minimal bit contention.

Lastly, ref. [34] introduces a proactive scheme tailored to preventing Roadside Unit (RSU) hotspot attacks within edge computing-based VANETs. The primary objective of this scheme is to thwart eavesdropping attempts on traffic information amassed by RSUs.



Cryptography serves as a pivotal mechanism for implementing robust authentication and access control protocols within the context of vehicular networks, ensuring that only authenticated users or devices are granted access to sensitive information. The utilization of digital certificates and Public Key Infrastructure (PKI) plays a central role in authenticating vehicles and users, while access control policies meticulously govern which entities are permitted access to data, the timing of such access, and the specific purposes for which access is granted. This framework guarantees that data remain exclusively accessible to authorized individuals.

A pioneering proposal in [35] advocates the deployment of short-lived certificates to enable vehicles to authenticate communications effectively. This involves the acquisition of short-duration certificates by vehicles from RSUs through a mutually authenticated process. Given the inherent communication overhead and computational complexity associated with cryptography-based schemes, a spectrum of tailored bulk verification schemes have been introduced to enhance the efficiency of signature verification. In [36], the introduction of batch verification within in-vehicle networks marked a significant advancement. It adeptly harnesses the properties of bilinear mapping during the message-signing and -verification processes, facilitating the simultaneous verification of multiple messages and substantially reducing verification time. This pioneering approach has spurred the development of numerous protocols aimed at optimizing both efficiency and security levels. Trust-based mechanisms, as outlined in [37], are particularly suited to counter insider attackers. This study introduces a trust-based framework designed to enhance the efficacy of spam detection, thereby fortifying defenses against black hole attacks and Denial of Service (DoS) attacks.

Within the domain of the Internet of Vehicles, digital signatures come to the forefront as a means to ascertain the origin and integrity of data. This ensures the secure transfer of data from vehicles to infrastructure, with a guarantee that data remain unaltered during transmission. Ref. [54] introduces an innovative group-signature-based scheme in which each group designates a group leader for key management. Subsequently, group members communicate amongst themselves using shared group secret keys and group public keys.

In summary, the utilization of cryptography, digital certificates, and access control policies establishes a secure framework for authenticating and authorizing access to sensitive vehicular network data, while advanced cryptographic techniques and trust-based mechanisms further enhance the security and efficiency of vehicular networks and communications.

### 2.2.2. Advanced Methods Derived from Cryptography

Figure 2 represents a schematic diagram of the three cryptographic-based privacy-protection methods and shows how the three methods utilize cryptography.

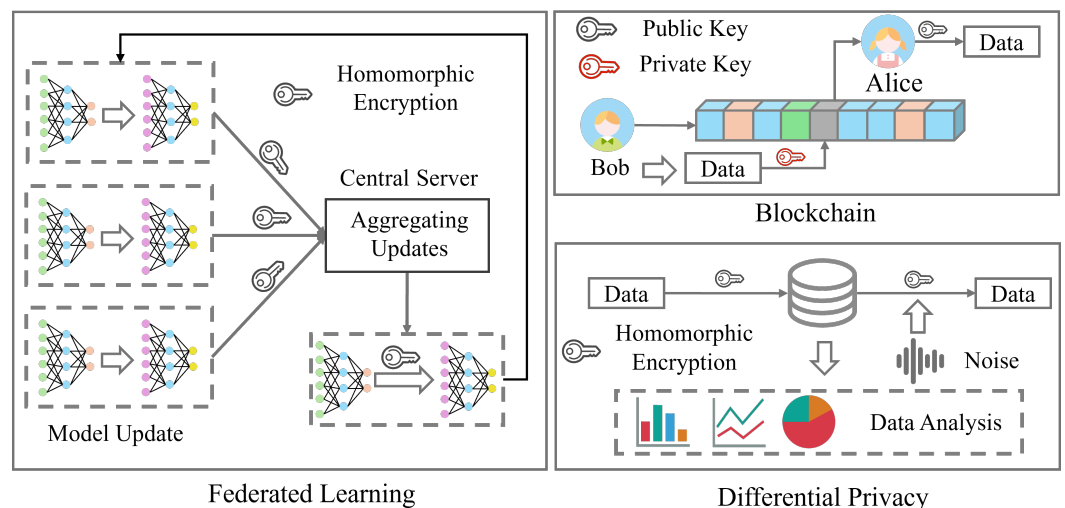


Figure 2. Schematics of the advanced methods derived from cryptography.

