Hindawi
Security and Communication Networks
Volume 2021, Article ID 6679882, 11 pages
https://doi.org/10.1155/2021/6679882

Research Article

BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs

Azees Maria,[1] **Vijayakumar Pandi**,[2] **Jeatha Deborah Lazarus**,[2] **Marimuthu Karuppiah**,[3] **and Mary Subaja Christo**[4]

[1]*Department of Electronics and Communication, GMR Institute of Technology, Rajam, Andhra Pradesh, India*
[2]*Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, Tamilnadu, India*
[3]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Delhi-NCR Campus, Ghaziabad, Uttar Pradesh, India*
[4]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India*

Correspondence should be addressed to Vijayakumar Pandi; vijibond2000@gmail.com

Received 23 November 2020; Revised 13 January 2021; Accepted 4 February 2021; Published 18 February 2021

Academic Editor: Debiao He

Smart driving has become conceivable due to the rapid growth of vehicular ad hoc networks. VANETs are considered as the main platform for providing safety road information and instant vehicle communication. Nevertheless, due to the open wireless nature of communication channels, VANET is susceptible to security attacks by malicious users. For this reason, secure anonymous authentication schemes are essential in VANETs. However, when vehicles reach a new roadside unit (RSU) coverage area, the vehicles need to perform reauthentication with the current RSU, which significantly diminishes the efficiency of the entire VANET. Therefore, the introduction of blockchain technology has created opportunities for VANETs to resolve the aforementioned challenges. Due to the decentralized nature of blockchain technology, rapid reauthentication of vehicles is achieved in this paper through secure authentication code transfer between the consecutive RSUs. The security strength of the proposed blockchain-based anonymous authentication scheme against various harmful security attacks is proven in the security analysis section to ensure that it provides better security. In addition, blockchain, as presented in the performance analysis section, is used to substantially diminish the computational cost compared to conventional authentication schemes.

1. Introduction

With the speedy development of smart cities, the VANETs have fascinated extensive attention in both academia and industry. The development of VANETs brings inordinate comfortable and convenient driving experience for vehicle drivers. Two types of communications, the vehicle-to-vehicle (V2V) communication and the vehicle-to-roadside unit (V2R) communication, are established in VANETs to make cooperation between vehicle users and exchange appropriate driving information through the dedicated short-range communication (DSRC) radio [1]. However, due to the unique characteristics of VANETs such as high mobility and dynamic topology, the entire system is susceptible to various kinds of security attacks. Moreover, the security and privacy should be taken into consideration in VANETs seriously. In the traditional authentication schemes, the centralized trusted authority (TA) is responsible for registration, key distribution, and revocation of vehicles. Since the TA is centralized, it is liable to security attacks such as self-tempering with message, leakage of vehicular information, and the spreading of forged information in the VANET system. In addition, a single-point security failure of data storage in the centralized TA may cause the leakage of vehicle users' personal information. Particularly, in VANETs, it is very tough to deal with the dissemination of forged messages from the authorized vehicle users. The dissemination of forged messages from the authorized vehicles in the VANET system not only decreases the

driving efficiency but also causes some accidents that can threaten the life of vehicle users [2–4].

A specific blockchain-coordinated VANET, as shown in Figure 1, is typically made up of three main bodies: on-board unit-enabled vehicle units, road side units, and blockchain. In depth, the vehicles in the VANET system are mounted with onboard units to gather safety-related messages from other neighbouring vehicles [5, 6]. Roadside infrastructure typically refers to roadside units (RSUs) that are used to communicate as transfer nodes. The blockchain is used to maintain the vehicle attributes and authentication information of users in the VANET [7, 8]. It is noted here that the authentication information is an important reference to the VANET's reliability. Blockchains enable authenticity to be checked and validated in the VANET with a decentralized consensus algorithm without the intercession of the TA. The authentication information of a vehicle requires to be checked from time to time by virtue of the authentication of vehicles to reauthenticate each vehicle with each RSU as they join the contact ranges of different RSUs, though, despite the fact that the frequent authentication to check the identity of the vehicle units brings additional issues such as enormous communication overhead and computation overhead. In most state-of-the-art analyses, every time a vehicle reaches a current RSU coverage area, it needs to be reauthenticated by the current RSU, which generates a lot of redundant overhead and diminishes the performance of the VANET system. Owing to the rapid change in the topology of the network, excessive delays will not continue without serious consequences. Subsequently, in order to lower the computational burden of RSUs and the network communication latency, it is important to diminish the redundancy caused by frequent authentication. Moreover, maintaining the reliability of the decentralized, untrusted VANET system and curbing the misconduct of vehicle users are daunting tasks [9]. Additionally, there is an absence of scalability during the anonymous authentication of vehicles, which prompts the incapability to adjust to the changing requests of VANETs.

Our contributions: to overcome the above problems, a blockchain-based anonymous authentication scheme is presented in this paper. The main contributions of this paper are summarized as follows:

To propose a blockchain-assisted time-efficient anonymous authentication to initially validate the legitimacy of the vehicle user, the RSUs are considered to be the miners in the proposed system which are able to verify the validity of a vehicle consumer via the consensus process. Moreover, the Merkle hash tree (MHT) is utilized in the system to understand the real-time authentication records. The authentication record can be extended to newly joined vehicles, which significantly upsurges the operability of the VANET system.

When a vehicle user is now a valid member of the VANET via the preliminary anonymous authentication, it is suggested to propose a blockchain-assisted successful V2R anonymous handover authentication. The authentication information of a vehicle should be transferred between dissimilar RSUs in order to achieve safe and convenient handover authentication, making the VANET system additionally scalable.

To track the disobedient vehicles, the legitimacy of the vehicle owner can be queried at any time in such a way that the traceability calculation can be accomplished by examining the historical records.

The rest of this paper is ordered as follows. Section 2 presents some relative works of this paper. Section 3 presents preliminaries that involve bilinear pairing, CDH problem, the concept of blockchain, and assumptions. Our proposed BBAAS work is presented in Section 4. The security analysis and performance analysis are seen in Sections 5 and 6. The conclusion is ultimately provided in Section 7.

