A Fog Computing and Blockchain-based Anonymous Authentication Scheme to Enhance Security in VANET Environments

Zahraa Sh. Alzaidi
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
pgs.zahraa.shaker@uobasrah.edu.iq

Ali A. Yassin
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
ali.yassin@uobasrah.edu.iq (corresponding author)

Zaid Ameen Abduljabbar
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq | Department of Business Management, Al-Imam University College, 34011 Balad, Iraq | Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, 518000, China
zaid.ameen @uobasrah.edu.iq

Vincent Omollo Nyangaresi
Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya | Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tami lnadu, 602105, India
vnyangaresi@jooust.ac.ke

Received: 7 August 2024 | Revised: 26 August 2024 | Accepted: 29 August 2024

ABSTRACT

Authentication of vehicles and users, integrity of exchanged messages, and privacy preservation are essential features in VANETs. VANETs are used to collect information on road conditions, vehicle location and speed, and traffic congestion data. The open exchange of information within VANETs poses serious security threats. Furthermore, existing schemes have higher communication and computational costs, making them incompatible with resource-constrained VANET applications. This study proposes a multifactor authentication and privacy-preserving security scheme for VANETs based on blockchain and fog computing to meet all these requirements. The proposed scheme uses fingerprints and Quick Response (QR) codes as a multifactor to authenticate vehicle users and fog-cloud computing techniques to reduce the computational burden on RSUs and improve service quality and resilience. Additionally, the scheme synchronizes a consistent ledger across all RSUs using blockchain technology to store and distribute vehicle authentication statuses. Through a thorough comparison with relevant current protocols, the scheme shows a much-reduced computing expense and communication burden in situations with high vehicle density within a timeframe of 6.3846 ms and 544 bytes for communication costs. In addition, the proposed scheme demonstrates a successful balance between efficacy and complexity, protecting confidentiality, anonymous authentication, and ensuring integrity and conditional tracking. Formal and informal security analysis showed that the proposed scheme is more reliable, practical, and secure against many hostile attacks, such as modification attacks, 51% attacks, Sybil attacks, and MITM attacks.

Keywords-VANET; blockchain; fog computing; fingerprint; QR code; anonymous authentication; security and privacy; integrity

I. INTRODUCTION

The smart city structure and its many characteristics have captivated worldwide interest due to its rapid adoption [1]. This may be accomplished by implementing intelligent systems, such as healthcare, transportation, waste management, etc., with the aid of new technology. Technological advances such as the Internet of Things (IoT), cloud computing, and wireless sensor networks are examples of progress in technology [2]. The concept of a smart city is gradually becoming a reality, and these facilities are enhancing the standard of living of individuals. Undoubtedly, smart cities and their apps have supplanted conventional systems to provide efficient and opulent amenities, although they nevertheless encounter their own set of obstacles. It is becoming more challenging to handle expanding intercity traffic due to its significant magnitude. Consequently, Intelligent Transportation Systems (ITS) are used to facilitate communication between vehicles and enhance road safety [3-5]. Managing traffic challenges, such as safety, control, and congestion, has become an essential and rapidly advancing technology. VANETs are autonomous, infrastructure-less mobile networks that use vehicles as mobile nodes. VANETs have three components: the Trusted Authority (TA), the On-Board Unit (OBU), and the Roadside Unit (RSU). In a VANET [6, 7], the OBU, which is known as a tamper-resistant device, is located within the vehicle and holds vehicle-specific information. This includes the results of several cryptographic operations and the vehicle's identification. The TA stores data for all vehicles and RSUs. OBU and TA may establish efficient communication through RSUs. A VANET encompasses both V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) communications [8, 9]. Within the context of V2V communication, vehicles share information within a designated range of RSUs. On the other hand, in V2I communication, vehicles can communicate information with RSUs. Ensuring the security and privacy of real-time information exchanged between a TA and moving vehicles using wireless communication has become a significant contemporary concern [10]. Enhanced security and privacy considerations require the implementation of more robust and reliable authentication infrastructures to ensure safe V2I connections [11]. Numerous academics have proposed multiple authentication techniques for secure and resilient V2I connections. However, most of these schemes are susceptible to a range of security concerns. Therefore, it is essential to provide a lightweight and robust authentication protocol to address security and privacy concerns in VANETs [12]. A genuine automobile user can connect to the RSU over an unsecured channel, which is susceptible to several security risks. Most of the schemes incur high computational and communication costs for communication. In addition, authentication of the legitimate vehicle user is overlooked in most of the proposed schemes, which leads to very high risks, especially in highly security-critical locations such as gas, gasoline, and oil tankers, as well as money transport vehicles, which should only be driven by authorized persons.

As the number of vehicles increases rapidly, the need to process associated data increases as well. For example, traffic route aggregation and traffic detection require real-time traffic data produced by vehicles. Thus, to collect and process the data, cloud computing is introduced into the architecture of traditional VANETs. However, cloud computing servers are far from vehicles, leading to high energy consumption and high latency [13]. To overcome these drawbacks, fog technology has been introduced to build vehicular network models. In fog-based vehicular networks, fog nodes with certain computing and storage capabilities are distributed at the edge of the network and can process the data generated by vehicles in a more timely manner. A fog node can be any device, such as an RSU or a powerful server. Fog-based VANETs have many distinctive features, including low latency, location awareness, support for more end nodes, and a wide geographical distribution [14].

