Abstract: Currently, the outbreak of COVID-19 pandemic has caused catastrophic effect on every aspect of our lives, globally. The entire human race of all countries and regions has suffered devastating losses. With its high infectiousness and mortality rate, it is of great significance to carry out effective precautions and prevention of COVID-19. Specifically, the transportation system has been confirmed as one of the crucial spreading routes. Hence, enhancing healthcare monitoring and infection tracking for high-mobility transportation system is infeasible for pandemic control. Meanwhile, due to the promising advantages in the emerging intelligent transportation system (ITS), vehicular ad hoc networks (VANETs) is able to collect and process relevant vehicular data for improving the driving experience and road safety, which provide a way for non-contact automatic healthcare monitoring. Furthermore, the proliferating cloud computing and blockchain techniques enable sufficient processing and storing capabilities, along with decentralized remote auditing towards heterogenous vehicular data. In this case, the automated infection tracking for pandemic control could be achieved accordingly. For the above consideration, in this paper we develop a practical homomorphic authentication scheme for cloud-assisted VANETs, where the healthcare monitoring for all involving passengers is provided. Notably, the integrated cloud-assisted VANET infrastructure is utilized, where the hybrid medical data acquisition module is attached. In this way, timely, non-contact measurement on all passengers’ physical status can be remotely done by vehicular cloud (VC), which could also drastically improve the efficiency and guarantee safety. Vulnerabilities of the employed dedicated-short-range-communication (DSRC) technique could be properly addressed with the applied homomorphic encryption design. Additionally, the decentralized blockchain-based vehicle recording mechanism is cooperatively performed by VC and edge units. Infection tracking on specific vehicle and individual can be offered in this way. Each signature sequence is collaboratively maintained and verified by the current roadside unit (RSU) and its neighbor RSUs. The security analysis demonstrates that the proposed scheme is secure against major attacks, while the performance comparison with the state-of-the-arts relevant methods are presented for efficiency discussion.

Keywords: vehicular ad hoc networks (VANETs); blockchain; homomorphic encryption; pandemic control; infection tracking

1. Introduction

Nowadays, the entire world is facing a severe global health crisis unlike any in the history, which is spreading human suffering and upending people’s lives. The coronavirus disease COVID-19, which is characterized as a lethal and highly infectious pandemic by the World Health Organization (WHO),
has caused thousands of deaths around the world and is keeping attacking societies at their core. So far, the COVID-19 outbreak has affected all segments of population grievously and it is particularly detrimental to every social groups within the most vulnerable situations. Devastating health and economic impacts of the pandemic are being borne by everyone worldwide. When considering the high infectiousness and mortality rate, effective precautions and prevention strategies on COVID-19 is indispensable for pandemic control. Meanwhile, due to its comparatively high-density population in enclosed space and untraceable characteristics, the transportation system has been confirmed as one of the crucial spreading routes of COVID-19 [1,2]. As for public transportation tools including railway, subway, airplane, and the corresponding public locations, like airport, train station, strict detection, and surveillance mechanisms, have been adopted by most of countries so far [3]. However, infection tracking and detection for spontaneous vehicles in public highway still depends on manual work, which requires huge labor forces and financial resource [4–6]. Moreover, the working personnel also faces inevitable risks due to close physical contact with possible infectors.

With the urgent requirements on pandemic control, the unique advantages of vehicular ad hoc networks (VANETs) could be taken into consideration [7,8]. That is, the advanced healthcare monitoring and infection tracking, which are the two most important factors of COVID control, could be carried out by VANETs in a non-contact way. Hence, the working personnel do not need to carry out highly-risky surveillance in each checkpoint station. Instead, each RSU could be assigned as the automatic checkpoint if necessary [9,10]. On the other hand, historical route tracking towards suspected infectors is also available, provided that the sensitive medical data are uploaded to the remote VC, along with the confidential vehicle route information [11,12]. In this way, effective pandemic control strategy against COVID-19 could be achieved with VANETs. In order to provide innovative vehicular data processing and traffic management analysis, the VANET is considered as the critical component of emerging intelligent transportation system (ITS) in populous metropolitan cities and regions [13–15]. Generally, VANET is the distributed heterogeneous wireless network that is constructed among vehicles and roadside facilities with the functionalities of real-time dynamic vehicular data transmission [16]. VANET facilitates advanced driving security and improves the driving experience.

A fundamental VANET infrastructure is composed of road-side unit (RSU), trusted authority (TA), and terminal vehicles [17–19]. TA performs as the centralized service center in charge of all the corresponding system settings, such as vehicle initialization and user registration, confidential key generation [20,21]. Currently, advanced cloud computing and edge data processing techniques have been adopted, so as to provide sufficient data processing capacity for massive vehicular data [22,23]. Hence, the cloud-assisted TA is able to simultaneously manage different VANET implementations, the global Internet of Vehicles (IoV) initiatives can be achieved in this way [24,25]. The rode-side units are the distributive VANET facilities that are responsible for instant interaction with all vehicles in the vicinity. Specifically, the edge computing architecture could be utilized between RSUs with the purpose of providing low-latency and reliable data transmission with remote TA [26,27]. The edge cluster that involves neighboring RSUs collaboratively cache the frequently used vehicular data instead of requesting it from remote TA. The bandwidth burden of cloud server can be alleviated in this way. On the other hand, the vehicles are defined as the VANETs users where massive heterogenous data and driving characteristics are aggregated and forwarded for further processing [28–30].

VANETs enable two distinctive data transmission types: vehicle-to-RSU (V2R) and vehicle-to-vehicle (V2V). They are both powered with the 802.11p-based dedicated short-range communication (DSRC) technique [31–33]. V2V communication refers to the wireless data exchange of surrounding vehicles, which could help avoid crashes, ease traffic congestion, and improve the environment. The transmitted data include speed, location, direction of travel, braking, and loss of stability. V2R communication refers to the direct data interaction between each vehicle and nearby RSU. Intuitively, security and privacy protection mechanisms are of significance due to the open
wireless data transmission characteristics of VANETs. That is, the transmitted vehicular data may be illegally eavesdropped or forged by adversaries, thus compromising the VANET data safety [34,35].

Nowadays, lots of studies with various safe strategies and cryptographic techniques have been made on VANET secure data transmission in order to address the VANET security issues [36–38]. However, the necessary parameters for practical implementation of VANET system have not yet been fully considered. When considering the globally urgent situation on COVID-19 pandemic control, potential usages and valuable applications of VANETs should be dug out. Measurements regarding VANETs and its relevant extensions should be prepared, now that the transportation system have become the one of the most dangerous scenarios for virus surveillance and infection tracking.

With the urgent motivation for automotive pandemic control, a practical homomorphic authentication scheme for cloud-assisted VANETs is developed. The proposed mechanism supports automotive healthcare monitoring and infection tracking for all involving passengers. Non-contract surveillance towards random vehicles can be remotely conducted by VC. First of all, our design applies the novel cloud-assisted VANET infrastructure with the hybrid medical data acquisition module. The WBAN layer is adopted for the integrated medical data acquisition. Notably, the essential user information on participating device is shared among edge RSU cluster. Secondly, the homomorphic encryption design is deployed for mutual authentication and key agreement. Meanwhile, the decentralized blockchain-based infection tracking mechanism on suspicious vehicles is presented. The historical route records for each vehicle can be securely preserved in VC. The signature sequence is collaboratively arranged by several RSUs at a time, offering distributive data confidentiality. Respectively, the security analysis and performance analysis are proposed, showing the superiority of the proposed scheme.

The remainder of this paper is organized, as follows. Section 2 briefly introduces the related research achievements. Section 3 illustrates the preliminary contents and relevant system settings. Section 4 presents the proposed homomorphic authentication design in cloud-assisted VANETs with blockchain-based healthcare monitoring for pandemic control. Section 5 presents the security analysis. Section 6 displays the performance analysis. The final conclusion is drawn in Section 7.

2. Related Works

Currently, many researches on VANET secure data transmission and privacy preservation have been made, while the practical requirements for medical surveillance in practical occasions have not been fully satisfied. In 2013, a expedite message authentication protocol (EMAP) is constructed for VANET secure data transmission [17]. The efficient revocation check process is enabled with the keyed hash message authentication code (HMAC), which drastically reduces the computation burdens of certificate revocation lists (CRLs). Meanwhile, the proposed EMAP deploys the probabilistic key distribution function for confidential key sharing among non-revoked OBUs during key updating. Afterwards, a privacy-preserving authentication scheme for VANETs is developed in [21], where the designated RSUs distribute the group private information to vehicles within its arranged domain. In this case, massive vehicles can be efficiently verified without causing extensive time consumption. Chuang et al. [20] presented a decentralized trust-extended message authentication mechanism (TEAM), where the transitive trust relationships frame is utilized, so as to reduce storage consumption. Similarly, Wang et al. presented a two-factor lightweight VANETs authenticating scheme in [24], where the decentralized certificate authority (CA) and biological password are applied. The non-repudiation property for conditional tracing is achieved. In 2019, Alazzawi et al. developed a pseudo-identity-based message verification scheme [15]. Data integrity and mutual authentication can be provided. Moreover, the proposed scheme is resistant to insider attack and man-in-the-middle (MITM) attack.