## Blockchain

Blockchain technology, underpinned by robust cryptographic algorithms, is a distributed ledger system, meticulously engineered to provide a secure repository for data. Cryptography is pivotal in enabling blockchain's key features of trustworthiness, transparency, and transaction traceability. This synergy between blockchain and cryptography enhances several intrinsic attributes of the technology, including decentralization, anonymity, and auditability [55]. Blockchain's application extends across diverse domains such as smart contracts, healthcare, communication systems, and finance, where it leverages these cryptographic foundations to bolster security. The integration of blockchain technology significantly enhances the security of distributed systems, particularly in cloud computing and the Internet of Things (IoT). As a result, blockchain emerges as a potent tool with significant potential to safeguard vehicle data and preserve privacy within the expansive landscape of the IoVs [56].

The blockchain-based VANET framework encompasses four pivotal stages: blockchain initialization, vehicle registration, Secure Broadcast Message (SBM) uploading, and blockchain record management. A paramount focus lies in safeguarding the identity and location privacy of participants. To address this challenge, ref. [38] presents a comprehensive solution that comprises UGG, IPP, and LPP algorithms, which are seamlessly integrated with dynamic threshold encryption and k-anonymity unity techniques during the SBM uploading phase within the blockchain-based VANETs context.

Within the ambit of cloud computing, the imperative for heightened security and protection is evident, as both authenticated users and potential attackers possess equal access rights within the Vehicular Cloud Computing (VCC) environment. In response, ref. [39] advocates the adoption of an effective and secure blockchain-based distributed cloud architecture as a transformative alternative to conventional cloud structures. This innovative approach serves to fortify drivers' privacy while simultaneously minimizing costs and facilitating on-demand sensing procedures within the Cooperative Roadside VANETs (CRVANETs) ecosystem.

The confluence of high-mobility, ad hoc network topologies, and the diverse spectrum of V2X interactions has ushered in a host of formidable challenges in TCP/IP-based vehicular networking. Pertinent concerns encompass key management, cache poisoning, and access control, among others, for developing Named Data Networking (NDN)-based Vehicular Edge Computing (VEC) networks. In response to these challenges, ref. [40] introduces a novel blockchain-based security architecture tailored for NDN-based VEC networks, offering a systematic approach to address these pressing security issues.

In the realm of energy trading, ref. [41] presents a decentralized blockchain-enabled energy trading scheme designed to facilitate cross-domain transactions efficiently. This innovative approach empowers reliable transactions between electric vehicles (EVs) and energy nodes, all while ensuring minimal processing delay. Additionally, comprehensive experimental evaluations are conducted to assess trading performance and location privacy-protection efficacy.

For user privacy and data safety in the context of the 5G IoVs, ref. [42] introduces a blockchain-enabled vehicular crowdsensing system. As vehicles evolve into consumer electronics products, privacy protection and data security have assumed paramount importance. This system caters to the growing concerns of users in vehicular crowdsensing applications by safeguarding their privacy and data integrity. Ref. [43] presents an innovative approach involving the utilization of a permissioned consortium blockchain system with smart contract capabilities. This methodology is devised to facilitate secure and conditionally privacy-preserving vehicular pseudonym issuance and management within the complex landscape of a multi-jurisdictional road network. The study successfully conducted a meticulous small-scale simulation of the proposed architecture utilizing the Vehicles in Network Simulation (Veins) platform, which seamlessly integrates traffic simulation services provided by SUMO and network simulation services offered by OMNeT++. Furthermore, the Hyperledger Fabric platform was employed as the foundation for the

permissioned consortium blockchain system, ensuring the security and integrity of the pseudonym issuance and management processes.