2. Related Works

The open wireless environment created by VANETs presents significant privacy and security problems that are not appropriate for implementation in real-time applications [10]. Zhang et al. [11] developed an identity-based batch verification (IBV) method for communications such as V2R and V2V in VANETs that used a temperature-proof privacy security unit, and each entity stored the master key of the system generally to generate pseudo-identities. Nevertheless, in each vehicle, keeping the master key of the system could cause efficient attacks and unexpected risks to the system. In addition, this system neglected to take into account the problem of scalability and the resulting overhead of communication. Some privacy problems, such as reliability, anonymity, and traceability, have become the domains to be studied with growing privacy interest in VANETs. An interesting privacy-preserving communication and exact reward given for V2G networks was proposed by Yang et al. in 2011 [12]. They suggested a form of exact and equal incentive model with good serviceability, where each participating vehicle for each service it provides is compensated by the operator of a V2G network. Taking into account the very unique existence of V2G networks, they made the first attempt to discuss privacy. In 2015, Wang et al. discovered that the framework of Yang et al. was unconfident and suggested the concrete attack model [13]. Then, with usable cryptographic primitives, they developed a new traceable privacy-preserving communication and precise reward scheme. Regretfully, the unlikability cannot be resolved by Wang et al.'s method. Due to the versatility of the vehicle, the question of privacy protection in V2G networks is more impressive. Han and Xiao examined numerous privacy preservation issues in V2G networks, including privacy of location, privacy recognition, anonymous authentication, billing and payment for privacy preservation, aggregation of concealed data, and publishing of privacy data preservation. Homomorphic encryption, ring signature, group signature, blind signature, third-party anonymity, and anonymity networks are utilized in these techniques [14]. Their paper does not project new schemes, and it is not possible to use the surveyed schemes in anonymous V2G network rewards. A complex key management scheme for location-based

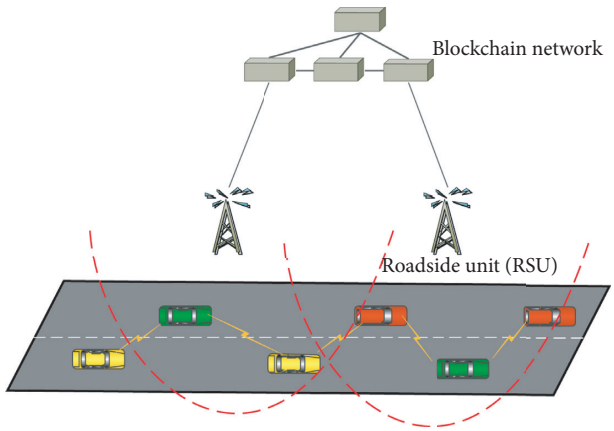

Figure 1: Illustration of VANET coordinated with the blockchain network.

services (LBSs) was suggested by Lu et al. [15]. With separate session keys, the LBS session is split into different time slots. A vehicular data authentication scheme [16] is defined afterward, where the probabilistic authentication technique is deployed for the detection of malicious actions. Moreover, community signature-based hash message authentication code (HMAC) is utilized in [17] for the purpose of avoiding computational delay for certificate revocation list (CRL) checking. Similarly, a distributed trust-extended authentication mechanism (TEAM) for distributed V2V communication was developed by Chuang and Lee [18]. Note that the system of transitive trust relationships is used in order to increase the efficiency of authentication. Numerous authentication schemes have been industrialized recently [19, 20], highlighting lightweight VANET authentication and protection of privacy. The aforementioned anonymous authentication schemes are somewhat ineffectual and inappropriate for practical VANET environments because of their high-level computational cost, communicational cost, and storage cost. Moreover, most of the existing anonymous authentication schemes were not concentrated on integrity preservation while transmitting the VANET data over the internet. Hence, to meet out these necessities, a new blockchain-based BBAAS anonymous authentication is proposed in this paper.

3. Preliminaries

In this section, a few vital preliminaries, which include bilinear pairing and computational Diffie–Hellman (CDH) problem, are discussed.

3.1. Bilinear Pairing. Let G_1 and G_2 be two multiplicative groups with the large prime order q. Let e: $G_1 \times G_2 \longrightarrow G_2$ symbolize a bilinear pairing, pleasing the following requirements:

(1) Bilinear: consider two randomly chosen generators $Q, S \in G_1$ and two randomly chosen elements $a, b \in Z_q^*$; then, $e(aQ, bS) = e(Q, S)^{ab}$

(2) Nondegeneracy: there is a generator $Q \in G_1$ such that $e(Q, Q)$is not equal to 1

(3) Computability: consider any two randomly selected points $Q, S \in G_1$; the bilinear pairing $e(Q, S)$ could be well calculated within the polynomial period

3.2. Computational Diffie–Hellman (CDH) Problem. The CDH and decisional Diffie–Hellman (DDH) problems are detailed clearly in Definitions 1 and 2, respectively, in this section.

Definition 1. (computational Diffie–Hellman problem in G). Let G be a multiplicative cyclic group of order q, and Q *is* the generator value of G. Then, for the given values $\{Q, Q^a, Q^b\}$, where $a, b \in Z_q^*$, the CDH problem stated that it is computationally intractable to compute the value Q^{ab}.

Definition 2. (decisional Diffie–Hellman problem in G). The DDH problem stated that $Q^{ab} = Q^c$ only with $\{Q, Q^a, Q^b, Q^c\}$, where $a, b, c \in Z_q^*$.

It is therefore explicitly confirmed that an opponent who is unable to overcome the CDH with a nonnegligible probability has no way of obtaining the protocol's secret values $a, b, c \in Z_q^*$ in G.

3.3. Blockchain Concept. A distributed, decentralized, irreversible, and immutable network framework is blockchain. The key benefit of the blockchain network is that, with very low computing costs, it can effectively deal with anonymous authentication issues [4–8, 21]. In this technology, the interaction of TA is completely avoided to evade the outdated centralized structure. Instead, the end user peer-to-peer communication is used to develop the decentralized structure. In order to validate the reliability of the transaction in each node database, blockchain uses the principles of cryptography, timestamp, prehash, Merkle root hash, nonce, and consensus algorithm such that transaction records are verifiable, transparent, irreversible, undeniable, difficult to tamper, immutable, and traceable.