Specifically, lots of schemes on vehicle conditional-privacy preserving (CPP) property have been developed. In 2010, a scalable robust authenticating method for secure VANETs transmission is proposed in [1]. Each RSU is responsible for maintaining the active vehicular groups within its vicinity. The authentic V2V broadcast is available for all participating vehicles with anonymous
identities. The benign third party is involved in the relevant vehicle revocation process. The negative impact of compromised RSUs is minimized in this case. Meanwhile, system salability is provided. Thereafter, Huang et al. developed the privacy-preserving authentication scheme with conditional privacy protection. The anonymous identity for each legitimate vehicle is activated until further revocation [3]. In 2012, a dynamic key arrangement mechanism with efficient updating for location-based services (LBSs) is proposed [9]. The double registration detection design is adopted. The newly joined vehicle autonomously updates its session key for forward secrecy. Subsequently, He et al. proposed an identity-based pairing-free mutual authentication and privacy protection method [7]. Better performance and minimized computational complexity for information processing can be achieved in this way. Similarly, a two-round certificateless-based cross-domain key agreement scheme for wireless mesh networks is presented [30]. The user in previous is adomainble to prove its identity to the current domain server for session key negotiation.

Currently, the VANET scenarios with cloud computing and blockchain techniques for remote data storing and parallel processing have been studied [33,34]. In 2017, Liu et al. constructed a vehicular message safe dissemination mechanism CMDS in the cloud-assisted VANET-cellular environment [31]. Reliable and confidential data processing can be processed by the related VANET gateways and nearby vehicles. Thereafter, emphasizing on emergency message dissemination, solution to the congestion avoidance issue is proposed in the assumed vehicular fog-assisted VANET [38]. Lin et al. discussed the vehicle heterogeneity of resource allocation in the vehicular cloud computing (VCC) system [37]. Optimal strategy for VCC allocation is presented under the improved semi-Markov decision process (SMDP) model. In 2019, Ma et al. proposed an efficient pairing-free authenticated key agreement design for secure interactions in fog-based VANETs [35]. As for blockchain infrastructure in VANETs, a blockchain-assisted distributed lightweight anonymous authentication scheme with cross-datacenter interaction in vehicular fog service (VFS) is presented [4]. Similarly, in [29], with the applied Merkle Patricia tree (MPT) structure, the conventional blockchain structure is extended. Hence, the distinctive verification process without CRLs is developed. Conditional privacy preserving is achieved as well.

To be concluded, existing researches on VANETs communication either emphasize security and privacy preserving with conventional cryptographic design or construct authenticated key agreement under advanced techniques such as cloud computing and blockchain. However, the potential usages of VANETs application have not been taken full consideration for pandemic control. For this purpose, we proposed a practical homomorphic authentication scheme with the unique functionalities of healthcare surveillance and infection tracking, which is of great significance for the pandemic control towards COVID-19.

3. Preliminaries

In this section, the necessary security and cryptographic concepts are respectively introduced, which include the definitions of homomorphic encryption, one-way hash function, and elliptic curve cryptosystem (ECC). Afterwards, the relevant notations of the proposed design, the novel VANET system model, and security requirements are illustrated.

3.1. Homomorphic Encryption

With its unique properties, homomorphic encryption can be widely applied into vast security designs and privacy preserving strategies. The homomorphic encryption design allows for the predefined standard computations on ciphertexts, with which the output matches the encryption result on the computations conducted on plaintexts. Hence, the transmitted data can be securely processed and out-sourced without revealing the privacy-related information. In other words, the related homomorphic encryption and decryption functionalities can be considered as the homomorphisms between plaintext and the ciphertext spaces. In practical communication scenarios with semi-trusted entities, homomorphic encryption could remove potential privacy barriers that inhibit data sharing,
The Paillier cryptosystem [39] is defined as one of the homomorphic cryptosystems on public key infrastructure (PKI). The Paillier encryption process is additively homomorphic. That is, the product of the two ciphertexts will decrypt to the sum of their corresponding plaintexts. In this case, \( m_1, m_2 \in \mathbb{Z}_n^* \) are defined as the plaintexts. \( r_1, r_2, r_3 < n \) are defined as the random integers for encryption process. The following additive homomorphic properties can be satisfied:

\[
\begin{align*}
E(m_1, r_1) \cdot E(m_2, r_2) \mod n^2 &= E(m_1 + m_2, r_3) \mod n, \\
E(m_1, r_1)^\mu \mod n^2 &= E(m_1 \mu, r_3) \mod n,
\end{align*}
\]

where \( \mu \in \mathbb{Z}_n^* \) holds. \( E(\cdot) \) denotes the encrypting operation.

The security of Paillier cryptosystem is based on the decisional composite residuosity assumption (DCRA) described, as follows:

**Definition 1** (Decisional Composite Residuosity Assumption (DCRA)). Define \( p \) and \( q \) as the two large primes with the condition \( n = pq \). Given \( \alpha \in \mathbb{Z}_n^* \), if there exist \( \gamma \in \mathbb{Z}_n^* \) satisfying \( \alpha \equiv \gamma^n \mod n^2 \), \( \alpha \) could be defined as the \( n \)-th residue modulo \( n^2 \). Note that, given the composite \( n \) and an integer \( \beta \), it is hard to decide whether \( \beta \) is the \( n \)-th residue modulo \( n^2 \).

**3.2. Elliptic Curve Cryptography (ECC)**

Define \( p > 3 \) as a large prime and \( \mathbb{F}_p \) as the finite field of order \( p \), where \( 4a^3 + 27b^2 \mod p = 0 \) and \( a, b \in \mathbb{F}_p \) [40]. In this case, \( E_p(a, b) \) is defined as the the elliptic curve over the finite field \( \mathbb{F}_p \), which has the following characteristic:

\[ y^2 = x^3 + ax + b \mod p, \]

where \( (x, y) \in \mathbb{F}_p \). The point doubling is defined as the unique addition operation on the curve \( E_p(a, b) \), only if the two points are identical. Otherwise, it is called the point addition. All of the points on \( E_p(a, b) \), as well as the point at infinity \( \infty \), construct an additive Abelian group \( E_p(\mathbb{F}_p) \), where \( \infty = (-\infty) \) is defined as the identity element.

**Definition 2** (Elliptic Curve Discrete Logarithm Problem (ECDLP)). Define \( P, Q \in \mathbb{G}_1 \), where \( Q = aP \). Hence, for any probabilistic polynomial-time (PPT) adversary \( \mathcal{A} \), the advantage in finding the integer \( a \in \mathbb{Z}_q^* \) to solve the ECDLP problem is defined as \( \text{Adv}^{\text{ECDLP}}_{\mathcal{A}, \mathbb{G}_1} \), which is negligible as the following equation:

\[
\text{Adv}^{\text{ECDLP}}_{\mathcal{A}, \mathbb{G}_1} = \Pr \left( \mathcal{A}(P, aP \in \mathbb{G}_1) \rightarrow a | \forall a \in \mathbb{Z}_q^* \right) \leq \varepsilon.
\]

**Definition 3** (Computational Diffie-Hellman Problem (CDHP)). Define \( \mathbb{G}_1 \) as the cyclic group with the large prime order \( q \). Given \( P, aP, bP \in \mathbb{G}_1 \) for \( a, b \in \mathbb{Z}_q^* \), where \( P \) is the generator of the cyclic group \( \mathbb{G}_1 \). Hence, for any probabilistic polynomial-time (PPT) adversary \( \mathcal{A} \), the advantage in finding computing \( abP \) for solving the given CDHP problem is defined as \( \text{Adv}^{\text{CDHP}}_{\mathcal{A}, \mathbb{G}_1} \), which is negligible as the following equation:

\[
\text{Adv}^{\text{CDHP}}_{\mathcal{A}, \mathbb{G}_1} = \Pr \left( \mathcal{A}(P, aP, bP \in \mathbb{G}_1) \rightarrow abP \in \mathbb{G}_1 | \forall a, b \in \mathbb{Z}_q^* \right) \leq \varepsilon.
\]

**3.3. Hash Function**

The one-way secure hash function \( h(\cdot) \) is constructed with the following properties [41]:

1. With a random message \( x \) of arbitrary length, the message digest of its fixed length output \( h(x) \) can be easily calculated.
2. It is hard to compute \( x = h^{-1}(y) \) with the given \( y \).
3. It is computationally infeasible to find \( x' = x \) such that \( h(x') = h(x) \), providing that \( x \) is given.
3.4. Notations

The notations used in our design are listed in Table 1, along with the corresponding description.

| Symbol          | Description                                      |
|-----------------|--------------------------------------------------|
| VC, \{RSU_1, \cdots, RSU_n\} | Vehicular Cloud, Road-Side Units |
| I^v, I^r, I^b | Vehicle Identities                                    |
| G_1         | Cyclic Group                                         |
| P             | Generator of G_1                                     |
| I^r, I^R     | RSU Identities                                       |
| \{\varphi_j, \xi_j\} | Vehicle Encryption Key Set                                |
| (\Gamma_j, \Theta_j) | Vehicle Decryption Key Set                            |
| \{\rho_i^R, s^R_i\} | RSU Partial Secret Key Set                            |
| (\sigma_j, h_j) | RSU Encryption Key Set                                |
| (\Lambda_i, k_i) | RSU Decryption Key Set                                |
| M_i, N_i, S_j, T_j | Large Prime Values                                   |
| \{k_j, \eta_j\} | Vehicle Partial Secret Key Set                       |
| \{\hat{h}_k\} | RSU Additional Information                           |
| \{h^T_1, \cdots, h^T_p\} | Route Records                                         |

3.5. System Model

In this section, the deployed cloud-assisted VANET infrastructure with healthcare monitoring function is briefly illustrated, which can be classified into four different communication layers, including the cloud layer, edge layer, vehicle layer, and WBAN layer. The four layers with the instructions are as follows. Meanwhile, Figure 1 shows the intuitive VANET system model.