In the domain of VANETs, the paramount concerns of privacy protection and data security during network transmission and subsequent data analysis have garnered significant attention. Ref. [44] proposes a visionary approach in the form of a Decentralized VANETs (DVANETs) architecture. This architectural paradigm strategically disentangles computing tasks from centralized cloud services, redistributing them to edge computing (EC) nodes. This fundamental reconfiguration effectively mitigates network communication overhead and minimizes congestion delays, ultimately fortifying the security and efficiency of DVANETs.

Notably, extant data sharing systems deployed within VANETs often exhibit limitations in their ability to provide selective data sharing with an adequate degree of privacy protection. To address this critical gap, ref. [45] introduces an innovative vehicular communication system, denoted as the “blockchain-based privacy-preserving and sustainable data query service”. This pioneering system is meticulously designed to enhance privacy preservation while simultaneously ensuring sustainability within the context of VANETs, thereby bridging the existing gap in privacy and data sharing.

### Federated Learning

Federated learning, a technique grounded in cryptographic protocols, stands as a highly effective privacy-preserving methodology within the realm of connected vehicles. By utilizing cryptographic measures such as secure multi-party computing, federated learning facilitates collaborative model training among vehicles or devices without the need to disclose local data, thereby upholding stringent privacy safeguards. These cryptographic protocols include advanced techniques such as secret sharing and functional encryption, enhancing the security and privacy of the distributed learning process. Moreover, within the domain of vehicular networks, federated learning is often strategically deployed in conjunction with cutting-edge technologies, including blockchain and differential privacy techniques, to fortify the comprehensive privacy-protection framework. Ref. [46] introduces a pragmatic privacy-preserving collaborative deep learning system that facilitates the cooperative construction of a collective deep learning model using data contributed by all participants, all while circumventing the need for direct data sharing and central data storage. To further mitigate potential privacy breaches stemming from the sharing of model parameters, this research leverages functional mechanisms to perturb the objective function of the neural network during the training process, thereby achieving  $\epsilon$ -differential privacy.

In the context of the IoVs, ref. [47] presents a novel NDN-based architectural framework, bolstered by Mobile Edge Computing (MEC). Within this proposed NDN-based architecture tailored for MEC-empowered IoVs, a federated learning scheme based on local differential privacy is deployed to enable rapid response and informed decision-making.

The burgeoning growth of interconnected networks, characterized by the exponential influx of heterogeneous data generated at the network edge, necessitates the development of distributed machine learning techniques. In response, a two-layer federated learning model is posited in [48]. This model capitalizes on the distributed end–edge–cloud architecture commonly encountered in the 6G environment, optimizing the efficiency and accuracy of the learning process while simultaneously ensuring robust data privacy protection and curtailing communication overheads. Ref. [49] introduces a comprehensive multi-party privacy-preserving machine learning framework, aptly named PFMLP. This framework is rooted in partially homomorphic encryption and federated learning techniques. The research delves into an in-depth comparative analysis, considering factors such as encryption key length, learning network structure, the number of learning clients, and more. These advanced methodologies address the challenge of safeguarding privacy in scenarios involving a substantial volume of data required for power load model training. To overcome



these challenges, [50] devises the FRF–CNN model, a hybrid solution that amalgamates federated learning, random forest, and convolutional neural network approaches.

### Differential Privacy

Differential privacy, a cornerstone in the field of cryptography, is a rigorous framework designed to make the outcomes of queries indistinguishable, even when only minor discrepancies exist in the underlying datasets [57]. This cryptographic approach achieves privacy through the deliberate introduction of random noise at various stages of data processing, including collection, aggregation, and distribution. By adding stochastic values to individual data points, it ensures the privacy of each data contributor. When specific data queries are necessary, differential privacy acts as a formidable tool to protect the results. Controlled noise is introduced into the query process to ensure that sensitive individual data are not inadvertently disclosed. Additionally, the integration of differential privacy with deep learning models is crucial for enhancing data privacy during both the training and inference phases. This combination is particularly significant in the domain of vehicular networks, where machine learning tasks require stringent data-protection measures.