A literature review showed that no attention has been paid to verifying the driver (user) before beginning the vehicle verification phase. It is important to recognize that the driver and his conduct serve as the foundation for both internal and external attacks. Many schemes tend to overlook this crucial aspect, which could have catastrophic consequences, particularly in locations with stringent security measures, such as oil and gas fields, and banks, as well as in vehicles that convey prominent individuals, such as heads of state. Moreover, previous schemes could not provide trustworthy data verification for carpooling records in the event of a central cloud server failure or data manipulation. A cloud server failure would result in the loss of all carpooling records. Furthermore, since a vehicle will pass through several RSUs throughout its trip, it must complete the authentication procedures with each consecutive RSU it encounters. Performing authentication at every RSU might result in repetitive calculations, leading to unnecessary additional workload and reduced effectiveness. Consequently, blockchain technology has recently been introduced to the VANET environment, because it offers security, performance, anonymity, decentralization, and immutability features [15, 16]. Specifically, public information such as public keys, aliases, and certificates can be managed through smart contracts on a blockchain, so that authentication and revocation can be effectively performed. In addition, during authentication, it only needs to retrieve public information from the blockchain and does not involve storing new data on the blockchain. Therefore, it can be used to implement user self-authentication and strengthen access control.

Proof of Work (PoW) is a frequently employed consensus technique in several blockchain networks. Its purpose is to verify transactions and add new blocks to the chain [17]. The PoW concept was proposed to ensure network security and reduce the risk of double spending. The PoW mechanism requires miners to solve intricate mathematical puzzles, called hashes, to verify transactions and append new blocks to the chain. PoW algorithms intentionally design the hash function to be computationally challenging, requiring a substantial amount of computing prowess to successfully solve the challenge and append a block to the chain. Miners compete to solve the challenge [18], rewarding the first miner with newly created Bitcoin. The inherent complexity of solving the hash problem provides the technique's security, making it prohibitively costly for an attacker to attempt network control. To carry out an assault, the perpetrator must have dominion over a substantial percentage of the network's processing power, often referred to as the hash rate. This is referred to as a 51% attack, which poses significant challenges due to its massive resource requirements.

This study proposes a new secure, lightweight, multifactor privacy-preserving authentication based on Blockchain and a fog computing scheme for VANETs. Fingerprints are used as the first stage, and then a QR code is used to verify the user, as validating the user in the first place maintains the system as a whole. Additionally, high-security locations require user verification as a first stage. The proposed scheme utilizes the Ethereum platform to employ blockchain technology, including the PoW consensus mechanism. The use of the Ethereum blockchain in a VANET provides transparency and addresses the issues of IoT devices by providing certifiable and unchangeable messages of any action that occurs. With cryptographic features, the Ethereum blockchain can mitigate transmission snooping and interruptions. On the other hand, blockchain technology has additional overhead that can be addressed by fog computing.

The primary motivation for this research stems from the examination of existing VANET authentication protocols, which revealed several issues, including a lack of vehicle user authentication, high computing power requirements, difficulties with multifactor authentication policies, and potential vulnerabilities to various attacks. To ensure that vehicle networks distribute data reliably and efficiently, communication delays must be reduced. To address these problems, a secure and efficient multifactor authentication scheme was proposed for VANETs based on blockchain and fog computing. The main contributions of this study are:

- Proposes a new and efficient authentication scheme for VANETs that ensures privacy and security. The scheme uses blockchain and fog computing technologies, as well as multifactor authentication for vehicle user verification.
- The proposed scheme is specifically designed for secure implementation in high-risk environments, including bank and police cars, as well as vehicles engaged in the transfer of sensitive products such as oil and gasoline.
- Proposes an innovative schema that ensures safe and privacy-conscious authentication by using fingerprint recognition and QR code verification to authenticate the legality of vehicle users every time a vehicle is started.

II. RELATED WORK

The pace of technological advancements is fast accelerating and there has been a growing focus on mutual authentication, security, and privacy in the VANET environment in recent years. There are many privacy and security concerns in VANETs. VANETs utilize wireless communication. Therefore, safeguarding the uninterrupted transmission of classified data is of utmost importance. In recent times, many authentication systems have been introduced.

In [19], the first Public Key Infrastructure (PKI-based) conditional privacy protection authentication solution was introduced to enhance vehicle communication security using anonymous certificates. However, to manage a large number of certificates, this approach requires the participation of a Certification Authority (CA). This approach is complicated to administer, requires ongoing certificate revocation and upgrades, and incurs computational and storage costs. In [20], edge computing and identity group signatures were used to develop an authentication framework for VANETs that allows both V2V and Vehicle-to-RSU authentication. To detect and punish malevolent vehicles, the method includes a mechanism for identification and revocation. However, this technique is prone to the key escrow issue, as the TA needs to provide secret keys for vehicles and RSUs, resulting in a lot of bilinear pairing operations and significant overhead. This approach also has to contend with issues such as high computing complexity and susceptibility to attacks that compromise Tamper-Proof Devices (TPDs), as it cannot withstand DoS attacks or achieve location privacy.