Cloud layer is considered to be the centralized data facility responsible for all of the essential system operations. Crucial system operations such as master key issuance and user registration, are all conducted by the remote cloud layer, which is defined to be trustworthy at all time. Meanwhile, massive amount of vehicular information gathered from the terminal devices is analyzed and safely stored. Particularly, the distributed cloud servers are capable of managing multiple VANET prototypes, which promotes the construction of global Internet of Vehicles (IoV) initiatives. For better description, we consider the entire cloud layer as the VC.
Edge layer is defined as the combination of the RSU clusters, each of which is organized by direct and indirect wired connection between the nearby RSUs within predefined vicinity. Each RSU of the clusters is able to independently conduct the vehicular data interaction tasks with in-range vehicles, while the essential user information on participating devices could be shared within the cluster members. That is, collaborative computation and data processing operations for mutual authentication and message delivery could be achieved. For example, the existing cross-domain verification issue can be addressed with the applied distributive VANET edge layer, since the frequent and reliable RSU-to-RSU data exchange are assumed within RSU clusters. Practically, as for cloud-assisted VANET, low latency and high reliability characteristics of vehicle-to-RSU transmission could be satisfied with the deployed edge computing architecture (edge layer). In this case, the edge cluster involving neighboring RSUs collaboratively cache the frequently used vehicular data instead of requesting it from remote TA. The bandwidth burden of cloud server can be alleviated in this way.

Device layer refers to the terminal vehicles, where the heterogenous vehicular data and real-time road information are aggregated. Each vehicle is equipped with the embedded on-board unit (OBU) for vehicular data transmission and reception. Meanwhile, the deployed tamper-proof device (TPD) is used for confidential message preserving. Large amounts of temporary and high-speed V2V and V2R networks are continuously constructed, while complex computation cannot be carried out due to the resource limitation in vehicle side.

WBAN layer is defined as the integrated facilities for extensive medical data acquisition. VANETs with healthcare monitoring functionality can be constructed accordingly. In our assumption, all of the passengers in each vehicle are equipped with wearable device such as electronic bracelet or smart watch. The sensitive medical parameters regarding COVID-19 pandemic control can be measured and collected for subsequent test. The automotive interaction between wearable devices and the regarding vehicle is enabled, so that the pandemic factors, such as body temperature, could be remotely measured by VC. Non-contract surveillance towards passing vehicles can be conducted in this way.

3.6. Security Requirements

The design purpose of the proposed scheme is to improve the security properties in terms of VANET transmissions, and provide automotive healthcare monitoring for all passengers of transportation systems, so that the urgent COVID-19 pandemic control requirements can be satisfied. Consequently, the following major security characteristics for VANET security scheme are introduced.

- Conditional Privacy Preserving: considering as one of the crucial features for privacy protection, conditional privacy contains two aspects: user privacy protection and targeted vehicle information retrieving. That is, the confidential user information should be safely stored in the whole session. The illegal tracking toward specific vehicle cannot succeed. Meanwhile, the VC responsible for VANET system management should be able to reveal the real identity of suspect vehicle if necessary.
- Anonymity: due to the open wireless transmission features, VANET communication channels may be eavesdropped by malicious devices. Normally, messages that originated from the same device naturally carry unique data patterns. In this case, by analyzing the eavesdropped information, vital parameters, such as transmitting frequency, user location may be exposed, which severely endangers user privacy. For this consideration, the anonymity of each VANET device should be guaranteed.
- Unforgeability: in practical VANET transmission, adversary may selectively forge the valid certificates, session keys, or signatures to pass the verification process. Hence, unforgeability against chosen message attack is the major property in secure data exchange.
- Mutual Authentication: in the VANET design, mutual authentication is the fundamental but leading security property, which guarantees that both VANET entities in one communication
session could authenticate each other. In this way, the impersonation attack towards certain device can be prevented.

- **Non-repudiation**: non-repudiation ensures the validity of the transmitted information. The message sender of VANET cannot deny the authenticity of the issued signature on the transmitted messages.

- **Session Key Establishment**: upon mutual authentication, the unique session key between individual vehicle and VANET system should be established, so as to provide subsequent secure data exchange.

### 4. Proposed Design

In this section, the proposed homomorphic authentication scheme for practical VANETs is illustrated in detail. The automotive healthcare monitoring and detection strategies for all passengers of passing vehicles can be achieved. Sensitive personal medical data are locally validated and then uploaded to remote VC for further analysis and historical retrieving. Subsequently, the efficient infection tracking mechanism on suspected cases can be done, where the precise time-oriented travelling route of individual passenger could be retrieved. Therefore, the current practical healthcare monitoring requirements for COVID-19 pandemic control can be met. Intuitively, our design emphasizes the automotive authentication and medical data sharing in high-mobility VANET scenarios. The pairing-free certificateless cryptography is employed for key escrow resilience. User anonymity for all participating vehicles, as well as the involving passengers, are well preserved. Meanwhile, random identity updating design for various communication session is provided. Motivated by the blockchain design, the hash value for each vehicle is maintained by each RSU upon validation. Moreover, the successive RSUs could efficiently verify the correctness of the chain information by taking use of the data sharing characteristic of edge RSU clusters.

Generally, the proposed design is composed of three communicating phases: device initialization, blockchain-based key agreement, and healthcare monitoring strategy, where the workflow is shown in Figure 2. In device initialization phase, the essential vehicle, and RSU registration are preliminarily conducted. The confidential private data including the original vehicle identity and corresponding key are safely preserved in VC. Afterwards, the mutual authentication and key distribution process between requesting vehicle and RSU is carried out in the key agreement phase, where the new vehicle is allowed to join the VANET network after interaction with VC. The blockchain data regarding private driving records of each vehicle is updated by the RSU cluster. Finally, the healthcare monitoring strategy is presented, where the physical conditions of all involving passengers are timely surveilled and uploaded to the remote server in a secure way. Notably, the RSUs can be classified into the regular RSUs without healthcare monitoring duty, as well as the checkpoint RSU that is assigned as the checkpoint for pandemic control. Detailed introduction of all the three phases are respectively presented, as follows.
4.1. Device Initialization Phase

The device initialization phase is designed for system initialization and vehicle registration prior to authentication. Notably, the VC is defined as the validated and trustworthy entity during the whole communication session. Therefore, the crucial VANET system parameters and master key are issued and distributed by VC. Initially, VC define $G_1$ as the cyclic group generated by the large prime order $q$, where $P$ denotes the generator of the cyclic group. Additionally, the utilized one-way hash functions $H_1, H_2, H_3, H_4, H_5, h_1, h_2, h_3, h_4$ are, respectively, performed as

$$
\begin{align*}
H_1 & : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G_1 \rightarrow Z_q^* \\
H_2 & : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^* \\
H_3 & : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^* \\
H_4 & : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^* \\
H_5 & : G_1 \rightarrow Z_q^* \\
h_1 & : \{0,1\}^* \times \{0,1\}^* \times G_1 \rightarrow Z_q^* \\
h_2 & : \{0,1\}^* \times G_1 \rightarrow Z_q^* \\
h_3 & : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^* \\
h_4 & : \{0,1\}^* \rightarrow Z_q^*
\end{align*}
$$

In this case, the VANET system parameters set will be published in the form of $param = \{G_1, q, P, H_1, H_2, H_3, H_4, H_5, h_1, h_2, h_3, h_4\}$.

As for individual RSU, VC assigns the original identity $I_i^r \in \{0,1\}^*$ to each legitimate RSU during offline registration. The corresponded RSU secret key $s_i^r \in Z_q^*$ is randomly generated and distributed to RSU as well. Therefore, the confidential RSU identity set $\langle I_i^r, s_i^r \rangle$ is safely stored in both VC and RSU itself. Similarly, the initial registration process of vehicle should be conducted in advance. That is, the distinctive vehicle original identity $I_i^v \in \{0,1\}^*$ and the corresponded vehicle secret key $k_i \in Z_q^*$ are issued by VC during offline registration. The confidential vehicle identity set is defined as $\langle I_i^v, k_i \rangle$.