Hash functions are primarily used in blockchain technology for data integrity preservation, consensus calculation for proof of work, linking of blocks with previous block hash, etc. The most commonly used hash functions in blockchain are SHA-256 and RIPEMD160. However, SHA-256 is mostly used to calculate the Merkle root hash from transaction records, whereas RIPEMD (RIPE Message Digest) 160 is mainly utilized to create bitcoin addresses. The block structure with the application of hash function in the calculation of Merkle root hash, which is similar to Merkle hash tree (MHT) mentioned in the data structure, is shown in Figure 2. In the MHT, the hash values of transaction records are calculated and stored in the leaf nodes. In the two leaf nodes, the hash values are taken and hashed in pairs and then stored in the block. As can be seen in Figure 2, until the last hash value is determined as the root hash value of Merkle, this method is repeated. For instance, to get a new

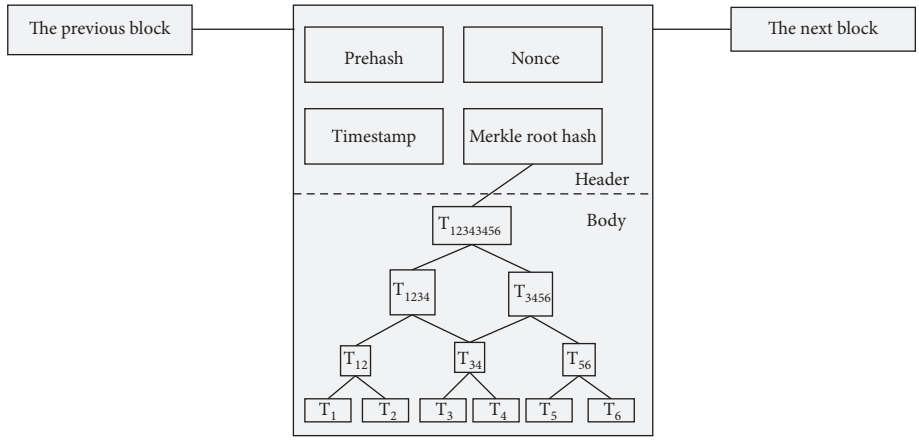

Figure 2: Block structure.

hash value hash AB, the hash values of two leaf nodes A and B are again hashed together.

3.4. System Model. In this paper, a blockchain-based anonymous authentication system is proposed for VANETs. The main components of the proposed system include the trusted authority (TA), RSU, vehicles, and the blockchain network.

Trusted authority: the vehicle users are required to submit their original credentials such as address and mail-id to the TA during the time of registration to enter inside the VANET system. After successful authentication in the TA, the TA is accountable to generate the public and private keys for registered vehicles and calculates an authentication code. These metrics are used to authenticate the vehicles as well as to track malicious vehicles with the assistance of RSUs.

Roadside units (RSU): the RSUs verify and anonymously authenticate all the broadcasted transactions of the vehicles. Moreover, the RSUs have the computing power to solve the puzzle to add the new block in the blockchain after successful initial authentication of a vehicle. If a vehicle enters the region of a current RSU after the previous RSU has been authenticated, the current RSU may use the statistics of the previous RSU to conduct handover authentication.

Vehicles: the TA provides secret and unique credentials to a vehicle user after his successful registration in the TA. These credentials of the vehicle user are stored in the on-board unit (OBU) which is equipped in the VANET vehicle to perform communication as well as computation operations in a secure manner during V2V and V2R communications to prevent external security attacks. When a vehicle enters into the coverage of an RSU, initial anonymous authentication or handover authentication needs are required to carry out with the RSU by using authentication code distributed by the TA.

3.5. Assumptions. The following assumptions are employed in this paper in order to establish the structure of the proposed scheme:

The trusted authority (TA) is considered to be the VANET system's control center with adequate storage space to maintain the dataset containing the real information of the vehicle user and RSUs

The RSUs have high computation capability to successfully perform reauthentication of vehicles in the authentication handover phase based on authentication code transactions

It is not possible for the adversaries to compromise more than 50% of the RSUs in the blockchain integrated network

The RSUs have adequate storage capacity, and they are different to each other

4. Proposed Scheme

The proposed blockchain-supported anonymous authentication system is outlined in this section, containing five phases: system description, system initialization, registration phase, anonymous authentication phase, and handover anonymous authentication phase.

4.1. System Description. The system overview of the proposed scheme is depicted in Figure 3. In this proposed system, the vehicle units are required to directly submit necessary materials which contain vehicle's private information to the nearest TA [22]. Only the TA preserves this private information in its database with high-level confidentiality. This private information will be used by the TA for tracking the vehicle's real identity from the pseudonym identities in case of disputes. In this proposed system, the TA is connected with the blockchain network along with the RSUs. The RSUs and vehicle units need to complete the initial authentication with the TA to get the authentication code as well as the pseudonym identity.

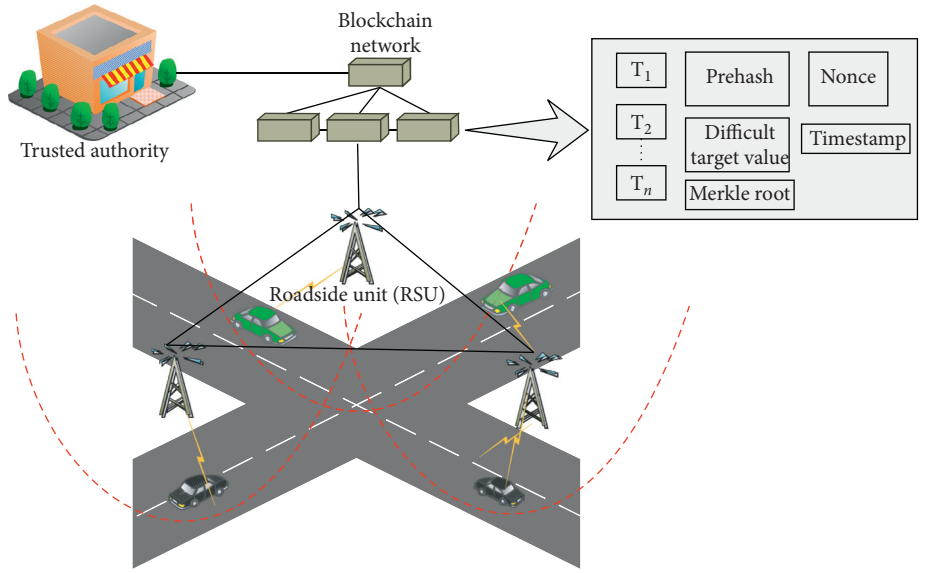

Figure 3: System overview.