In [21], a certificateless Conditional Privacy-Preserving Authentication (CPPA) system was proposed that provided efficient data transfer and demonstrated security inside the random oracle concept. Although the signature and verification costs were relatively low, this technique did not fulfill the transmission overhead criteria for sending traffic emergency alerts. The transmission overhead still exceeded the requirements of the Internet of Vehicles (IoV) [21]. Two separate certificateless authentication techniques for VANETs based on Elliptic Curve Cryptography (ECC) were developed. Although these schemes fulfill some criteria, they do not provide sufficient support for independence and do not ensure the confidentiality of a vehicle's location since the pseudonym of the vehicle might be linked, compromising its anonymity. In [22], a new approach to creating pseudonyms for automobiles was introduced, in which all OBUs had a single pseudonym, called the "pseudonym root," and produced individual pseudonyms based on this root. Therefore, the OBU did not need an expansion of its storage. Furthermore, this system did not use the bilinear pairing method, leading to an increased computing burden. Additionally, the system lacked a certification revocation listing, which resulted in additional computational and transmission costs. This method had a streamlined process of mutual validation among all parties involved and provided enhanced anonymity to safeguard privacy and withstand frequent attacks.

In [23], a trust management paradigm was proposed to ensure both accuracy and security criteria. The inherent ambiguity of the data was considered to enhance precision. The system integrated both direct and indirect trust associated with the cars utilizing Dempster-Shafer Theory (DST). The precision of trust assessment was enhanced by using contextual information to differentiate the specific communication types targeted by hostile vehicles. The messages analyzed included Lane Change Warning (LCW), Stopped Vehicle Warning (SVW), and Emergency Brake Warning (EBW). In addition, further functions were used to improve the security of the model and improve the accuracy of trust evaluation. The actions of rewarding, forgetting, punishing, and forgiving were used in this scenario. However, this method could not provide privacy, scalability, or responsiveness.

In [24], the efficiency of authentication was improved by keeping information on the blockchain and mandating pseudonym changes through TAs. In [25], vulnerabilities were detected in the system presented in [26], allowing the deduction of confidential parameters and vehicle paths. B-DSPA [25] is a privacy-preserving system that uses smart contracts to record accidents and conduct forensic investigations to improve safety. In [27], an intelligent method was presented to provide secure communication in VANETs without relying on a TA. Smart contracts were used on a publicly accessible blockchain, where RSUs established a network. These contracts facilitated the generation of cryptographic keys for safe communication without requiring a TA. This method verified that the keys used for communication were associated with registered automobiles, although causing a little delay. Furthermore, the Blockchain process consisted of four distinct steps: car registration, key registration, RSU verification, and RSU key registration. However, there is a potential for danger while engaging in communication, as an individual can intercept and manipulate communications, resulting in MITM attacks [28].

In summary, several schemes have been proposed for the current VANET challenges. However, the vast majority are vulnerable to a variety of security attacks, including replay, vehicle impersonation, RSU impersonation, MITM, and anonymity attacks. This study proposes an anonymous authentication technique that offers enhanced security for users, guarantees message integrity, and minimizes computational complexity. This is achieved by strategically using the ECC and a unique integration of blockchain and fog computing. The suggested scheme implements a fingerprint-based and QR code approach to greatly enhance the physical security of vehicles. This approach also uses blockchain and fog computing to address the challenges associated with privacy-sensitive anonymous authentication in VANETs. Using this approach, OBUs would eliminate the need to reauthenticate while transitioning between RSUs. Furthermore, it satisfies most security requirements, including scalability, authentication, availability, data integrity, and traceability. The proposed scheme demonstrated resilience against the most recent forms of attacks, such as modification attacks, reboot attacks, Sybil attacks, and 51% attacks.

III. PROPOSED SCHEME

This study proposes a privacy-preserving, multifactor authentication scheme to establish secure communication within VANETs. This approach integrates fog computing principles with blockchain technology. The proposed scheme uses a fingerprint and QR code to authenticate vehicle users and comprises five main stages: setup, registration, login and anonymous authentication, secure exchange message, and revocation phase.

A. Initialization Phase

This phase involves the TA to generate the initial system parameters and register the remaining entities of VANETs.

- Step 1: The TA initially chooses the finite elliptic curve $y^2 = x^3 + ax + b \ (mod\ q)$, where q is a large prime number and a , $b \in$ finite field ($\mathbb{F}p$). P and Q are points on this elliptic curve.
- Step 2: The TA chooses τ and δ at random from the multiplicative group Z_q^*, where q is the size of the group, and chooses $h{:}\{0,1\}^*$ as the hash function.
- Step 3: The TA determines its private key (T_{PR}) at random, $\tau \in Z_q^*$, computes its relevant public key as $T_{PU} = \tau P$ and the verification key (T_V) as $T_V = \delta P$.
- Step 4: The TA publishes important parameters (T_{PU}, T_V, P, Q, h , $e(P,Q), q$) to all RSUs, OBUs, and fog nodes.

B. Registration Phase

1) Vehicle User and OBU Registration Phase

During the registration process, every i-user provides authentic credentials on both their own identity and their vehicle. The registration steps for each i-user (U_1, U_2,… , U_n) are in the following order:

- Step 1: $U_i \rightarrow TA$: Each user (U_1, U_2,… , U_n) submits legitimate credentials encompassing personal and vehicle details ($ID_i, Phno_i, Add_i$) and vehicle (VN_i, VID_i) to the regulatory body TA.
- Step 2: $U_i \rightarrow TA$: Scans and digitizes the users' fingerprints (FP_i) to ensure the highest level of privacy and security.
- Step 3: TA: The authentication procedure implemented by TA depends on the selection of a critical parameter $\rho_i \in Z_q^*$. This value is crucial in the computation of the first authentication ID (A_{FID}) using A_{FID}= $\rho_i(\tau + \delta)$.
- Step 4: After obtaining the real identities of users, TA assigns dummy vehicle IDs (D_{IDV}) from Z_q^* to enhance the secrecy of data transfer.
- Step 5: TA: To improve security, TA uses $A_{SID} = h\ (D_{IDV} \times A_{FID})$ to calculate the second authentication ID (A_{SID}), fortifying the relationship between D_{IDV} and A_{FID} for reliable authentication.
- Step 6: : The TA generates a unique QR code (QRV_i) for every user (U_i). The complete user-specific data ($U_i, Phno_i$, ID_i, Add_i, FP_i,VN_i, and VID_i) are included in this QR code.
- Step 7: The TA meticulously chooses a random number ∈ Z_q^* . The TA then computes QRV_i using the chosen cryptographic hash function h, as follows: $QRV_i = h(\eta(U_i \parallel Phno_i \parallel ID_i \parallel FP_i \parallel Add_i \parallel VN_i \parallel VID_i\ ))$, and then generates the symmetric key (SK_i) using the AES algorithm.
- Step 8: TA → OBU_i: The resulting FP_i and SK_i are securely transmitted to the respective OBU and QR to the user.
- Step 9: TA → U_i : Concluding the authentication loop with enhanced privacy and security protections, TA securely provides ρ_i, A_{FID}, and A_{SID} to the OBU.
- Step 10: TA →Blockchain: To ensure process integrity and record it, TA stores D_{IDV}, QRV_i, FP_i, SK_i, and A_i on the blockchain when $A_i = e(\mathrm{P},\mathrm{Q})^{\rho_i}$.

2) RSU Registration Phase

- Step 1: TA → RSU: The RSU registration begins with the calculation of first verifications, which are denoted as an $ID(V_{FID}) = \left(\frac{1}{\tau+\delta}\right) Q$ for every RSU.
- Step 2: To improve the security and confidentiality of RSU identifiers, the TA strategically chooses a dummy ID ($D_{IDR} \in Z_q^*$). The second verification ID (V_{SID}) is then calculated using the formula $V_{SID} = h(D_{IDR} \times V_{FID})$, which allows it to combine the dummy ID with the previously calculated V_{FID}.
- Step 3: TA → RSU: After the registration is successfully finished, the TA safely saves the resulting verifications ID_i (V_{FID} and V_{SID}) along with the parameter δ in the RSU.

C. Login and Anonymous Authentication Phase

1) User and OBU Login and Anonymous Authentication Phase

This phase begins when the user enters the vehicle and initiates the vehicle user authentication sequence. Figure 1 shows the user validation process, illustrating the steps involved in verifying users' identities and authorizations within the scheme.

- Step 1: When the driver enters the vehicle, he touches the fingerprint scanner on the dashboard to start the engine. The user's fingerprints are captured by this scanner (TFP_i).
- Step 2: The fingerprints of the driver (TFP_i) are compared to those stored in the OBU (FP_i). A successful match allows the vehicle to start operating others go to step 3.
- Step 3: Present the QR code to the OBU scanner to acquire QRV_i.
- Step 4: The OBU efficiently chooses a random element $g_i \in Z_q^*$ to compute the value of $Rh_i = (g_i, QRV_i, TFP_i)$.
- Step 5: Rhk_i is encrypted using $Rhk_i = (g_i \oplus SK_i)$.
- Step 6: Subsequently, Rh_i, Rhk_i, and, FP_i are submitted to the RSU, after which the RSU transmits them to the blockchain.
- Step 7: The blockchain side compares based on FP_i. If it matches, proceed to the next step, else turn off the vehicle.
- Step 8: The blockchain sends an SMS to the owner with the vehicle's location, requesting their consent to turn the vehicle on or not.
- Step 9: After the user has been authenticated, the OBU initiates the OBU authentication process and sends ($\rho_i P$) to the RSU.
- Step 10: Following that, the RSU transmits $D_{IDR}P$ to the OBU.
- Step 11: The OBU computes k as $k = \rho_i \mathrm{D}_{\mathrm{IDR}} P$, and the RSU computes k' by $k' = D_{IDR}\, \rho_i P$ at the same time.
- Step 12: OBU calculates k_1 as $k_1 = A_{FID} \oplus h(k)$ and then sends k_1 to the RSU.
- Step 13: RSU calculates the value of A_{FID} by $A_{FID} = k_1 \oplus h(k')$.
- Step 14: After obtaining A_{FID}, RSU computes $A_i = e(A_{FID}P, V_{FID})$ and subsequently submits a request to the blockchain to retrieve A_i. The goal is to minimize re-authentication time and ensure authenticity without any outside assistance.
- Step 15: Once A_i is obtained from the blockchain and confirmed its match, $ARV_i$is calculated using the formula $ARV_i = (D_{IDR}, D_{IDV}, h(D_{IDV}, D_{IDR}))$.
- Step 16: To reduce the number of re-authentications required, the ARV_i is shared with all RSUs.
- Step 17: The RSU calculates k_2 by $k_2 = A_{FID} \oplus D_{IDR}$ and then sends k_2 to the OBU.
- Step 18: When the OBU receives k_2, it decrypts it to get the D_{IDR} using $D_{IDR} = A_{FID} \oplus k_2$.