Note that the secure data exchange for RSU and vehicle initialization is assumed. At this point, VC maintains the records of all the registered RSUs and vehicles in its database. Notably, the private
vehicular information, such as user name, address, social security identifier, and phone number, are stored. Table 2 shows the data structure of the vehicular records in VC.

Table 2. Data Structure of Vehicular Records for Registered Entities.

| Type          | No. | Original Identity Set | Location | Name/Addr./SSN/Route Info. | Add. Info. |
|---------------|-----|-----------------------|----------|---------------------------|------------|
| RSU           | 1   | ⟨I_T , s_R 1⟩          | ○        | \                          | \          |
|               | 2   | ⟨I_T , s_R 2⟩          | ○        | \                          | \          |
|               | ... | ...                   | ...      | ...                        | ...        |
|               | i   | ⟨I_T , s_R i⟩          | ○        | \                          | \          |
| Vehicle       | 1   | ⟨I_V , k_1⟩            | \        | {h_1^p, h_2^p, ...}        | ⟨TS^p, ϕ⟩, ... |
|               | 2   | ⟨I_V , k_2⟩            | \        | {h_1^p, h_2^p, ...}        | ⟨TS^p, ϕ⟩, ... |
|               | ... | ...                   | ...      | ...                        | ...        |
| Passenger     | 1   | cid_1                 | \        | {ϕ}                        | \          |
|               | 2   | cid_2                 | \        | {ϕ}                        | \          |
|               | ... | ...                   | ...      | ...                        | ...        |
|               | n   | cid_n                 | \        | {ϕ}                        | \          |

With the purpose of illegal tracing prevention and privacy protection, the RSU anonymous identity is created by each legitimate RSU. That is, the registered RSU randomly generates its partial secret key e_R^i ∈ Z^n_q and periodically extracts the time-oriented anonymous identity I_R^i, as

$$I_R^i = h_1 (TS^i, I_T, e_R^i, s_R^i P),$$

where the above TS^i is referred to as the current timestamp, so that the freshness of identity can be assured. The session identity I_R^i is effective only within certain time period and will expire in the subsequent time. The RSU partial secret key set ⟨e_R^i, s_R^i⟩ is preserved in its storage, while e_R^i is kept secret to VC.

According to the confidential information, the homomorphic encryption infrastructure can be built for each registered RSU. Initially, RSU selects two large prime N_i and M_i, so that gcd (M_i, N_i, (M_i - 1) (N_i - 1)) = 1 holds. Subsequently, RSU randomly chooses h_i ∈ Z^*_{N_i}, so that ω_i = M_i N_i. Hence, the computation on Λ_i and k_i can be conducted according to

$$\begin{cases} \Lambda_i = \text{lcm} (M_i - 1, N_i - 1) \\ k_i = \ell_i (h_i^{\Lambda_i} \mod \omega_i^2) \mod \omega_i \end{cases},$$

where $\ell_i (x) = \frac{x - 1}{\omega_i}$. At this point, the RSU homomorphic encryption key set is extracted in the form of ⟨ω_i, h_i⟩. Afterwards, RSU carries out the following calculations:

$$\begin{cases} \mathcal{P}_i = e_R^i s_R^i P \\ \mathcal{Z}_R^i = H_1 (TS^i, I_R^i, \omega_i, h_i, \mathcal{P}_i) \end{cases},$$

where TS^i denotes the latest timestamp. Therefore, RSU broadcasts the parameters set ⟨TS^i, I_R^i, ω_i, h_i, ϕ_i, Z_R^i⟩ periodically to all devices within its range.
4.2. Blockchain-Based Key Agreement Phase

In this section, the authentication and key management for vehicle is introduced. Initially, while assuming the vehicle with \( \langle V, k_i \rangle \) is approaching the effective domain of the aforementioned RSU with anonymous identity \( I_j \), the vehicle itself generates the random partial secret key \( \varphi_j \in \mathbb{Z}_q^* \). In this case, the partial secret key set \( \langle k_j, \varphi_j \rangle \) is stored in vehicle side. For anonymity protection, the vehicle temporary identity is applied as

\[
I_j = h_2 \left( \ell_i, \varphi_j P \right).
\]

As mentioned above, vehicle is acknowledged of the broadcast RSU public information set \( \langle TS_1^i, I_j^1, h_i, \mathcal{R}_i, \mathcal{P}_i, \mathcal{Z}_i \rangle \). Firstly, freshness validation on the received timestamp \( TS_2^i \) is first performed by comparing whether \( |TS_2^i - TS_1^i| \leq \varepsilon_1 \) holds, where \( TS_2^i \) refers to the current timestamp. Subsequently, correctness of the certificate \( \mathcal{Z}_i \) is verified, so as to guarantee the message integrity. Upon verification, the RSU homomorphic encryption key pair \( \langle \vartheta_i, h_i \rangle \) can be extracted by vehicle. Meanwhile, similar homomorphic encryption design for vehicle can be constructed as well. That is, the vehicle with identity \( I_j \) selects two large prime \( \mathcal{P}_j \) and \( \mathcal{Q}_j \) so that \( \gcd (\mathcal{P}_j, \mathcal{Q}_j - 1) (\mathcal{Q}_j - 1) = 1 \) holds. Subsequently, vehicle randomly chooses \( \xi_j \in \mathbb{Z}_q^* \), where \( \mathcal{P}_j = \mathcal{P}_j \mathcal{Q}_j \). Hence, the computation on \( \mathcal{P}_j \) and \( \mathcal{Q}_j \) can be conducted according to

\[
\begin{align*}
\Gamma_j &= \text{lcm} (\mathcal{P}_j - 1, \mathcal{Q}_j - 1) \\
\Theta_j &= \phi_j \left( \xi_j^{\mathcal{P}_j} \mod \mathcal{P}_j \right) \mod \mathcal{Q}_j,
\end{align*}
\]

where \( \phi_j (y) = \frac{y - 1}{\mathcal{Q}_j} \). At this point, the vehicle homomorphic encryption key set is extracted in the form of \( \langle \mathcal{P}_j, \xi_j \rangle \).

Preliminarily, with the purpose of managing the historical driving information, the block chain is built in the form of \( \langle h_{\circ} (\cdot), h_{\circ} (TS_{1}^i, \xi_j, h_i, \mathcal{P}_j, \mathcal{Q}_j) , \ldots \rangle \), where \( h_{\circ} (\cdot) \) represents the previous hash value generated by the last encountered RSU. The entire block chain is distributively stored in \( \mathcal{P}_c \) while the vehicle itself stores its successive two hash values of the chain, which contains the authentication timestamp and the information of the last RSU, such as location and verification number. Notably, the vehicle does not preserve all of the chain data in storage for the consideration of inherent resource limitation, while the previous two hash values as well as the related timestamp \( TS_{2i-1}^i \) for signature are enough for further validation. For better description, the two stored hash values are simplified as \( h_{\circ} (\mathcal{P}_j - 1) \) and \( h_{\circ} (\mathcal{Q}_j - 1) \), which are generated by the previous RSU with identity \( I_{j-1} \) as

\[
h_{\circ} (\mathcal{P}_j - 1) = h_{\circ} (TS_{\ell-1}^i, \xi_{\circ}^{\mathcal{P}_j - 1}, h_{\circ} (\mathcal{P}_j - 2)).
\]

Upon extracting the RSU homomorphic encryption key pair \( \langle \vartheta_i, h_i \rangle \), the vehicle intends to construct the authentication process with RSU. Moreover, the previous blockchain data should also be validated and updated. Hence, the following calculations are conducted:

\[
\begin{align*}
Y_j &= \varphi_j^{\mathcal{P}_j} \\
K_j &= h_3 \left( TS_3^i, I_j^1, k_i \varphi_j P \right) \\
3_j &= h_3 \left( TS_3^i, I_j^1, k_i, I_j, K_j \right) \\
\mathcal{Z}_j &= \text{Enc}_{\langle \vartheta_i, h_i \rangle} \left( \left| \mathcal{P}_j \right| \left| \mathcal{Q}_j \right| \left| TS_{\ell-1}^i \right| h_{\circ} (\mathcal{P}_j - 1) \right) \left| 3_j \right| \\
\end{align*}
\]

where the homomorphic encryption \( \text{Enc}_{\langle \vartheta_i, h_i \rangle} [M] \) is performed as

\[
\text{Enc}_{\langle \vartheta_i, h_i \rangle} [M] = h_{\circ} (M) \cdot \varphi_j^{\mathcal{P}_j} \mod \mathcal{Q}_j^2.
\]
At this point, the vehicle requesting packet with its vehicle homomorphic encryption key set \( \langle \vartheta_j, \xi_j \rangle \) are issued as
\[
\langle \text{Request}, T S^j_{3}, I_{j}, Y_{j}, \Xi^j_{V} \rangle,
\]
where the blockchain information is also included.