Once the initial authentication process is completed in the TA, based on the authentication code, the RSUs can authenticate the vehicles using the blockchain network when they enter inside the coverage region of RSUs. Then, when the vehicle enters into the current RSU communication range, the current RSU authenticates the vehicle based on the handover certificate (OC) given by the previous RSU. Once the authentication is successful in the current RSU, it will give the authentication token to the vehicle.

4.2. System Initialization. The system initialization phase aims to produce secret keys for the TA. The TA generates two cyclic groups G_1 and G_2 with order p satisfying the bilinear map relation e: $G_1 \times G_2 \longrightarrow G_T$. g_1 and g_2 are the generators of the cyclic groups G_1 and G_2, respectively. Moreover, the TA chooses three cryptographic H_1, H_2, H_3 in such a way that H_1: $G_1 \longrightarrow \{0,1\}^*$, $H_2\{0,1\}^* \longrightarrow Z_q^*$, and H_3: $\{0,1\}^* \longrightarrow Z_q^*$. By randomly choosing the private key β, the TA generates its public key (Q_{TA}) as $Q_{TA} = g_1^{\beta}$ and publishes system parameters $\{p, g_1, g_2, G_1, G_2, G_T, e, H_1, H_2, H_3, Q_{TA}\}$.

4.3. Registration. The offline registration is performed in the TA for the vehicles and RSUs as follows. The vehicle users need to submit all the necessary private information such as phone number, mail-id, and address. Once the private information is successfully submitted and validated by the TA, the TA chooses a random number $u_i \in Z_q^*$ for each vehicle user and computes $PK_v = g_1^{u_i}$ as the public key of the vehicle user. Then, it gives the private key and public key to the vehicle user in a secret manner in the offline mode after its successful registration in the TA. Moreover, the TA computes an authentication code (AC) for each vehicle user at time t as follows:

$$AC(t) = \frac{\sum_{i=1}^{n} v_i a_i}{n}. \quad (1)$$

Here, $v_i \in Z_q^*$ represents the identity value chosen by the TA to each vehicle user, $a_i \in Z_q^*$ represents the identity value given by the vehicle user to the TA during the time of registration, and n represents the number of vehicles. Once the AC is generated, the TA broadcasts vehicle transaction details to all the TAs by encrypting them by mutually agreed session keys among the TAs. All TAs are dedicated to solve the puzzle after getting the broadcast information from the local TA. Once the minor successfully solves the puzzle, a validated AC along with the pseudonym identity is then appended at the end of the blockchain as a new block. Here, the pseudonym identity is also generated by the TA to each vehicle to preserve the real identity from other entities in the network. The TA helps to update and store the AC of a vehicle user in the blockchain. These AC values of each vehicle are updated in the blockchain for the investigation of the new RSUs in the VANET. Lastly, all TAs and RSUs save a copy of the updated blockchain in its database when the authenticated AC is attached to the blockchain.

4.4. Anonymous Authentication. The RSUs will authenticate the vehicles in this phase using the AC created by the TA in the registration process. In this phase, it is required for an RSU to validate the legitimacy a vehicle user anonymously when the vehicle reaches network coverage area of that particular RSU. Once the vehicle user enters the first RSU area, he will pass the pseudonym ID to the RSU along with the node number. Then, the RSU checks the identity and authentication code of the pseudonym. In this phase, a session key is generated between the RSU and vehicle as follows.

The vehicle user computes $SK_v = PK_r^{u_i}$, where $PK_r = g_2^{k_i}$ is the public key of the RSU and k_i is the private key of the RSU. Similarly, the RSU calculates $SK_{r,1} = PK_v^{k_i}$, where

$\mathrm{PK}_v = g_1^{u_i}$ represents the public key of the vehicle user. Then, the RSU selects a master key $r_i \in Z_q^*$ and calculates $\mathrm{SK}_r = g_1^{r_i}$. This SK_r value is kept secret by the RSU. In addition, the RSU calculates $\mathrm{PK}_{r,1} = g_2^{r_i}$ and sends this value to the vehicle user along with a timestamp value T_1.

Then, the vehicle user checks the freshness of the timestamp T_1 and computes $\mathrm{SK}_{v,1}$ as

$$\mathrm{SK}_{v,1} = \mathrm{PK}_{r,1} \cdot \mathrm{SK}_v^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_v))}. \tag{2}$$

Here, ID represents the pseudonym identity of the vehicle user. Then, the vehicle computes the session key as

$$\mathrm{SK} = e\left(\mathrm{SK}_{v,1}, g_1\right). \tag{3}$$

Then, the RSU computes

$$\mathrm{SK}_{r,2} = \mathrm{SK}_r \cdot \mathrm{SK}_{r,1}^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))}. \tag{4}$$

If the vehicle's AC is classified as zero, the vehicle is deemed to be revoked, and the RSU will not provide services. A revoked vehicle consumer will not be disguised as an ordinary vehicle due to the blockchain's tamper-resistance feature, and it will not be permitted to share data with the RSU. The session key is created by the RSU as

$$\mathrm{SK} = e\left(g_2, \mathrm{SK}_{r,2}\right). \tag{5}$$

Proof of correctness:

$$\begin{aligned}
\mathrm{SK} &= e\left(g_2, \mathrm{SK}_{r,2}\right) \\
&= e\left(g_2, \mathrm{SK}_r \cdot \mathrm{SK}_{r,1}^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))}\right) \\
&= e\left(g_2, g_1^{r_i} \cdot \mathrm{PK}_v^{k_i H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))}\right) \\
&= e\left(g_2, g_1^{r_i} \cdot g_1^{k_i u_i H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))}\right) \\
&= e\left(g_1, g_2^{r_i} \cdot g_2^{k_i u_i H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))}\right) \\
&= e\left(g_1, \mathrm{PK}_{r,1} \cdot \mathrm{SK}_v^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))}\right) \\
&= e\left(\mathrm{SK}_{v,1}, g_1\right).
\end{aligned} \tag{6}$$

4.5. Handover Authentication. When a vehicle user leaves the previous RSU coverage region and the current RSU coverage region arrives, this handover authentication is performed to transfer the authentication details of the vehicle and the previous RSU to the subsequent RSU. Then, the previous RSU passes the AC and block number of the vehicle to the current RSU in the blockchain for investigation. If the vehicle's AC is not zero, then the latest RSU accepts the existing authentication of the previous RSU. Therefore, the current RSU is not required to authenticate the vehicle's AC again. Then, the current RSU will execute the following steps.