2) RSU Login and Anonymous Authentication

The RSU offers location-based information to the vehicles within its coverage region. Every vehicle in VANET needs to verify the authenticity of the RSU to have confidence in the information it provides. In this process:

- Step 1: RSU selects $z_i \in Z_q^*$ and calculates the following parameters:
  1. $r_i = z_i P$
  2. $\omega_i = h(A_{FID} \times T_{PU})$
  3. $\vartheta_i = (z_i + \omega_i \delta) mod\ q$
- Step 2: Next, it computes j_1 as $j_1 = D_{\mathrm{IDR}} \oplus \vartheta_i$ and j_2 as $j_2 = A_{SID} \oplus \omega_i$.
- Step 3: Then, the RSU transmits r_i, j_1, and j_2 to the OBU.
- Step 4: After receiving r_i, j_1, and j_2, the OBU proceeds to retrieve ϑ_i' and ω_i' as a preliminary step. It then proceeds to verify $\vartheta_i' P = r_i + \omega_i' T_V$. Once this condition is met, the OBU will accept the RSU and get location-based information.

D. Secure Exchange Message Phase

Vehicles can communicate and distribute traffic data, including many features such as traffic patterns, weather, collisions, and gridlock. After receiving this information, other vehicles could be aware of the problem beforehand and help create a safer driving environment.

- Step 1: OBU chooses a $\ell_i \in Z_q^*$ and calculates important parameters, such as $B_1 = \ell_i T_{PU}$, $C_1 = \vartheta_i T_{PU}$, and $F = B_1 + C_1$.
- Step 2: The OBU chooses a random element $n_i \in Z_q^*$ and computes $S_i = n_i\, T_{PU}$.

- Step 3: Calculate μ_i by $\mu_i = h(ms_i \times S_i)$ and then ν_i using $\nu_i = \mu_i(n_i + \ell_i + \vartheta_i) \bmod q$.
- Step 4: Next, the OBU assigns $Sig_i = (S_i, ms_i)$ as a message's signature. The unique signature's distinctive character will maintain the message's integrity. The immutable and untampered nature of the signature ensures its integrity.
- Step 5: The timestamp discrepancy (ΔT) is calculated by T_r - T_s, where T_s represents the current timestamp of message transmission and T_r denotes the timestamp upon receiving the message. This option represents the acceptable time difference between T_s and T_r.
- Step 6: OBU_i /OBU_j or RSU_i: Transmit the OBU (ν_i, T_s, ms_i, Sig_i, F, D_{IDV}, and Rc_i) to the other OBU/RSU.
- Step 7: The rejection counter Rc_i is used to assess whether the message should be accepted or rejected. Each time the vehicle refuses a message, the counter increments by one until it reaches the maximum rejection threshold of 3. Then, the vehicle is blocked from transmitting messages.
- Step 8: The OBU/RSU verifies the rejection counter (Rc_i). If the value of Rc_i is equal to 3, then block OBU, otherwise, it proceeds to the next phase.
- Step 9: Subsequently, the timestamps T_r - T_s <= ΔT undergo thorough validation. Afterward, a careful calculation of μ_i' using the formula $\mu_i' = h(ms_i \times S_i)$ is performed. This validation entails examining the consistency of the equation $\nu_i T_{PU} = \mu_i(S_i + \mathrm{F})$. The message ($ms_i$) is authenticated by adhering to these strict conditions. Any variation leads to rejection, indicating that the message has become outdated beyond the allowed limit ΔT.
- Step 10: After that, the value of Rc_i is increased by one unit ($Rc_i = Rc_i + 1$) and then evaluate it to see if it equals the threshold of three. When the counter reaches three, the scheme advances to the next phase and inhibits the OBU from delivering messages. Alternatively, the OBU proceeds with the process of transmitting the messages.

E. Revocation Phase

The proposed scheme ensures that the revocation procedure swiftly addresses any abnormal or harmful behaviors shown by vehicle users after authentication. The TA commences the process of revocation in response to complaints from users of neighboring vehicles. After the authentication procedure is over, if a vehicle participates in deceitful behavior by spreading misleading information to others, the OBUs increase the RC_i of the malevolent OBUs each time they engage in such deceptive actions. After that, the TA promptly implements remedial measures to remove the vehicle from the VANET system, thereby preventing any further misuse. The revocation phase comprises a meticulously organized series of steps.

- Step 1: Assume that a vehicle sends a disingenuous message (ms_m^*), represented as (ν_m, ms_m^*, T_s, Sig_i, F, D_{IDV}, and $\mathrm{RC_m}$), to other vehicles.
- Step 2: When surrounding vehicles discover this false information, they report it by increasing the RC_m and transmitting (ν_m, ms_m^*, T_s, Sig_i, F, D_{IDV}, and $\mathrm{RC_m}$) to the TA via the RSU.
- Step 3: The TA must collect reports from a minimum of three OBUs. These reports should include information indicating that the RC_m has reached three.
- Step 4: Afterward, the TA revokes the authorization of the specific vehicle user by sending $(D_{IDV}, h(D_{IDV}, \delta))$ to all RSUs.
- Step 5: Furthermore, the TA also communicates with a police station, sharing the vehicle user's identity (ID_m) as well as the vehicle's VN_m, VID_m to perform a thorough inquiry and investigation.
- Step 6: Each RSU validates the information it receives by calculating $Rv = h(D_{IDV}, \delta)$. If Rv matches the received $h(D_{IDV}, \delta)$, the relevant D_{IDV} is included in the block list shared across all RSUs.
- Step 7: As a result, the OBU linked to D_{IDV} is prohibited from any further communications. This stringent revocation procedure ensures the integrity of the VANET system by promptly isolating and restricting compromised entities.