Upon receipt of the requesting packet, freshness verification is conducted by checking whether \( |T S_{3}^{cur} - T S^j_{3}| \leq \varepsilon_2 \) holds, where \( T S_{3}^{cur} \) refers to the current timestamp. If validated, RSU is able to decrypt the received \( \Xi^j_{V} \) by computing
\[
\langle N_i || \vartheta_j, \xi_j || T S^j_{\ell - 1} , h^o_{\ell - 1} , h^o_{\ell - 2} || 3_i \rangle
\]
\[
= \text{Dec}^{k_i}_{i, \Lambda_i} \left[ \Xi^j_{V} \right]
\]
\[
= \ell_i \left( \left[ \Xi^j_{V} \right] \Lambda_i \mod \theta_i^2 \right) \mod \theta_i,
\]
where the RSU homomorphic decryption \( \text{Dec}^{k_i}_{i, \Lambda_i} \left[ C \right] \) is performed in the way of
\[
\text{Dec}^{k_i}_{i, \Lambda_i} \left[ C \right] = \frac{\ell_i \left( C \Lambda_i \mod \theta_i^2 \right)}{\ell_i} \mod \theta_i.
\]
The mathematical correctness for decryption can be illustrated as
\[
\text{Dec}^{k_i}_{i, \Lambda_i} \left[ \text{Enc}^{o_j}_{i, \lambda_i} \left[ M \right] \right]
\]
\[
= \ell_i \left( \left[ \text{Enc}^{o_j}_{i, \lambda_i} \left[ M \right] \right] \Lambda_i \mod \theta_i^2 \right) \mod \theta_i
\]
\[
= \ell_i \left( h^o_{\lambda_i} \mod \theta_i^2 \right) \mod \theta_i
\]
\[
= M \mod \theta_i.
\]

Hence, \( \langle N_i || \vartheta_j, \xi_j || T S^j_{\ell - 1} , h^o_{\ell - 1} , h^o_{\ell - 2} || 3_i \rangle \) is successfully extracted from \( \Xi^j_{V} \) by RSU. The message confidentiality can be guaranteed by verifying \( 3_i \) with the acquired \( N_i \) and the previously broadcast \( \vartheta^o \) from RSU. If validated, RSU stores the vehicle homomorphic encryption key set \( \langle \vartheta_j, \xi_j \rangle \).

Moreover, the extensive validation procedure on blockchain should be carried out. In our assumption, upon successful authentication with certain RSU, vehicle will request RSU to verify and update its current blockchain values \( \langle T S^j_{\ell - 1} , h^o_{\ell - 1} , h^o_{\ell - 2} \rangle \). Dynamic information sharing among nearby RSUs is enabled, according to the aforementioned cloud-assisted VANET system model with edge RSU cluster. That is, the identity information \( \diamond^j_{\ell - 1} \) of the previous RSU will be broadcast in the way of \( \text{RSU}_{\ell - 1} \rightarrow \text{RSU}_j \). Hence, with the received \( \diamond^j_{\ell - 1} \) from RSU cluster, and the current blockchain \( \langle T S^j_{\ell - 1} , h^o_{\ell - 1} , h^o_{\ell - 2} \rangle \) from vehicle, RSU checks \( h^o_{\ell - 2} \neq h^o_{\ell - 1} \) so as to confirm the correctness of chain value. Subsequently, RSU computes \( h^o_{\ell} \) according to
\[
h^o_{\ell} = h^o_{\ell - 1} \cdot \diamond^j_{\ell - 1} \text{ mod } \theta_i^2
\]
where the \( T S^j_{\ell} \) denotes the current timestamp, and \( \diamond^j_{\ell} \) is the identity information of current RSU. Meanwhile, with the extracted \( \vartheta^o = o^j_{s_i} s^o_{\ell} \) and \( Y^j_{t} = o_{j} \vartheta^o \), RSU conducts the following calculation on \( \Psi^j_{t} \) as
\[
\Psi_j = \left( e_R^j s_R^j \right)^{-1} Y_j \\
= e_j \left( e_R^j s_R^j \right)^{-1} \mathcal{A}^j \\
= e_j \left( e_R^j s_R^j \right)^{-1} \left( e_R^j s_R^j \right) P \\
= e_j P
\] (15)

At this point, RSU uploads \(\langle TS^i_4, I_j, \Psi_j, \mathcal{A}^j, TS^\circ_4, \mathcal{O}^i_4 \rangle\) to VC for the cloud verification. Notably, the vehicle identity information \(\langle I_j, k_j \rangle\) are stored in VC server. Therefore, VC is able to confirm the vehicle identity \(I^j_V\) with the transmitted \(\langle TS^i_4, I_j, \Psi_j, \mathcal{A}^j, TS^\circ_4, \mathcal{O}^i_4 \rangle\) from RSU. If matches, the requesting vehicle is the legitimate registered device. The vehicle access to VANET system will be granted. As for chain value updating, VC refreshes the stored blockchain values with the uploaded \(\langle TS^\circ_4, \mathcal{O}^i_4 \rangle\) of RSU as well. Hence, the record \(\langle h^4_0, \cdots, h^4_{i-1}, h^4_i \rangle\) is updated. The \(\langle TS^\circ_4, \mathcal{O}^i_4 \rangle\) information is securely preserved as additional contents for further vehicle tracking. In our assumption, every time that the vehicle communicates with a new RSU, VC will receive confirmation message along with the crucial contents \(\langle TS^\circ_4, \mathcal{O}^i_4 \rangle\) for chain updating. With all acquired information, VC is able to synchronize the decentralized blockchain values with vehicle itself, where the chain updating for vehicle is performed by the involved RSU.

Subsequently, VC distributes the acknowledgement message \(\langle \text{Ack}, I_j, \delta_j \rangle\) to RSU, where

\[
\delta_j = h_2 \left( I_j, k_j, e_j P \right).
\] (16)

Upon receiving the acknowledgement, the vehicle identity can be updated as

\[
I^j_\text{new} = h_2 \left( I_j, e_R^j s_R^j P \right),
\] (17)

which includes the RSU partial key set \(\langle e_R^j, s_R^j \rangle\). In our design, the anonymous vehicle identity is safely updated as soon as the successful that verifies session is conducted. In this case, the message unlinkability for various communication sessions, and untraceability for specific vehicle, can be achieved.

Next, RSU is able to deliver the essential information \(\langle \delta_j, TS^\circ_4, h^\circ_{i-1}, h^\circ_i \rangle\) to vehicle following the vehicle homomorphic encryption process with the previous vehicle key set \(\langle \mathcal{A}_j, \zeta_j \rangle\) and its own \(e_R^j\) as

\[
\begin{aligned}
\Xi_j^i &= \text{Enc}^e_{e_R^j} \left( \mathcal{A}_j \right) \left[ \delta_j || TS^\circ_4 || h^\circ_{i-1} || h^\circ_i \right] \\
\Phi_j &= H_4 \left( TS^i_4, I_j, \Xi_j^i \right).
\end{aligned}
\] (18)

Note that the homomorphic encryption \(\text{Enc}^e_{e_R^j} \left( \mathcal{A}_j \right) \left[ M \right]\) can be performed as

\[
\text{Enc}^e_{e_R^j} \left( \mathcal{A}_j \right) \left[ M \right] = e_j^M \cdot e_R^j \mod \mathcal{A}_j^2.
\] (19)

Hence, the packet \(\langle TS^i_4, I_j, \Xi_j^i, \Phi_j \rangle\) is then delivered to the destined vehicle.

Upon receiving \(\langle TS^i_4, I_j, \Xi_j^i, \Phi_j \rangle\), freshness confirmation is first carried out by checking whether \(| TS_{\text{cur}}^i - TS^i_4 | \leq \epsilon_3 \) holds, where \(TS_{\text{cur}}^i\) refers to the current timestamp. Subsequently, the received \(\Xi_j^i\) can be decrypted as
where the vehicle homomorphic decryption $\text{Dec}^{\Theta_j}_{\langle\mathcal{D},\Gamma\rangle}[C]$ is performed, as

$$\text{Dec}^{\Theta_j}_{\langle\mathcal{D},\Gamma\rangle}[C] = \frac{\phi_j\left((C^j \mod D_j^2)\right)}{\Theta_j} \mod D_j.$$  \hspace{1cm} (21)

Note that the mathematical correctness for the vehicle homomorphic decryption can be briefly illustrated as

$$\text{Dec}^{\Theta_j}_{\langle\mathcal{D},\Gamma\rangle}\left[\text{Enc}^{\Theta_j}_{\langle\mathcal{D},\delta_j\rangle}\left[\text{Enc}^{\Theta_j}_{\langle\mathcal{D},\delta_j\rangle}[M]\right]\right] = \frac{\phi_j\left((C^j \mod D_j^2)\right)}{\Theta_j} \mod D_j.$$  \hspace{1cm} (22)

At this point, $\delta_j$ can be successfully extracted from $\Xi^j_{\mathbb{R}}$. Confidentiality of the delivered packet can be confirmed by checking $\Phi_j$. If validated, the vehicle conducts the final authentication, as $\delta_j = h_2(\ell^{j},k_j,p_j)$.