The RSU first computes two handover keys HK_1 and HK_2. Then, these keys are sent to the current RSU.

$$\begin{aligned}
\mathrm{HK}_1 &= \mathrm{SK}_{r,1}^{zH_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}, \\
\mathrm{HK}_2 &= \mathrm{PK}_{r+1}^{zk_i},
\end{aligned} \tag{7}$$

where $z \in Z_q^*$ represents the random number and $\mathrm{PK}_{r+1} = g_2^{k_i+1}$ represents the public key of the current RSU. After obtaining HK_1 and HK_2 from the preceding RSU, the current RSU sends HK_2 to the vehicle user. Then, the current RSU chooses a random number $w \in Z_q^*$ and calculates $\mathrm{HK}_r = g_1^w$ and $\mathrm{HK}_{r,1} = g_2^w$. Then, HK_r is kept as a secret value, and $\mathrm{HK}_{r,1}$ is sent to the vehicle user as a handover code. By receiving $\mathrm{HK}_{r,1}$ and HK_2, the vehicle computes

$$\begin{aligned}
\mathrm{HK}_v &= \mathrm{HK}_2^{u_i H_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}, \\
\mathrm{HK}_{v,1} &= \mathrm{HK}_{r,1} \cdot \mathrm{HK}_v.
\end{aligned} \tag{8}$$

Lastly, the vehicle user calculates the new session key as

$$\mathrm{SKNV} = e\left(\mathrm{HK}_{v,1}, g_1\right). \tag{9}$$

Then, the current RSU computes the new session key as

$$\begin{aligned}
\mathrm{HK}_{\mathrm{ho}} &= \mathrm{HK}_1^{k_{i+1}}, \\
\mathrm{HK}_{\mathrm{ho},1} &= \mathrm{HK}_r \cdot \mathrm{HK}_{\mathrm{ho}},
\end{aligned} \tag{10}$$

where $k_{i+1} \in Z_q^*$ represents the private key of the current RSU.

$$\mathrm{SKNR} = e\left(g_2, \mathrm{HK}_{\mathrm{ho},1}\right). \tag{11}$$

Proof of correctness:

$$\begin{aligned}
\mathrm{SKNR} &= e\left(g_2, \mathrm{HK}_{\mathrm{ho},1}\right) \\
&= e\left(g_2, \mathrm{HK}_r \cdot \mathrm{HK}_{\mathrm{ho}}\right) \\
&= e\left(g_2, g_1^w \cdot \mathrm{HK}_1^{k_{i+1}}\right) \\
&= e\left(g_2, g_1^w \cdot \mathrm{SK}_{r,1}^{k_{i+1} z H_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}\right) \\
&= e\left(g_2, g_1^w \cdot g_1^{k_i u_i k_{i+1} z H_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}\right) \\
&= e\left(g_2^w \cdot \mathrm{PK}_{r+1}^{k_i u_i z H_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}, g_1\right) \\
&= e\left(\mathrm{HK}_{r,1} \cdot \mathrm{HK}_2^{u_i H_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}, g_1\right) \\
&= e\left(\mathrm{HK}_{r,1} \cdot \mathrm{HK}_2^{u_i H_3(\mathrm{ID}\|\mathrm{AC}\|\mathrm{SK})}, g_1\right) \\
&= e\left(\mathrm{HK}_{r,1} \cdot \mathrm{HK}_v, g_1\right) = e\left(\mathrm{HK}_{v,1}, g_1\right) = \mathrm{SKNV}.
\end{aligned} \tag{12}$$

5. Security Analysis

In this section, we briefly analyse the security strength of our blockchain-assisted anonymous authentication scheme with respect to various security attacks, anonymity, and forward secrecy.

5.1. Security Theorems

Lemma 1. *Assume an attacker A may possibly intrude upon the mutual authentication between the vehicle and the RSU through a nonnegligible benefit η. In this regard, a challenger C is constructed, which can resolve the CDH problem with η.*

Proof. Let us consider that an attacker (A) generates authorized $\mathrm{SK}_{v,1} = \mathrm{PK}_{r,1} \cdot \mathrm{SK}_v^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_v))}$ with η, where $\mathrm{PK}_{r,1} = g_2^{r_i}$ and T_1 represents the current timestamp. For instance, A will generate a new session key $\mathrm{SK} = e(\mathrm{SK}_{v,1}, g_1)$ with a different AC of an adversary, and the attacker should pass the RSU's AC verification in the blockchain. However, the attacker cannot create $\mathrm{SK}_v^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_v))}$ value of any vehicle user. Moreover, if the attacker tries to change any AC value of the user using the block number, it will reflect in the previous blocks due to previous hash available in the header as shown in Figure 4.