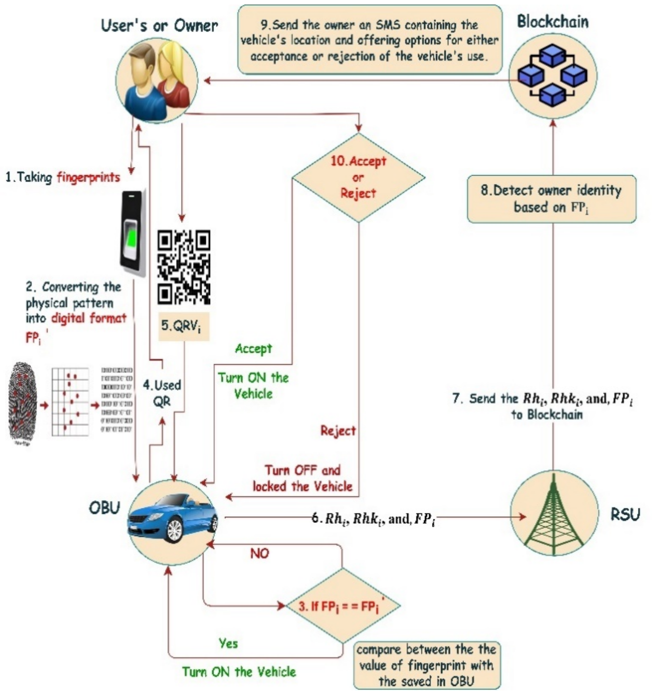

User's or Owner
9.Send the owner an SMS containing the vehicle's location and offering options for either acceptance or rejection of the vehicle's use.
Blockchain
1.Taking fingerprints
10.Accept or Reject
8.Detect owner identity based on FP_i
2. Converting the physical pattern into digital format FP_i'
5.QRV_i
Accept
Turn ON the Vehicle
4.Used QR
7. Send the Rh_i, Rhk_i, and, FP_i to Blockchain
Reject
Turn OFF and locked the Vehicle
OBU
6. Rh_i, Rhk_i, and, FP_i
RSU
NO
3. If $FP_i == FP_i'$
Yes
Turn ON the Vehicle
compare between the the value of fingerprint with the saved in OBU

Fig. 1. The vehicle user authentication phase.

IV. SECURITY ANALYSIS

A. Informal Security Analysis

1) Modification Attacks

To carry out a message modification attack, the attacker must alter the message's content. The vehicle user transmits the parameters $(\nu_i,\ ms_i,\ T_s,\ Sig_i, \text{F}, D_{IDV}, and\ Rc_i)$ to the other vehicle. To send a fraudulent message, one must alter the message's substance, known as ms_i. However, when the message content is altered, the end user not only verifies the message content but also assesses the value of ν_i, which is calculated using $\nu_i = \mu_i(n_i + \ell_i + \vartheta_i) mod\ q$, where μ_i is defined as $\mu_i = h(ms_i \times S_i)$. Furthermore, the vehicle user calculates the value of S_i using $S_i = n_i T_{PU}$, where n_i is a randomly selected number and belongs to the set of non-zero integers modulo q. As a result, the intricacy of determining the random number is associated with the Discrete Log Problem (DLP). Therefore, determining the values of S_i and μ_i is challenging. Therefore, the value of ν_i transmitted by the verified vehicle user is immutable. The offered technique interconnects both the message ms_i and ν_i, protecting against a message modification attack.

2) Implantation Attack

The protection of vehicle communication networks is of utmost importance, especially when considering impersonation attacks. In this situation, malevolent actors seek to impersonate authorized vehicle users or RSUs, to obtain access to important credentials. To counteract this danger, the suggested protective measure entails a sequence of safe transactions. Upon entering the car, an authenticated user must provide either a fingerprint or a QR code for an OBU scan. Employing a fingerprint authentication method ensures that the user remains impervious to impersonation threats. When using a QR code, the owner's consent is required. After that, OBU selects the value of g_i, and $Rh_i = (g_i, QRV_i, TFP_i)$ is computed. Subsequently, the OBU calculates $Rhk_i = (g_i \oplus SK_i)$ and transmits Rh_i and Rhk_i securely to the RSU. Moreover, once the vehicle user enters the coverage area of the RSU, the authorized user transmits $\rho_i P$ to the RSU. The value of ρ_i and the QR code are decided by the TA, and they are transferred securely and offline to an authenticated vehicle user, ensuring the vehicle user's authentication. In response, the RSU transmits a fabricated identity, $D_{IDR}P$, that the TA has safely selected. Consequently, it is challenging for an opponent to compromise the integrity of the TA to acquire the necessary authentication information. Therefore, the proposed approach offers protection against impersonation attacks.

3) MITM Attack

A MITM attack presents a substantial security threat when an unauthorized entity covertly intercepts, alters, or broadcasts communication vehicles and roadside equipment. This kind of attack has the potential to jeopardize the integrity and confidentiality of important information transferred inside the network. A prospective attacker can intercept and modify communications related to route information, traffic conditions, or safety alarms, generating potentially dangerous driving situations. If a malicious node intercepts the packet containing $(\nu_i,\ ms_i,\ T_s,\ Sig_i, \text{F}, D_{IDV}, \text{and}\ Rc_i)$ that is sent between OBU_i and OBU_j, the MITM attacker will attempt to intercept the packet and modify it to include $(\nu_i,\ ms_i^*,\ T_s,\ Sig_i, \text{F}, D_{IDV}, and\ Rc_i)$. The scheme employs a digital signature using Sig_i, and the end user verifies both the message content and the value of ν_i. The value of ν_i is calculated using the formula $\nu_i = \mu_i(n_i + \ell_i + \vartheta_i)\ mod\ q$, where μ_i is obtained by $\mu_i = h(ms_i \times S_i)$. In addition, the value of S_i is calculated using the formula $S_i = n_i\ T_{PU}$, where n_i is a randomly selected number by the OBU from the set of integers Z_q^*. Therefore, the complexity of identifying the random number involves the DLP, widely recognized as a difficult problem to resolve. Consequently, determining the values of S_i and μ_i is challenging. Therefore, it is impossible to alter the value of ν_i sent by the verified vehicle user. Both the messages ms_i and ν_i are interconnected, and the proposed approach offers protection against a MITM attack.