At this point, mutual authentication between RSU and requesting vehicle is completed. In our design, the semi-trusted RSUs can perform the authentication and updating procedures without accessing the confidential vehicle secrets. Meanwhile, $s_{k,j} = H_5(k_j,\rho_j,p_j)$ is used as the shared session key established between remote VC and participating vehicle. In this case, the constructed homomorphic cryptographic scheme of $\left[\text{Enc}^{\Theta_j}_{\langle\mathcal{D},\lambda_j\rangle},\text{Dec}^{\Theta_j}_{\langle\mathcal{D},\Gamma\rangle}\right]$ and $\left[\text{Enc}^{\Theta_j}_{\langle\mathcal{D},\delta_j\rangle},\text{Dec}^{\Theta_j}_{\langle\mathcal{D},\Gamma\rangle}\right]$ could guarantee secure and reliable data exchange. Moreover, the vehicle could also extract the updated blockchain values $\langle h^s_{\ell-1}, h^s_{\ell} \rangle$ and related timestamp $TS^s_{\ell}$ from $\Xi^s_{\mathbb{R}}$. Hence, the previous value $\langle TS^{s}_{\ell-1}, h^{s}_{\ell-1}, h^{s}_{\ell-2} \rangle$ can be replaced with the updated $\langle TS^{s}_{\ell}, h^{s}_{\ell-1}, h^{s}_{\ell-2} \rangle$. In the next authentication session with successive RSU, the newly generated $\langle TS^{s}_{\ell+1}, h^{s}_{\ell}, h^{s}_{\ell+1} \rangle$ will be issued in the same way. The blockchain record $\langle h^{s}_{\ell}, \cdots, h^{s}_{\ell-1}, h^{s}_{\ell-2}, h^{s}_{\ell-3} \rangle$ is maintained by VC and vehicle itself, while the validation processes on successive values of the chain are operated by all of the involved RSUs. With the precise signing information $\langle TS^{s}_{\ell-1}, h^{s}_{\ell-1}, h^{s}_{\ell-2} \rangle$ of the encountered RSU on the road, the driving routes of particular vehicle could be securely recorded in a decentralized way. All of these strategies enable the following healthcare monitoring and infection tracking design.

4.3. Healthcare Monitoring Strategy

With the preliminary operations introduced in the previous two phases, the healthcare monitoring strategy can be achieved, along with the infection tracking algorithm for COVID-19 pandemic control. The RSUs can be classified into regular RSUs and the checkpoint RSU, as shown in Figure 2. Regular RSU is in charge of vehicular data exchange of conventional VANETs, while the checkpoint RSUs take the responsibility of traffic surveillance and healthcare monitoring particularly.
As for practical scenarios of pandemic control in transportation system, all of the regular RSUs can be practical as the checkpoint if necessary. Extensive modification on RSU hardware is not required, thus any regular RSUs can switch to checkpoint RSU easily. Therefore, effective and reliable healthcare monitoring functionality could be provided to any road sections under emergency situations. Intuitively, the above key management and mutual authentication operations are illustrated in terms of regular RSU, while the healthcare monitoring strategy in this section will be described with the assistance of checkpoint RSU. That is, real-time physical status of the passengers in the passing vehicles are monitored, collected, and uploaded to VC at final. Additionally, the driving route information on vehicles will be attached to wearable device of individual passenger. Hence, infection tracking towards suspected persons is available.

We assume that the aforementioned vehicle is approaching the checkpoint RSU in the next (RSU \(_i \rightarrow\) RSU \(_{i+1}\)). At this point, the vehicle possesses the essential chain values \(<TS_i, h^\theta_{i+1}, h^\phi_i\>) sent by the previous RSU. The blockchain-based key agreement phase is the same as above until the generation of packet \(<TS_i, I_j, \Xi^j, \Phi_j\>). In the assumption of checkpoint RSU, a simple request is attached to the packet and then sent to destined vehicle in the form of \(\langle\text{Request}, TS_i, I_j, \Xi^j, \Phi_j\rangle\). After validation, the vehicle is then aware of the request for healthcare monitoring towards its passengers.

In our assumption, the passengers in vehicles are considered to be the essential parties for healthcare monitoring in VANETs. Preliminarily, each passenger should register to VC in advance. Hence, the confidential identities set of the registered passengers are issued as \{cid_1, ..., cid_n\}, where the distributed cid is the unique original identity. The identity set \{cid_1, ..., cid_n\} for all the legitimate passengers is safely stored in VC server. As for individual passenger, the wearable device, such as smart watch or smart bracelet, is mandatory for medical data measurement and aggregation. Moreover, with the assistance of the intra body area network (intra-BAN) and the connected medical sensors, precise and seamlessly physical data collection can be provided. Notably, each passenger and their corresponded wearable device is assumed to be the same entity with identity cid.

As mentioned above, in the range of the checkpoint RSU \(_{i+1}\), the parameters set \(<TS_{i+1}, I_{i+1}, \Theta_{i+1}, h_{i+1}, \Sigma^i_{i+1}\>) is periodically to all devices. Importantly, all of the wearable devices could also acquire the RSU parameters set. Hence, with the same validation and decryption process, the RSU homomorphic encryption key set \(\langle\Theta_i, h_i\rangle\) is then acquired by passenger with cid_i, provided that there are n passengers within one vehicle. Note that, for the n devices, the temporary identity tid_i is generated as \(tid_i = h(cid_i, TS_i^\theta)\). Hence, each wearable device delivers the sensitive medical data regarding pandemic control to vehicle in the form of \(\text{Enc}^{cid_i}_{\langle\Theta_i, h_i\rangle}[\text{tid}_i, \text{data}]\). The vehicle then gathers all n packets from different passengers and forwards it to RSU in the form of

\[
\text{Enc}^{\theta}_{\langle\Theta, h\rangle}[\text{Enc}^{\text{cid}_1}_{\langle\Theta, h\rangle}[\text{tid}_1, \text{data}], ..., \text{Enc}^{\text{cid}_n}_{\langle\Theta, h\rangle}[\text{tid}_n, \text{data}]].
\]

RSU can then decrypt the identities tid_i and medical data from the passengers. If unique patterns are detected, then RSU sends the warning report to VC and request for retransmission. Eventually, the gathered healthcare data, along with the current RSU information \(\Theta^i_{i+1}\), are upload to VC and stored for further usage. In the further time, if certain passenger is infected, its historical healthcare record and route information can be retrieved in the VC database, the infection tracking method is accordingly available, which is of great significance for pandemic control.

5. Security Analysis

In this section, the major security characteristics of the proposed design are discussed, respectively. Moreover, comparisons with the existing methods in terms of the VANET authentication and key management are presented.
5.1. Security Discussions

**Theorem 1.** The authentication process is proven to be correct if and only if the certificates are successfully issued following the device registration and authentication strategy.

**Proof of Theorem 1.** Initially, the specific vehicle with \( \{I_{V_i}, k_J\} \) approaches the regular RSU with original identity set \( \{I_{L_i}, s_R^1\} \). RSU itself issues the public parameter set \( \langle TS_{2}^1, I_{R}, \sigma_1, h_1, \rho_1, \Xi_1^1 \rangle \), where

\[
\begin{aligned}
I_{R}^1 &= h_1 \left( TS_{1}^1, I_{R}, \sigma_1, s_R^1 P \right) \\
\Lambda_1 &= \text{lcm} \left( \lambda_i - 1, \lambda_j - 1 \right) \\
\rho_1 &= \sigma_1^1 s_R^1 P \\
\Xi_1^1 &= H_1 \left( TS_{2}^1, I_{R}, \sigma_1, h_1, \rho_1 \right)
\end{aligned}
\]

(24)

With the assigned vehicle homomorphic encryption mechanism \( \text{Enc}^{\rho_1}_{\left(I_{V_i}, k_J\right)} \left[ M \right] = h_1^{M} \cdot e_1^{\rho_1 \text{mod} \rho_2} \), \( \langle \text{Request}, TS_{V_i}^1, I_{V_i}, Y_{V_i}, \Xi_{V_i} \rangle \) can be generated by vehicle in the form of \( \Xi_{V_i} = \text{Enc}^{\rho_1}_{\left(I_{V_i}, k_J\right)} \left[ N \right] \). At this point, the blockchain has not been generated, since it is in the first RSU range. Upon receiving the confirmation message from remote VC, RSU computes \( h_1^o = h_1^o \left( TS_{1}^o, \rho_1 \right) \), where \( TS_{1}^o \) denotes the current timestamp, and \( \rho_1 \) is the identity information of current RSU. Note that the crucial contents \( \langle TS_{1}^o, \rho_1 \rangle \) is uploaded to VC for chain updating. Only with the delivered acknowledgement message \( \langle \text{Ack}, I_{V_i}, \delta_j \rangle \) from VC, the RSU is able to legitimately pass the verification process \( \delta_j \equiv h_2 \left( I_{V_i}, k_J, \rho_1 \right) \) in vehicle side. Similarly, in the next authentication session of second RSU with \( \langle I_{V_i}, s_R^2 \rangle \), the VC hash chain is updated as \( \langle h_1^o, h_2^o \rangle \), where \( h_2^o = h_1^o \left( TS_{2}^o, \rho_2 \right) \). Following this way, in the \( I \) session, RSU is able to deliver the essential information \( \langle \delta_j, TS_{V_i}^o, h_{i-1}^o, h_i^o \rangle \) to vehicle following the vehicle homomorphic encryption process. Note that \( \delta_j \equiv h_2 \left( I_{V_i}, k_J, \rho_1 \right) \) holds, Assuming the length of partial secrets \( (k_j, \rho) \) is \( t \), respectively. Hence, the probability to successfully pass the validation process is \( \frac{1}{t} \). The correctness of our design can be proven.