During the charging process of electric vehicles, there exists a vulnerability wherein the location and movement trajectories of these vehicles can be potentially exposed, thereby precipitating a cascade of intricate privacy and security challenges. In response to this pressing concern, ref. [51] presents an innovative spatial decomposition algorithm based on quadtrees. This algorithm is strategically devised to fortify the location privacy of electric vehicles, shielding them from inadvertent disclosure.

Traditional approaches to safeguarding trajectory data often exhibit limitations, with some focusing solely on geographical location protection, while others concentrate solely on semantic location preservation. In alignment with the principles of differential privacy, ref. [52] introduces an optimized privacy scheme grounded in differential privacy, enriched by reinforcement learning techniques within the context of vehicular ad hoc networks.

While differential privacy garners considerable attention due to its rigorous definition and robust privacy assurances, recent research highlights its susceptibility to correlated data, potentially compromising individual privacy. Ref. [53] delves into a multifaceted exploration of perturbation mechanisms, examining them from two distinct perspectives to mitigate this vulnerability.

In addition, ref. [8] delves into the intricacies of dismantling data barriers while concurrently upholding privacy protection. The study shifts the paradigm of vehicle data representation from textual format to a graph-structured data form, systematically accounting for the volume of interactive data and potential privacy leakage during data dissemination. Notably, the article introduces innovative concepts such as graph differential privacy (DP) and anonymity protection to robustly safeguard vehicle privacy within this evolving landscape.

## 2.3. The Different Disclosure Entities

### 2.3.1. Internal Threats

Internal personnel or system administrators possess the potential to misuse their authorized privileges, thereby gaining access to sensitive data. Consequently, it is imperative to implement measures aimed at mitigating internal security threats.

### 2.3.2. External Threats

Malicious hackers and external threat actors may endeavor to infiltrate the vehicular network system. Therefore, it is imperative to implement heightened security measures to fortify defenses against external threats.

### 2.3.3. Third-Party Partners

The sharing of data with third-party service providers and data-sharing partners necessitates the establishment of rigorous contractual agreements and privacy arrangements to guarantee the proper safeguarding of data.

## 3. Challenges

The tradeoff between information loss and information availability in VNs presents a significant challenge: it requires carefully preserving user privacy through controlled information loss while simultaneously ensuring that the data remain sufficiently detailed and accessible to support the network's functionality. In VNs, this balance is particularly crucial, as these networks handle sensitive data like location and travel patterns, which must be protected in order to maintain user privacy. However, overly restricting data flow or excessively anonymizing it can undermine the network's effectiveness in areas such as traffic management, safety enhancement, and real-time decision-making. Thus, finding an equilibrium where privacy is safeguarded without sacrificing the critical utility of the data is key to the successful operation of vehicular networks.

In VNs, the dynamic and rapidly changing nature of information and models, coupled with the necessity for frequent multi-interactions, creates significant pressure on wireless channels. This scenario demands a high bandwidth to accommodate the continuous and simultaneous exchange of vast amounts of data. However, the limited availability and capacity of wireless channels often struggle to keep pace with these demands, leading to potential bottlenecks in communication. This challenge is further amplified by the need for real-time data transmission, which is critical for ensuring efficient traffic management and safety in VNs. Thus, optimizing wireless channel usage and enhancing its capacity are essential for maintaining the smooth and efficient operation of vehicular networks.

The real-time updating of information and models in VNs presents a substantial challenge in terms of data storage. As the number of vehicles within the network increases, the volume of data generated and needing to be stored escalates correspondingly. Each vehicle not only contributes to the influx of real-time data but also necessitates a certain amount of data backup for operational and safety purposes. This continuous and voluminous data stream exerts significant pressure on existing storage resources, demanding not just larger storage capacities but also more efficient data management strategies to ensure that the critical information is stored securely, accessibly, and in a manner that supports the network's real-time decision-making capabilities.

Privacy concerns in VNs often necessitate restrictions on the transmission of sensitive information and models, posing a notable challenge. Such limitations, while crucial for safeguarding user data, can impede the inherently collaborative functionality of these networks. This constraint potentially affects the overall efficiency and effectiveness of VNs, as the restricted flow of critical data might hinder the network's ability to make informed decisions, optimize traffic flow, and enhance safety measures. Balancing the need for privacy with the imperative of seamless data exchange thus becomes a key issue in maintaining the operational integrity of vehicular networks.