4) DoS Attack

In this attack, a malicious vehicle can forge and broadcast a large number of invalid messages to use up the vehicle's computational resources, potentially dropping legitimate messages. The proposed approach involves the use of pseudonyms (D_{IDV}, D_{IDR}), by both the OBU and RSU throughout their V2V and V2I connections, guaranteeing their legitimacy as users. This is a common occurrence in any message exchange that includes ν_i, ms_i^*, T_s, Sig_i, F, D_{IDV}, and RC_i. However, if one of the users' behaviors changes, malicious entities can be promptly identified and removed using RC_i. When the receiving OBUs discover these deceptive messages, they increase the RC_i and send important information $\nu_i,\ ms_i^*,\ T_s,\ Sig_i, \text{F}, D_{IDV}, and\ RC_i$ to a TA using RSUs. Additionally, the scheme will limit the malicious user to forging a maximum of nine messages. After that, the scheme will revoke the entitlement.

5) 51% Attack

A 51% attack in a blockchain network occurs when a single entity gains control over more than 50% of the network's mining power, granting it the ability to modify transactions. A decentralized network prevents such attacks, ensuring that no single entity can control the network's computational resources. To execute such an attack, the attacker needs to possess more than 50% of the overall hashing power. The ability to thwart a 51% attack is contingent upon the degree of decentralization inside the network, wherein no single entity holds the bulk of the hashing power.

6) Sybil Attacks

In the proposed scheme, the vehicles use pseudonyms (D_{IDV}, D_{IDR}) in their V2V and V2I communications, ensuring the anonymity of their identities. This is done in every conversation involving ν_i, ms_i^*, T_s, Sig_i, F, D_{IDV}, and Rc_i. Nevertheless, if a malicious vehicle is detected, the TA can expose the real identity of the vehicle, which is hidden behind its dummy identity. An effective security system is implemented to prevent the dissemination of misleading messages (ms_i^*) that consist of data elements, such as ν_i, ms_i^*, T_s, Sig_i, F, D_{IDV}, and Rc_i. Upon detecting these fraudulent communications, the receiving vehicles verify their legitimacy and transmit relevant information $(Sig_i, ms_i^*, T_s, D_{IDV}$, and $Rc_i)$ to a TA via RSUs. The TA expeditiously enforces a crucial security measure by revoking the permissions and privileges of the vehicle user associated with the unique identification (D_{IDV}). This scheme has integrity and privacy preservation for the VANET system at the same level and defends against the Sybil attack. It is an important factor to consider for research and development in this field. For example, the attacker may create the illusion of a vehicle (MV) smoothly passing through a traffic congestion area, impacting the judgment of other drivers. This condition can lead to inaccurate decisions, potentially causing more congestion or even vehicle pile-ups, posing significant threats to the safety of drivers and passengers.

From an integrity perspective, in each communication encompassing v_i, ms_i^*, T_s, Sig_i, F, D_{IDV}, and Rc_i, the vehicles employ pseudonyms (D_{IDV}, D_{IDR}) in their V2V and V2I communications, ensuring the anonymity of their identities. However, in the event of identifying a malicious vehicle, the TA can unveil the true identity of the vehicle behind its pseudonymous identity. A robust security system is established to thwart the spread of deceptive messages (ms_i^*) comprising data elements, such as v_i, ms_i^*, T_s, Sig_i, F, D_{IDV}, and Rc_i. When these false messages are detected, the receiving vehicles validate their authenticity and forward pertinent information ($Sig_i, ms_i^*, T_s, D_{IDV}$) to a TA through RSUs. The TA promptly implements a critical security action by withdrawing the rights and privileges of the vehicle user linked to the distinctive identifier ($\mathrm{D_{IDV}}$). Such an approach enhances the overall security and integrity of VANET communications, protecting against Sybil threats, making it a crucial consideration for research and development in this domain.

7) Spoofing Attacks

In a spoofing attack, an attacker attempts to create numerous fake identities by obtaining the ID of an i-node that the TA maps. However, the proposed identity management system based on blockchain technology prevents such activities from occurring. Each participant in the VANET (OBU or RSU) receives a unique and secure dummy identity (D_{IDV}, D_{IDR}) from the decentralized scheme, which securely stores inside the blockchain. Moreover, the identification of both genuine and false identities linked to an i-node poses a significant obstacle for prospective intruders. In addition, during V2V and V2X communication, the use of a signature ensures integrity and prevents any tampering of the information. Even if the attacker manages to intercept the communication, he is unable to alter its content without the knowledge of all parties involved.