**Theorem 2.** Message unlinkability within various RSUs effective range can be achieved. Moreover, dynamic chain updating is performed upon each successful validation.

**Proof of Theorem 2.** Assuming specific vehicle with route \( \text{RSU}_1 \rightarrow \text{RSU}_n \) is in the \( i \)-th RSU domain \( i \in [1, n] \), the vehicle with \( \langle I_{V_i}, k_J \rangle \) utilizes the temporary identity \( I_{L_i} = h_2 \left( I_{V_i}, k_J, P \right) \), where the random partial secret key is adopted. Note that the temporary identity varies for different sessions. Furthermore, upon receiving the acknowledgement at final step, the vehicle identity can be updated as \( I_{R}^1 = h_2 \left( I_{V_i}, k_J, P \right) \). The delivered packet from RSU is \( \langle TS_{V_i}^1, I_{V_i}, \Xi_{R}, \Phi_1 \rangle \). That is, dynamic vehicle identities are used in the same authentication session, which significantly prevents information eavesdropping and tracing. Unlinkability on the confidential vehicular data during transmission can be provided as well. Additionally, the vehicle does not preserve all of the chain data in storage for the consideration of inherent resource limitation, while the previous chain values denoted as \( h_{i-2}^o \) and \( h_{i-1}^o \) are stored for chain validation and updating. Note that the previous RSU calculates \( h_{i-1}^o = h_1^o \left( TS_{i-1}^o, \rho_{i-1}^o \right) \). With the constructed homomorphic encryption strategy, the chain values can be managed by each encountered RSU in a decentralized way. Specifically, the vehicle and each RSU share the two successive chain values, while VC preserves the integrated blockchain for further usage.

**Theorem 3.** Conditional identity privacy preservation for vehicle and RSUs is achieved. Untraceability towards specific vehicle is guaranteed, while the remote VC is capable of retrieving the real identity of certain vehicle under extreme situations.
Proof of Theorem 3. In the device initialization phase, the registered RSU randomly generates its partial secret key \( e_R^h \in \mathbb{Z}_q^* \) and periodically extracts the time-oriented anonymous identity \( I_R^i \) as \( I_R^i = h_1(\langle TS_1^i, I_R^i, e_R^h, P \rangle) \), where the random partial secret key set \( \langle e_R^h, e_R^0 \rangle \), along with the current timestamp \( TS_1^i \) is applied. Similarly, for anonymity protection, the vehicle temporary identity is applied as \( I_V = h_2(\langle I_V, e_V^j, P \rangle) \) and \( I_V^j = h_2(\langle I_V^j, e_V^{j^2}, P \rangle) \). Note that the distinctive identity \( I_V \in \{0,1\}^* \) and \( I_V^j \in \{0,1\}^* \) remain hidden all of the time. Each \( I_R^i \) is only effective within a certain time period and will expire periodically. In this way, anonymous identities for both RSUs and vehicles are provided. Privacy preservation property is provided in this way. Meanwhile, the entire block chain regarding driving route and real identity is safely stored in \( \text{VC} \). Therefore, \( \text{VC} \) is able to reveal the original identity of all RSUs or vehicles, which is crucial for detecting and revoking the compromised VANET entities. Accordingly, conditional identity privacy preserving is provided.

\[ \square \]

Theorem 4. Replay attacking resistance is provided during the whole authentication process. Reusage of the previous information from past authentication sessions cannot pass the current validation.

Proof of Theorem 4. In the device initialization phase and key agreement phase, the fresh timestamps are widely used in each calculation. Meanwhile, the certificates with all transmitted elements are presented so as to guarantee data integrity. As mentioned above, the RSU public information set is broadcast in the form of \( \langle TS_2^i, I_R^i, e_R^h, P, \mathcal{R}_i, \mathcal{Z}_i^j \rangle \), where the latest time stamp is included. In the subsequent authentication session, the vehicle calculates the certificate \( \mathcal{Z}_V = \text{Enc}_{(e_V^j, P)}[N_j||\mathcal{Z}_V^j||\mathcal{Z}_V^j] \) according to the intermediate values \( \langle N_j, \mathcal{Z}_j \rangle \), which is related to the timestamp \( TS_2^j \). In this case, provided that, in specific moment \( T_{\text{off}} \), the adversary \( \mathcal{A}_1 \) is able to collect \( z \) transmitted packets \( \langle \text{Request}, TS_2^i, I_i, Y_i, \mathcal{Z}_V^j \rangle_{i \in \mathbb{I}} \) during certain time interval \( [T_{\mathcal{R}}, T_{\mathcal{Z}}] \) \( (T_{\mathcal{R}} < T_{\text{off}}) \). Intuitively, the probability for \( \mathcal{Z}_V^j \) to pass the verification is \( \frac{1}{2^z} \), where the length of output \( \mathcal{Z}_V^j \) is assumed to be \( t \). Therefore, our design has proved to be resistant to replay attack.

\[ \square \]

Theorem 5. Certificateless authentication design is deployed in the proposed authentication session. No-repudiation characteristic is provided for vehicles.

Proof of Theorem 5. In the aforementioned device initialization phase, the original identity for vehicle is assigned as \( I_V^j \), while the assigned secret key \( k_j \) is safely shared among \( \text{VC} \) and vehicle. Meanwhile, the vehicle itself randomly generates the partial key \( e_j \in \mathbb{Z}_q^* \) and keeps it secret to \( \text{VC} \). Therefore, with the characteristics of ECDLP, it is difficult to extract \( e_j \) from the published \( I_V = h_2(\langle I_V, e_V^j, P \rangle) \) or \( Y_j = e_jP \). The impersonation towards specific vehicle cannot be accepted by the receiver. Similarly, the RSU partial secret key \( e_R^0 \in \mathbb{Z}_q^* \) is randomly generated by RSU and kept hidden to \( \text{VC} \). Therefore, \( \text{VC} \) does not have full control over the participating vehicles and RSUs. Hence, the certificateless authentication property is provided.

\[ \square \]

5.2. Security Properties Comparison

In this section, the security properties comparison with existing VANETs secure communication is presented. The proposed protocol is compared with the state-of-the-art authentication and key management methods: AKMB [42], IBCPA [7], and EPCBV [43] in order to demonstrate its superiority on security properties. The comparison results presented in Table 3 show that the proposed scheme could meet the desirable security requirements that are introduced in Section 3.6.
### Table 3. Comparison Results on Security Properties.

| Scheme                                | AKMB [42] | IBCPA [7] | EPCBV [43] | The Proposed Scheme |
|---------------------------------------|-----------|-----------|------------|--------------------|
| Anonymous Identity Updating           | ×         | ×         | ×          | ○                  |
| Unforgeability                        | ○         | ○         | ○          | ○                  |
| Collusion Attack Resilience           | ○         | ×         | ○          | ○                  |
| Sibling Attack Resilience             | ○         | ×         | ×          | ○                  |
| Session Key Establishment             | ○         | ○         | ○          | ○                  |
| Conditional Privacy Preserving        | ○         | ○         | ○          | ○                  |
| Scalability                           | ×         | ×         | ○          | ○                  |
| Key Escrow Resilience                 | ○         | ○         | ○          | ○                  |
| Replay Attack Resistance              | ×         | ○         | ○          | ○                  |
| Unlinkability                         | ×         | ×         | ×          | ○                  |

6. Performance Analysis

In this section, the performance of the proposed scheme is discussed, which specifically emphasizes on the crucial properties for resource-limited VANETs environment, such as storage overhead and computation cost.

6.1. Storage Overhead

In practical environment, the VANET entities, including vehicles and RSUs, are the fundamental units in V2V and V2R wireless communication. Due to the resource restriction, the storage overhead required for the authentication process should be optimized. The state-of-the-art VANETs authentication schemes, including AKMB [42], IBCPA [7], and EPCBV [43] are also analyzed. Hence, the advantages of our scheme on storage overhead can be demonstrated as shown in Figure 3, where the storage cost for individual RSU is presented. Obviously, less storage overhead is required in the proposed scheme.
6.2. Computation Cost

In this section, the computation cost of the proposed design is analyzed. The time consumption for authentication in RSU side is discussed in terms of the number of participating vehicles. Note that the complex pairing calculations are not adopted in our design. The comparison results with AKMB [42], IBCPA [7], and EPCBV [43] are presented in Figure 4. Intuitively, less time consumption is required for authenticating process with resource limited vehicles, which proves the performance advantages of our design.