The implementation of blockchain and federated learning methods in VNs places a significant demand on computational resources and capabilities. These advanced techniques, while offering enhanced privacy and security, are computationally intensive, potentially challenging the feasibility of their deployment in VNs, particularly those constrained by limited computing power. The intensive processing needs for maintaining a blockchain's distributed ledger or for executing federated learning algorithms, which involve complex data computations across multiple nodes, can strain the existing computational infrastructure of VNs. This presents a critical challenge: ensuring that these networks are equipped with sufficient computational capacity to leverage these privacy-preserving technologies without compromising their operational efficiency and real-time responsiveness.

The inherent distributed structure of VNs often lacks a strong internal drive for mutual privacy protection among participating entities, presenting a unique challenge. This de-

centralized nature can lead to uneven adoption and implementation of privacy-enhancing measures, as individual nodes in the network may not uniformly prioritize or have the capability to implement such measures. This inconsistency in privacy protection across the network not only poses risks to data security but also undermines the collective trust and efficacy of the network. Ensuring that all entities within VNs are equally committed to and equipped for robust privacy protection is essential for maintaining the overall integrity and trustworthiness of these complex, interconnected systems.

The implementation of cryptography methods in secure communications often entails multiple exchanges of cryptographic keys, a process that can introduce security vulnerabilities if not managed with utmost care. Each key exchange represents a potential point of attack, where unauthorized entities might intercept or compromise the keys, thereby undermining the security of the encrypted communication. This challenge necessitates not only robust encryption algorithms but also secure and efficient key management protocols to ensure that the integrity and confidentiality of the data are maintained throughout the key exchange and subsequent communication processes. Managing this aspect effectively is crucial for upholding the security standards in any system relying on cryptographic methods for data protection.

Relying on third parties for the generation and delivery of cryptographic keys in secure communication systems introduces significant trust challenges. This reliance places a critical aspect of security—the handling of keys which are the cornerstone of encryption—in the hands of external entities. Ensuring the trustworthiness, security, and reliability of these third parties is paramount, as any breach or lapse in their integrity could compromise the entire encryption process. This challenge necessitates rigorous vetting, continuous monitoring, and robust legal and technical safeguards to ensure that these third parties adhere to the highest standards of security and reliability in their operations. The difficulty lies in establishing and maintaining this level of trust while balancing the practicalities of working with external partners in a security-sensitive environment.

While the use of encryption to protect privacy in IoVs can enhance security, it also poses challenges in terms of computational resources, storage requirements, and energy consumption. For example, the encryption process requires a significant amount of computational power that may be beyond the processing power of some vehicles, while encrypted data increase storage and energy requirements. In addition, real-time is an important requirement in the IoVs, while encryption and decryption delays may affect the responsiveness of the system. Key management is also a challenge in IoVs and needs to be carefully designed to prevent key leakage or misuse. Standardization of encryption algorithms and compatibility issues needs to ensure interoperability between different devices. The development of quantum computing poses a threat to existing cryptographic techniques, and security strategies need to be proactively strengthened to protect against potential quantum attacks. In conclusion, IoVs encryption strategies need to balance practicality and security, optimize system design, effectively manage resources, and develop comprehensive security standards and policies through cross-disciplinary cooperation. This is the way to meet the real-time and operational efficiency requirements of IoVs while improving security.

#### 4. Discussion

In summary, privacy-protection technologies and techniques are evolving to meet the new challenges posed by technological and business developments. However, all the above privacy-protection methods are based on one premise, i.e., all vehicles, in addition to the arithmetic power required for their own traveling, selflessly contribute additional arithmetic power for the operation of privacy protection, even if the object of protection is not themselves. However, this major premise is actually not reasonable to a certain extent, as arithmetic power can be said to be a scarce resource in IoVs due to its strong demand for high-rate communication. As a result, many of the algorithms modeled in the literature are relatively ideal.