Moreover, the calculation of $\mathrm{SK}_{v,1} = \mathrm{PK}_{r,1} \cdot \mathrm{SK}_v^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_v))}$ to crack $\mathrm{SK} = e(g_2, \mathrm{SK}_{r,2}) = e(g_2, \mathrm{SK}_r \cdot \mathrm{SK}_{r,1}^{H_2(\mathrm{ID}\|\mathrm{AC}\|T_1\|H_1(\mathrm{SK}_{r,1}))})$ is the CDH problem, with a complexity of $\eta_0 \geq \eta(1 - 1/q)/qH_1$. This hardness of the CDH problem prevents an adversary from violating the mutual authentication of the RSU and vehicle user in the proposed scheme. □

Theorem 1. *The proposed scheme provides secure session key agreement if the computational Diffie–Hellman (CDH) problem is intractable.*

Proof. It is stated that the proposed confidentiality preservation scheme is session key agreement secure if $\chi(A)$ is negligible. Let $\chi(A)$ represent the probability that the attacker A could guess the session key of the vehicle user in the anonymous authentication phase. Let $\chi(S)$ represent the event in which A guessed the session key in the authentication process correctly. Hence, $\Pr[\chi(S)] \geq (\eta/2)$, where η represents the nonnegligible advantage of A. Let $\chi(v)$ and $\chi(r)$ represent the event test queries made by A to guess the session key in oracle of the vehicle side and RSU side, respectively. Let $\chi(C)$ represent the event that violates mutual authentication in the anonymous authentication phase of the proposed scheme. Then,

$$\begin{aligned}
\Pr[\chi(S)] &= \Pr[\chi(S)\wedge\chi(P)] + \Pr[\chi(S)\wedge\chi(D)\wedge\chi(C)] \\
&\quad + \Pr[\chi(S)\wedge\chi(D)\wedge\chi(C)] \geq \frac{\eta}{2}, \\
\Pr[\chi(S)\wedge\chi(P)] &+ \Pr[\chi(S)\wedge\chi(D)\wedge\chi(C)] \geq \frac{\eta}{2} \\
&\quad - \Pr[\chi(S)\wedge\chi(D)\wedge\chi(C)] \geq \frac{\eta}{2} - \Pr[\chi(C)].
\end{aligned} \tag{13}$$

Since the events $\chi(S)\wedge\chi(D)\wedge\chi(C)$ and $\chi(P)$ are equal, the equation can be rewritten as $\Pr[\chi(S)\wedge\chi(P)] \geq (\eta/4) - (\Pr[\chi(C)]/2)$. According to Lemma 1, $\Pr[\chi(C)]$ is negligible. In the proposed work, the values $z, w \in Z_q^*$ were randomly chosen, and $\mathrm{HK}_{v,1} = \mathrm{HK}_{r,1} \cdot \mathrm{HK}_v$ is calculated. Therefore, A could solve a CDH problem with the hardness $(\eta/2) - \Pr[\chi(C)]$. Hence, it is proved that the proposed scheme is session key agreement secure. □

5.2. Anonymity.

In the proposed scheme, the vehicle units are required to directly submit necessary materials which contain vehicle's private information to the nearest TA. Only the TA preserves this private information in its database with high-level confidentiality. This private information will be used by the TA for tracking the vehicle's real identity from the pseudonym identities in case of disputes. Since the RSUs authenticate the vehicles based on the authentication code and dummy identity available in the blockchain, the real identities are not revealed to other entities in the network at any cost. During the calculation of session key $\mathrm{SK} = e(\mathrm{SK}_{v,1}, g_1)$ also, the real identities are not disclosed to RSUs. Therefore, the proposed scheme achieves authentication with anonymity.

5.3. Replay Attack and Man-in-the-Middle Attack.

An adversary can delay the message that is sent between the RSU and the vehicle in this proposed BBAAS method. If the message is delayed, however, then the timestamp attached will be invalid. Then, it will not authenticate the message. If the timestamp is not correct, then without performing other steps, the vehicle or the RSU simply discards the message received. Suppose if the attacker wants to send a message to the current RSU that is authenticated by the previous RSUs, the message would then be ineffective in fulfilling the authentication as well. Both the current RSU and the vehicle can compute a new session key to encrypt the communicating messages. Therefore, if the message is not encrypted with the new session key, then also the RSU discards the messages immediately. Moreover, the man-in-the-middle attack is also not possible in the proposed scheme due to the linkage of generated AC in the blockchain. Once the AC is generated, it is updated immediately in the blockchain by the TA. Hence, man-in-the-middle attack is meaningless in our proposed scheme.

5.4. Nontraceability and Impersonation Attack.

Based on Theorem 1 and Lemma 1, A cannot calculate the valid session keys of the vehicle and RSU. Consequently, the proposed scheme can withstand against the impersonation attack. The RSUs choose secret random numbers $w, z \in Z_q^*$ for performing handover authentication in our proposed scheme. Moreover, the RSU selects a master key $r_i \in Z_q^*$ and calculates $\mathrm{SK}_r = g_1^{r_i}$. Here, this SK_r value is kept secret by the RSU. In addition, these are the temporary keys randomly generated. Since no constant values are used for the session key generation, our proposed scheme also achieves nontraceability.

5.5. Message Modification Attack.

In this proposed method, the integrity is preserved from malicious uses. To preserve integrity, the preceding block hash value is linked with the

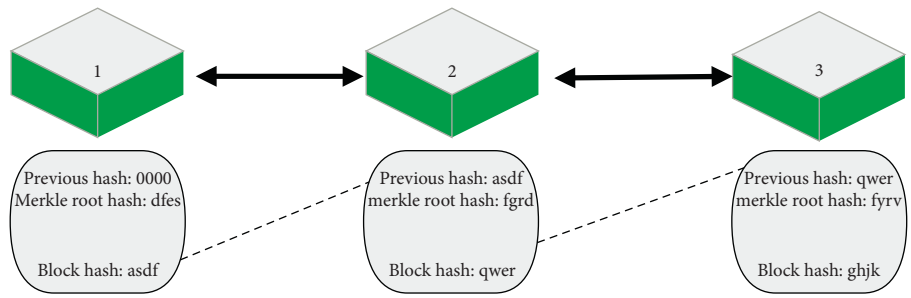

Figure 4: Linkage of previous hash with the current block hash value.

next block hash value. If any modifications occurred in any block, it will be reflected to the entire blockchain as shown in Figure 5. Since the miners solved the puzzle and added the new block in the blockchain based on the proof of work, the modifications in any block will be reflected in the TA also. Therefore, message modification attack is not possible in our proposed scheme.

6. Performance Analysis

In this section, the performance of the proposed BBAAS scheme is represented in terms of storage cost, communicational cost, and computational cost.