![Computation Comparison (RSU)](image)

**Figure 4.** Comparison Results of Computation Cost.

7. Conclusions

In this paper, emphasizing automotive pandemic control in intelligent transportation system, a practical homomorphic authentication method for healthcare monitoring in cloud-assisted VANETs is developed. In the proposed scheme, medical surveillance and infection tracking towards suspected passengers can be achieved. Our design applies the novel cloud infrastructure with the hybrid medical data acquisition module. Non-contract surveillance towards random vehicles can be remotely conducted by vehicular cloud. Moreover, the decentralized blockchain-based route recording mechanism is enabled, where the accurate and timely route information for each involved vehicle can be securely uploaded and analyzed in VC. The chain updating operations are collaboratively conducted by several decentralized RSU edge entities at a time, so that vehicular data confidentiality is guaranteed. Analysis on the featured security properties and comparison with other schemes prove that our design can meet the practical security requirements. Meanwhile, performance analysis with other studies show its efficiency. With these unique advantages, the proposed design can be utilized for the current COVID-19 pandemic control.

**Author Contributions:** Conceptualization, H.T. and I.C.; Methodology, H.T.; Formal analysis, H.T.; Investigation, P.K.; Writing—Original Draft Preparation, H.T.; Writing—Review and Editing, H.T. and I.C.; Supervision, I.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2020R1A2C2007091).

**Conflicts of Interest:** The authors declare no conflict of interest.
References

1. Zhang, L.; Wu, Q.; Solanas, A.; Domingo-Ferrer, J. A Scalable Robust Authentication Protocol for Secure Vehicular Communications. *IEEE Trans. Veh. Technol.* 2010, 59, 1606–1617. [CrossRef]

2. Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019; pp. 1–6.

3. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* 2011, 12, 736–746. [CrossRef]

4. Yao, Y.; Chang, X.; Mišić, J.; Mišić, V.B.; Li, L. BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services. *IEEE Internet Things J.* 2019, 6, 3775–3784. [CrossRef]

5. Tan, H.; Chung, I. Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. *IEEE Access* 2019, 7, 151459–151474. [CrossRef]

6. Li, J.; Lu, H.; Guizani, M. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. *IEEE Trans. Parallel Distrib. Syst.* 2015, 26, 938–948. [CrossRef]

7. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* 2015, 10, 2681–2691. [CrossRef]

8. Lo, N.; Tsai, J. An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings. *IEEE Trans. Intell. Transp. Syst.* 2016, 17, 1319–1328. [CrossRef]

9. Lu, R.; Lin, X.; Liang, X.; Shen, X. A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs. *IEEE Trans. Intell. Transp. Syst.* 2012, 13, 127–139. [CrossRef]

10. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs. *Wirel. Commun. Mob. Comput.* 2018, 2018, 1–13. [CrossRef]

11. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* 2016, 65, 1711–1720. [CrossRef]

12. Zhang, Q.; Gan, Y.; Zhang, Q.; Wang, R.; Tan, Y. A Dynamic and Cross-Domain Authentication Asymmetric Group Key Agreement in Telemedicine Application. *IEEE Access* 2018, 6, 24064–24074.

13. Tian, Z.; Shi, W.; Wang, Y.; Zhu, C.; Du, X.; Su, S.; Sun, Y.; Guizani, N. Real-Time Lateral Movement Detection Based on Evidence Reasoning Network for Edge Computing Environment. *IEEE Trans. Ind. Inform.* 2019, 15, 4285–4294. [CrossRef]

14. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection. *J. Internet Technol.* 2018, 19, 481–488.

15. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. Efficient Conditional Anonymity With Message Integrity and Authentication in a Vehicular Ad-Hoc Network. *IEEE Access* 2019, 7, 71424–71435. [CrossRef]

16. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A Distributed Key Management Framework with Cooperative Message Authentication in VANETs. *IEEE J. Sel. Areas Commun.* 2011, 29, 616–629. [CrossRef]

17. Wasef, A.; Shen, X. EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Mob. Comput.* 2013, 12, 78–89. [CrossRef]

18. Tan, H.; Chung, I. A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs. *Sensors* 2018, 18, 3930. [CrossRef]

19. He, D.; Kumar, N.; Wang, H.; Wang, L.; Choo, K.R.; Vinel, A. A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network. *IEEE Trans. Dependable Secur. Comput.* 2018, 15, 633–645. [CrossRef]

20. Chuang, M.; Lee, J. TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks. *IEEE Syst. J.* 2014, 8, 749–758. [CrossRef]

21. Zhu, X.; Jiang, S.; Wang, L.; Li, H. Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* 2014, 63, 907–919. [CrossRef]

22. Shen, J.; Tan, H.; Ren, Y.; Liu, Q.; Wang, B. A Practical RFID Grouping Authentication Protocol in Multiple-Tag Arrangement With Adequate Security Assurance. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 31 January–3 February 2016; pp. 693–699.
23. Tan, H.; Chung, I. A Secure Cloud-Assisted Certificateless Group Authentication Scheme for VANETs in Big Data Environment. In Proceedings of the 2019 International Conference on Big Data Engineering (BDE2019), Hong Kong, China, 11–13 June 2019; pp. 107–113.

24. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. *IEEE Trans. Veh. Technol.* 2016, 65, 896–911. [CrossRef]

25. Tan, H.; Song, Y.; Xuan, S.; Pan, S.; Chung, I. Secure D2D Group Authentication Employing Smartphone Sensor Behavior Analysis. *Symmetry* 2018, 11, 969. [CrossRef]

26. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Trans. Ind. Inform.* 2020, 16, 4146–4155. [CrossRef]

27. Zhou, T.; Shen, J.; Li, X.; Wang, C.; Tan, H. Logarithmic Encryption Scheme for Cyber-Physical Systems Employing Fibonacci Q-matrix. *Future Gener. Comput. Syst.* 2020, 108, 1307–1313. [CrossRef]

28. Tan, H.; Xuan, S.; Chung, I. HCDA: Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs. *Symmetry* 2020, 12, 1003. [CrossRef]

29. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* 2019, 27, 2792–2801. [CrossRef]

30. Li, Y.; Chen, W.; Cai, Z.; Fang, Y. CAKA: A Novel Certificateless-Based Cross-Domain Authenticated Key Agreement Protocol for Wireless Mesh Networks. *Wirel. Netw.* 2016, 22, 2523–2535. [CrossRef]

31. Liu, B.; Jia, D.; Wang, J.; Lu, K.; Wu, L. Cloud-Assisted Safety Message Dissemination in VANET–Cellular Heterogeneous Wireless Network. *IEEE Syst. J.* 2017, 11, 128–139. [CrossRef]

32. Tan, H.; Gui, Z.; Chung, I. A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs. *IEEE Access* 2018, 6, 74260–74276. [CrossRef]

33. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* 2019, 14, 1779–1790. [CrossRef]

34. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* 2019, 20, 1621–1632. [CrossRef]

35. Ma, M.; He, D.; Wang, H.; Kumar, N.; Choo, K.R. An Efficient and Provably SecureAuthenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. *IEEE Internet Things J.* 2019, 6, 8065–8075. [CrossRef]

36. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. Comments on ‘Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks’. *IEEE Trans. Intell. Transp. Syst.* 2017, 19, 2149–2151. [CrossRef]

37. Lin, C.; Deng, D.; Yao, C. Resource Allocation in Vehicular Cloud Computing Systems With Heterogeneous Vehicles and Roadside Units. *IEEE Internet Things J.* 2018, 5, 3692–3700. [CrossRef]

38. Ullah, A.; Yaqoob, S.; Imran, M.; Ning, H. Emergency Message Dissemination Schemes Based on Congestion Avoidance in VANET and Vehicular FoG Computing. *IEEE Access* 2019, 7, 1570–1585. [CrossRef]

39. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology—EUROCRYPT ’99*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.

40. Smart, N.P. The Discrete Logarithm Problem on Elliptic Curves of Trace One. *J. Cryptol.* 1999, 12, 193–196. [CrossRef]

41. Merkle, R.C. A Fast Software One-way Hash Function. *J. Cryptol.* 1990, 3, 43–58. [CrossRef]

42. Tan, H.; Chung, I. Secure Authentication and Key Management With Blockchain in VANETs. *IEEE Access* 2020, 8, 2482–2498. [CrossRef]

43. Gayathri, N.B.; Thumbur, G.; Reddy, P.V.; Muhammad, Z.U.R. Efficient Pairing-Free Certificateless Authentication Scheme With Batch Verification for Vehicular Ad-Hoc Networks. *IEEE Access* 2018, 6, 31808–31819. [CrossRef]

**Publisher’s Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.