With the development of blockchain and other new technologies, many industries are facing changes in new business models and leaps in application paradigms. Cryptography algorithms combined with blockchain, artificial intelligence, the Internet of Things, and other new technologies will promote the industry to realize the transformation from a centralized application form to a distributed application form. For example, blockchain technology based on multi-party secure computing cryptography algorithms can help build large-scale collaboration and interaction networks based on algorithms to safeguard trust and value transfer; artificial intelligence technology based on cryptography can realize the automation and intelligence of data processing and business under the premise of security.

Considering that the development of distributed secure computing can enable every individual who contributes data or resources to obtain the corresponding value in the group, this extension from group benefits to individual benefits may be the key to solving the above problems. The guarantee of individual resource interests realized through technology and algorithms can effectively realize the problem of individual arithmetic contribution in the community, and the establishment of a cyclic ecology of mutual protection of other individuals' private data may become a new development prospect for the future of vehicular network security and privacy protection.

**Author Contributions:** Conceptualization, Y.L. and M.W.; methodology, N.J.; validation, F.L.; formal analysis, X.J.; writing—original draft preparation, M.W.; writing—review and editing, Y.L. and R.B.; supervision, R.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding

**Data Availability Statement:** This manuscript aims at theoretical analysis, which does not involve simulation experiments. Therefore, there is no dataset has to be publicly available.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Sağlam, E.T.; Bahtiyar, Ş. A survey: Security and privacy in 5G vehicular networks. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 108–112.
2. Corser, G.P.; Fu, H.; Banihani, A. Evaluating location privacy in vehicular communications and applications. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 2658–2667. [[CrossRef](#)]
3. Li, G.; Li, L.; Li, J.; Li, Y. Network Voronoi Diagram on uncertain objects for nearest neighbor queries. *Inf. Sci.* **2015**, *301*, 241–261. [[CrossRef](#)]
4. Peng, T.; Liu, Q.; Meng, D.; Wang, G. Collaborative trajectory privacy preserving scheme in location-based services. *Inf. Sci.* **2017**, *387*, 165–179. [[CrossRef](#)]
5. Talat, H.; Nomani, T.; Mohsin, M.; Sattar, S. A survey on location privacy techniques deployed in vehicular networks. In Proceedings of the 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 8–12 January 2019; pp. 604–613.
6. LaMarca, A.; Langheinrich, M.; Truong, K.N. *Pervasive Computing: 5th International Conference, PERSASIVE 2007, Toronto, Canada, May 13–16, 2007, Proceedings*; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4480.
7. Wu, X.; Xu, X.; Bilal, M. Toward privacy protection composition framework on internet of vehicles. *IEEE Consum. Electron. Mag.* **2021**, *11*, 32–38. [[CrossRef](#)]
8. Li, Y.; Tao, X.; Zhang, X.; Wang, M.; Wang, S. Break the data barriers while keeping privacy: A graph differential privacy method. *IEEE Internet Things J.* **2022**, *10*, 3840–3850. [[CrossRef](#)]
9. Huang, J.; Fang, D.; Qian, Y.; Hu, R.Q. Recent advances and challenges in security and privacy for V2X communications. *IEEE Open J. Veh. Technol.* **2020**, *1*, 244–266. [[CrossRef](#)]
10. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [[CrossRef](#)]
11. Hataba, M.; Sherif, A.; Mahmoud, M.; Abdallah, M.; Alasmay, W. Security and privacy issues in autonomous vehicles: A layer-based survey. *IEEE Open J. Commun. Soc.* **2022**, *3*, 811–829. [[CrossRef](#)]
12. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [[CrossRef](#)]
13. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [[CrossRef](#)]
14. Voigt, P.; Von dem Bussche, A. The eu general data protection regulation (gdpr). In *A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10, pp. 10–5555.