6.1. Storage Cost. In blockchain technology, the storage overhead is considered as an important parameter in the RSU and TA. Generally, the block header of the single block is approximately 80 bytes [5]. In the blockchain, it is assumed that every new block is generated for every 10 minutes; then, the storage overhead is 80 bytes $*$ 60 minutes/10 minutes $*$ 24 $*$ 365 = 4.2 MB per year. In the BBAAS, the TA requires to store $\{v_i \in Z_q^*, a_i \in Z_q^*\}$ in its database for every vehicle user. Moreover, the TA generates AC to each vehicle user. Therefore, the maximum storage overhead in the TA side is 4.2 MB + n $*$ (64 + 64 + 64) bits per year, where n represents the number of vehicles registered in the TA per year, 1248 bits. In addition, the storage overhead in the vehicle side in the BBAAS is about 64 + 64 + 64 bits. In this scheme, each vehicle requires to store v_i, a_i, and ACin its database for every vehicle user.

6.2. Computational Cost. The computational cost of the BBAAS is analysed with Qi Feng et al.'s scheme [23], Dong Zheng et al.'s scheme [24], Zhaojun Lu et al.'s scheme [25], and Lun Li et al.'s scheme [26] as shown in Table 1. To find out the actual timing values of various cryptographic primitives of the proposed BBAAS, a 2 GHz laptop with 4 GB installed memory is used, with Cygwin 1.7.35–15 [27], PBC library [28], and GCC version 4.9.2 being considered. The average timing values found in the calculation of computational overhead are listed as follows:

T_p: the average amount of time for carrying out a bilinear pairing process≈2.7 ms

T_{mul}: the average amount of time for carrying out a point multiplication process≈0.6 ms

T_{mh}: the average amount of time for carrying out a map-to-point hash function process≈1.6 ms

T_{add}: the average amount of time for carrying out a point addition process≈0.6 ms

T_{exp}: the average amount of time for carrying out a modular exponentiation process≈1.6 ms

T_h: the average amount of time for carrying out a general hash function process≈1.6 ms

From Table 1, it is clearly shown that the BBAAS takes one time-consuming bilinear pairing operation, one time-consuming hashing operation, and one less time-consuming point multiplication operation for anonymous authentication operation.

From Figure 6, it is very clear to understand that the BBAAS takes only around 490 ms for anonymous authentication of 100 users, whereas the other existing approaches take more than 580 ms for verifying 100 vehicle users, which tells that the BBAAS takes less computational time for anonymous authentication compared to related schemes. Moreover, the computational time of the BBAAS increases linearly as the number of vehicle users increases.

6.3. Communication Cost. In the BBAAS, once the vehicle user enters the region of the first RSU, he will transfer the pseudonym ID along with the node number to the RSU. Here, pseudonym ID is an element of Z_q^*, and the block number is 32 bits in length. In addition, the RSU calculates $\text{PK}_{r,1} = g_2^{r_i}$ and sends this value to the vehicle user along with a timestamp value T_1. Here, $\text{PK}_{r,1}$ is an element of G_2. Then, in the BBAAS handover phase, the RSU first computes two handover keys HK_1 and HK_2. Then, these keys are sent to the current RSU. After obtaining HK_1 and HK_2 from the previous RSU, the current RSU sends HK_2 to the vehicle user. Therefore, the total communication cost for anonymous authentication is 64 + 32 + 1024 = 1090 bits. Then, the computation cost for the handover authentication phase is 1024 + 1024 = 2048 bits. The communication cost of various schemes is listed in Table 2. From Figure 7, it is clearly shown that the communication costs of our proposed BBAAS during the authentication phase and handover authentication phase are less compared to the related existing schemes.

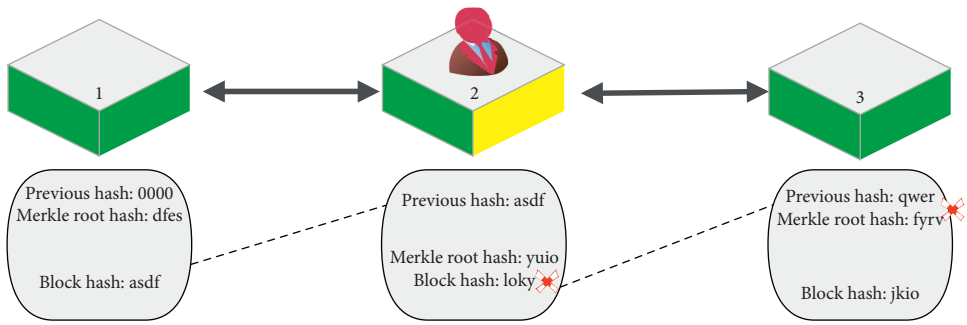

Figure 5: Message modification attack.

Table 1: Computational cost of various authentication schemes.

Method	One vehicle	n vehicles
Qi Feng et al.'s scheme	$2T_p + 2T_h + 3T_{\text{exp}}$	$(n+1)T_p + 2nT_h + 3nT_{\text{exp}}$
Dong Zheng et al.'s scheme	$2T_p + 2T_h + 3T_{\text{mh}} + 3T_{\text{add}}$	$2nT_p + 2nT_h + 3nT_{\text{mh}} + 3nT_{\text{add}}$
Zhaojun Lu et al.'s scheme	$2T_p + 3T_h + 3T_m$	$(n+1)T_p + 3nT_h + 3nT_m$
Lun Li et al.'s scheme	$3T_p + 2T_m + 2T_h$	$3nT_h + 2nT_m + (1+2n)T_p$
Proposed scheme	$2T_p + T_m + T_h$	$(n+1)T_p + nT_m + nT_h$

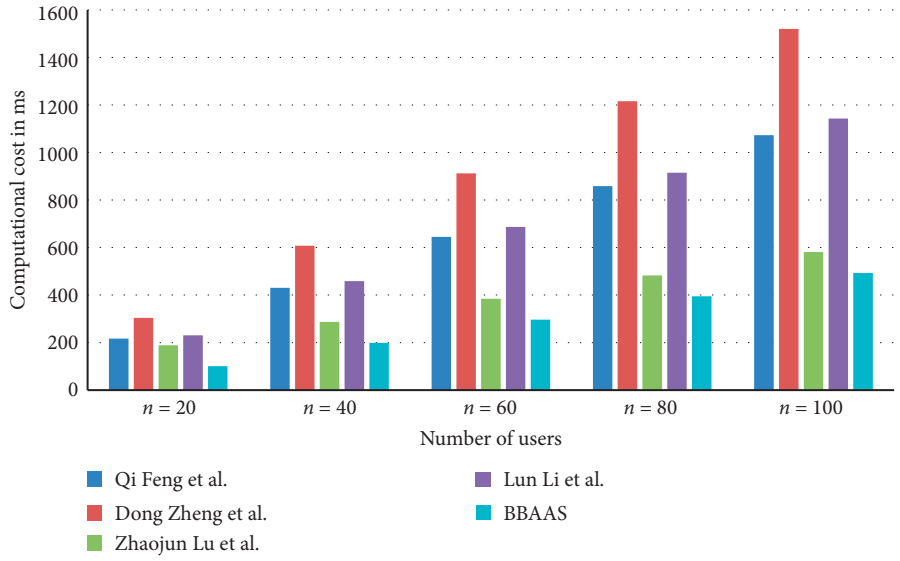

Figure 6: Computational cost of various schemes.

Table 2: Communicational cost of various schemes.

Qi Feng et al.'s scheme (bits)	Dong Zheng et al.'s scheme (bits)	Zhaojun Lu et al.'s scheme (bits)	Lun Li et al.'s scheme (bits)	BBAAS (authentication phase) (bits)	BBAAS (handover authentication phase) (bits)
4096	5440	4416	6048	1096	2048

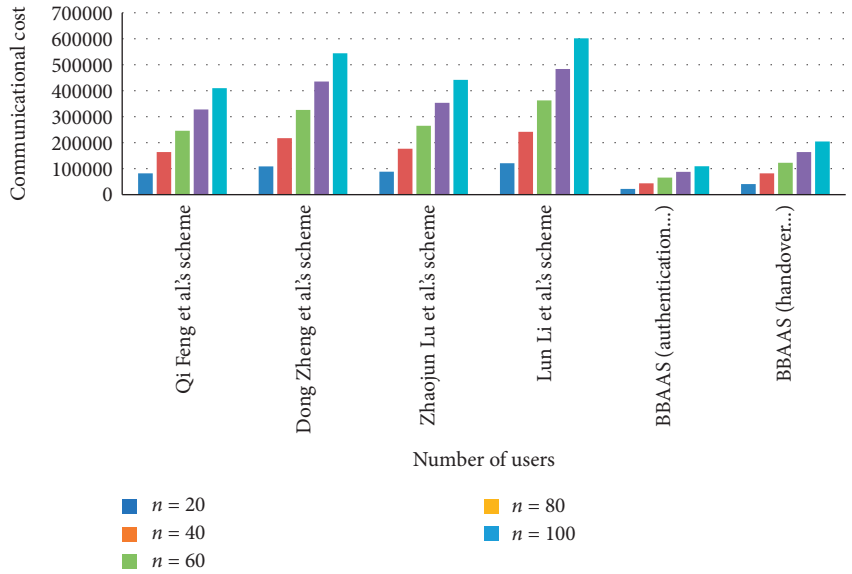

Figure 7: Communicational cost of various schemes.

7. Conclusions

Recently, there are no anonymous authentication and handover authentication schemes for blockchain-based VANETs that provide provable security to RSUs and vehicle users with less computational cost and communicational cost. Motivated by this, a blockchain-based anonymous authentication scheme is proposed in this paper for providing secure communication in VANETs. In the proposed scheme, the RSUs can effectively authenticate the vehicles in an anonymous manner, and they also perform future communications through the shared session key. Moreover, the integrity of the transmitting message is completely preserved to avoid modification attack due to the support of the blockchain. In addition, the BBAAS provides high-level confidentiality during message transmission in VANETs. The performance analysis section proved that the BBAAS is efficient in terms of computational cost, storage cost, and communication cost, and so, it is highly practical for real-time applications. In future works, it is decided to develop blockchain-assisted ownership exchange protocols which allow the handover of ownership of one vehicle user to another vehicle user in a secure and distributed manner during the time of vehicle reselling.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] M. Azees, P. Vijayakumar, and L. Jegatha Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[2] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[3] M. Azees and P. Vijayakumar, "omputationally efficient key distribution scheme for vehicular ad-hoc networks," *Australian Journal of Basic and Applied Sciences*, vol. 10, pp. 171–175, 2016.

[4] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, 2017.

[5] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, http://www.bitcoin.org/bitcoin.pdf.

[6] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[7] E. F. Jesus, V. R. L. Chicarino, C. V. N. D. Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, pp. 1–27, Article ID 7817614, 2018.

[8] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, and C.-M. Chen, "An improved blockchain-based authentication protocol for iot network management," *Security and Communication Networks*, vol. 2020, pp. 1–16, Article ID 8836214, 2020.

[9] P. Vijayakumar, M. Azees, and L. J. Deborah, "Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks," in *Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*.

[10] L. Zhu, C. Chen, X. Wang, and A. O. Lim, "SMSS: symmetricmasquerade security scheme for VANETs," in *Proceedings*

of the 10th International Symposium Autonomous Decentralized Systems, pp. 617–622, Tokyo, Japan, March 2011.

[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the IEEE INFOCOM-27th Conference Computer Communication*, pp. 246–250, Phoenix, Arizona, April 2008.

[12] Z. Yang, S. Yu, W. Lou, and C. Liu, "P. 2: $P{2}$: privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[13] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2340–2351, 2015.

[14] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: a survey," *Computer Communications*, vol. 91-92, pp. 17–28, 2016.

[15] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2012.

[16] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Journal of Information Science*, vol. 262, pp. 172–189, 2014.

[17] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

[18] M.-C. Chuang and J.-F. Lee, "TEAM: trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2014.

[19] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[20] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[21] C. Lin, D. He, X. Huang, X. Xie, and K. K. R. Choo, "Blockchain based system for secure outsourcing of bilinear pairings," *Information Sciences*, vol. 527, pp. 590–601, 2020.

[22] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: a blockchainbased anonymous reputation system for trust management in vanets," 2018, https://arxiv.org/abs/1807.06159.

[23] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146–4155, 2020.

[24] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[25] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2792–2801, 2019.

[26] L. Li, J. Liu, L. Cheng et al., "CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[27] Cygwin: Linux Environment Emulator for Windows. [Online]. Available: http://www.cygwin.com/.

[28] PBC library: https://crypto.stanford.edu/pbc/.