15. Xu, C.; Wu, H.; Liu, H.; Gu, W.; Li, Y.; Cao, D. Blockchain-oriented privacy protection of sensitive data in the internet of vehicles. *IEEE Trans. Intell. Veh.* **2022**, *8*, 1057–1067. [[CrossRef](#)]
16. Luo, X.; Wang, J.; Xu, J.; Shen, M. Research on Data Privacy Protection of Internet of Vehicles Based on Differential Privacy. *Proc. IOP Conf. Ser. Earth Environ. Sci.* **2020**, *428*, 012007. [[CrossRef](#)]
17. Chen, W.; Wu, H.; Chen, X.; Chen, J. A review of research on privacy protection of internet of vehicles based on blockchain. *J. Sens. Actuator Netw.* **2022**, *11*, 86. [[CrossRef](#)]
18. Chen, H.; Laine, K.; Player, R. Simple encrypted arithmetic library-SEAL v2. 1. In Proceedings of the Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, 7 April 2017; Revised Selected Papers 21; Springer: Berlin/Heidelberg, Germany, 2017; pp. 3–18.
19. Hallman, R.A.; Laine, K.; Dai, W.; Gama, N.; Malozemoff, A.J.; Polyakov, Y.; Carпов, S. Building applications with homomorphic encryption. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 2160–2162.
20. Di Matteo, S.; Gerfo, M.L.; Saponara, S. VLSI Design and FPGA implementation of an NTT hardware accelerator for Homomorphic seal-embedded library. *IEEE Access* **2023**, *11*, 72498–72508. [[CrossRef](#)]
21. Garay, J.A.; Gennaro, R. *Advances in Cryptology—CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2014, Proceedings, Part II*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8617.
22. 802.1AC-2016/Cor 1-2018; IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Service Definition-Corrigendum 1: Logical Link Control (LLC) Encapsulation EtherType. IEEE: Piscataway, NJ, USA, 2018.
23. Dworkin, M.J. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*; Special Publication (NIST SP); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2007.
24. Dworkin, M.; Barker, E.; Nechvatal, J.; Fote, J.; Bassham, L.; Roback, E.; Dray, J. *Advanced Encryption Standard (AES)*; Federal Inf. Process. Stds. (NIST FIPS); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001; Volume 11.
25. Carnevale, B.; Falaschi, F.; Crocetti, L.; Hunjan, H.; Bisase, S.; Fanucci, L. An implementation of the 802.1 AE MAC Security Standard for in-car networks. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 24–28.
26. Liu, T.J.; Chen, C.W. Wireless access in vehicular environments. In *Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications*; IGI Global: Hershey, PA, USA, 2010; pp. 90–107.
27. ITS Committee. *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*; IEEE Vehicular Technology Society: Washington, DC, USA, 2013; Volume 1609.
28. Rescorla, E. *The Transport Layer Security (TLS) Protocol Version 1.3*; Technical Report; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2018.
29. Pfeiffer, O. *Implementing Scalable Can Security with Cancrypt*; Embedded Systems Academy: Sunnyvale, CA, USA, 2017.
30. Feng, X.; Wang, L. S2PD: A selective sharing scheme for privacy data in vehicular social networks. *IEEE Access* **2018**, *6*, 55139–55148. [[CrossRef](#)]
31. Guo, N.; Ma, L.; Gao, T. Independent mix zone for location privacy in vehicular networks. *IEEE Access* **2018**, *6*, 16842–16850. [[CrossRef](#)]
32. Tyagi, P.; Dembla, D. Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation. In Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, 24–27 September 2014; pp. 2084–2090.
33. Li, X.; Liu, J.; Yao, Q.; Ma, J. Efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks. *IEEE Access* **2017**, *5*, 5281–5291. [[CrossRef](#)]
34. Huang, X.; Yu, R.; Pan, M.; Shu, L. Secure roadside unit hotspot against eavesdropping based traffic analysis in edge computing based internet of vehicles. *IEEE Access* **2018**, *6*, 62371–62383. [[CrossRef](#)]
35. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
36. Zhang, C.; Lu, R.; Lin, X.; Ho, P.H.; Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 246–250.
37. Raya, M.; Papadimitratos, P.; Gligor, V.D.; Hubaux, J.P. On data-centric trust establishment in ephemeral ad hoc networks. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1238–1246.
38. Li, H.; Pei, L.; Liao, D.; Sun, G.; Xu, D. Blockchain meets VANET: An architecture for identity and location privacy protection in VANET. *Peer-Netw. Appl.* **2019**, *12*, 1178–1193. [[CrossRef](#)]
39. Nadeem, S.; Rizwan, M.; Ahmad, F.; Manzoor, J. Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 288–295. [[CrossRef](#)]
40. Lei, K.; Fang, J.; Zhang, Q.; Lou, J.; Du, M.; Huang, J.; Wang, J.; Xu, K. Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks. *J. Grid Comput.* **2020**, *18*, 593–613. [[CrossRef](#)]



41. Long, Y.; Chen, Y.; Ren, W.; Dou, H.; Xiong, N.N. Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k-anonymity. *IEEE Access* **2020**, *8*, 192587–192596. [[CrossRef](#)]
42. Wang, S.; Sun, S.; Wang, X.; Ning, Z.; Rodrigues, J.J. Secure crowdsensing in 5G internet of vehicles: When deep reinforcement learning meets blockchain. *IEEE Consum. Electron. Mag.* **2020**, *10*, 72–81. [[CrossRef](#)]
43. Chulerttiyawong, D.; Jamalipour, A. A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement. *IEEE Access* **2021**, *9*, 127305–127319. [[CrossRef](#)]
44. Chen, J.; Li, K.; Philip, S.Y. Privacy-preserving deep learning model for decentralized vanets using fully homomorphic encryption and blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 11633–11642. [[CrossRef](#)]
45. Yeh, L.Y.; Shen, N.X.; Hwang, R.H. Blockchain-based privacy-preserving and sustainable data query service over 5G-VANETs. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 15909–15921. [[CrossRef](#)]
46. Zhao, L.; Wang, Q.; Zou, Q.; Zhang, Y.; Chen, Y. Privacy-preserving collaborative deep learning with unreliable participants. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1486–1500. [[CrossRef](#)]
47. Han, X.; Tian, D.; Duan, X.; Sheng, Z.; Zhou, J.; Leung, V.C. A Dual Mode Privacy-Preserving Scheme Enabled Secure and Anonymous for Edge Computing Assisted Internet of Vehicle Networks. In Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Alicante, Spain, 22–26 November 2021; pp. 65–70.
48. Zhou, X.; Liang, W.; She, J.; Yan, Z.; Kevin, I.; Wang, K. Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5308–5317. [[CrossRef](#)]
49. Fang, H.; Qian, Q. Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet* **2021**, *13*, 94. [[CrossRef](#)]
50. Wu, Y.; Shen, Z.; Tian, Y.; Cai, Z.; Li, F. Electric vehicle charging load forecasting based on federal learning. In Proceedings of the International Conference on Electronic Information Engineering and Computer Communication (EIECC 2021), Changchun, China, 23–26 May 2021; Volume 12172, pp. 229–234.
51. Li, Y.; Zhang, P.; Wang, Y. The location privacy protection of electric vehicles with differential privacy in V2G networks. *Energies* **2018**, *11*, 2625. [[CrossRef](#)]
52. Chen, X.; Zhang, T.; Shen, S.; Zhu, T.; Xiong, P. An optimized differential privacy scheme with reinforcement learning in VANET. *Comput. Secur.* **2021**, *110*, 102446. [[CrossRef](#)]
53. Chen, J.; Ma, H.; Zhao, D.; Liu, L. Correlated differential privacy protection for mobile crowdsensing. *IEEE Trans. Big Data* **2017**, *7*, 784–795. [[CrossRef](#)]
54. Lin, X.; Sun, X.; Ho, P.H.; Shen, X. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
55. Xu, L.; Chen, L.; Gao, Z.; Carranco, L.; Fan, X.; Shah, N.; Diallo, N.; Shi, W. Supporting blockchain-based cryptocurrency mobile payment with smart devices. *IEEE Consum. Electron. Mag.* **2020**, *9*, 26–33. [[CrossRef](#)]
56. Benarous, L.; Boudjit, S. Security and privacy evaluation methods and metrics in vehicular networks. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 1–6.
57. Jiang, W.; Chen, M.; Tao, J. Federated learning with blockchain for privacy-preserving data sharing in Internet of vehicles. *China Commun.* **2023**, *20*, 69–85. [[CrossRef](#)]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.