8) Anonymity Authentication

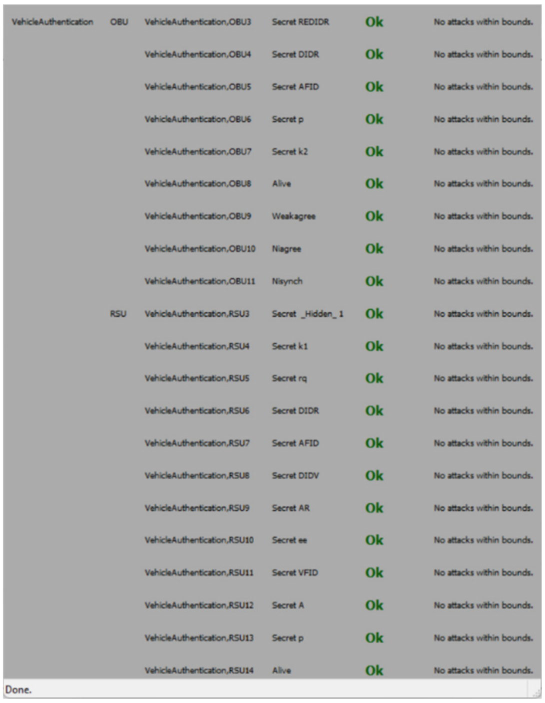
During the anonymous authentication process, only dummy identities are used for an OBU (D_{IDV}) or RSU (D_{IDR}). The TA provides these dummy IDs for vehicle users or RSUs during their first offline registration. Furthermore, the TA, OBUs, and RSUs transfer data using only dummy identities. The real identity of the OBUs is known only to the TA, thereby preventing attackers from counterfeiting pseudonyms. Furthermore, in the case of illegal OBUs found, only the TA can disclose the correlation between dummy identities and real identities. The RSU is capable of authenticating the OBU anonymously, without knowledge of the vehicle's real identity. Therefore, if an opponent captures the dummy identity, he will not have access to any information about the real identity. Therefore, the proposed approach ensures the preservation of privacy for both the vehicle user and the RSU.

9) Perfect Forward Secrecy

If a hostile entity acquires the private key (T_{PR}) of TA, it might attempt to leak the confidential parameters. However, this situation does not benefit the adversary, as ECC and the secret parameter v_i conceal all communications. Therefore, the proposed scheme can achieve flawless forward secrecy.

B. Formal Security Analysis with Scyther Tool

A security analysis using the Scyther tool showed that the proposed scheme can attain higher levels of security and privacy than alternatives. The proposed scheme was implemented using the SPDL language. The results were then shown for the cases of $Automatic\ Claim$ and $Verification\ Claim$. Figure 2 displays the Scyther results of the proposed scheme.



VehicleAuthentication	OBU	VehicleAuthentication,OBU3	Secret REDIDR	Ok	No attacks within bounds.
		VehicleAuthentication,OBU4	Secret DIDR	Ok	No attacks within bounds.
		VehicleAuthentication,OBU5	Secret AFID	Ok	No attacks within bounds.
		VehicleAuthentication,OBU6	Secret p	Ok	No attacks within bounds.
		VehicleAuthentication,OBU7	Secret k2	Ok	No attacks within bounds.
		VehicleAuthentication,OBU8	Alive	Ok	No attacks within bounds.
		VehicleAuthentication,OBU9	Weakagree	Ok	No attacks within bounds.
		VehicleAuthentication,OBU10	Niagree	Ok	No attacks within bounds.
		VehicleAuthentication,OBU11	Nisynch	Ok	No attacks within bounds.
	RSU	VehicleAuthentication,RSU3	Secret _Hidden_ 1	Ok	No attacks within bounds.
		VehicleAuthentication,RSU4	Secret k1	Ok	No attacks within bounds.
		VehicleAuthentication,RSU5	Secret rq	Ok	No attacks within bounds.
		VehicleAuthentication,RSU6	Secret DIDR	Ok	No attacks within bounds.
		VehicleAuthentication,RSU7	Secret AFID	Ok	No attacks within bounds.
		VehicleAuthentication,RSU8	Secret DIDV	Ok	No attacks within bounds.
		VehicleAuthentication,RSU9	Secret AR	Ok	No attacks within bounds.
		VehicleAuthentication,RSU10	Secret ee	Ok	No attacks within bounds.
		VehicleAuthentication,RSU11	Secret VFID	Ok	No attacks within bounds.
		VehicleAuthentication,RSU12	Secret A	Ok	No attacks within bounds.
		VehicleAuthentication,RSU13	Secret p	Ok	No attacks within bounds.
		VehicleAuthentication,RSU14	Alive	Ok	No attacks within bounds.

Done.

Fig. 2. Verification results in Scyther tool.

C. Performance Analysis

1) Computational Cost

The computational cost analysis of the proposed scheme was compared with others, such as [29], [30], [31], [32], [33], and [34]. Table II presents the computational analysis performed on different methods compared to the proposed scheme. Figure 3 shows that the proposed scheme exhibits superior performance based on the data provided. The MIRACL library [35] was used to simulate the scheme with anonymity authentication and conditional privacy protection, which is an integer and rational arithmetic cryptographic library. This library was employed to evaluate the performance of the proposed scheme and compare it to others, as described in [33, 36]. The method in [33, 37] was used to ascertain the duration of cryptographic procedures. Table I displays the execution time durations for cryptographic operations.

TABLE I. EXECUTION TIME OF FUNDAMENTAL CRYPTOGRAPHIC OPERATIONS

Operation	General Meaning	Time
Ex_{ecc-sm}	Time required for executing a scalar multiplication operation.	0.3218 ms
Ex_{ecc-pa}	Time needed for executing a point addition operation.	0.0024 ms
Ex_{bp}	Time taken to perform a pairing operation.	5.086 ms
Ex_{h}	Time taken for executing a one-way hash function operation.	0.001 ms
Ex_{e}	Time required for executing an exponentiation operation over the group G.	2.126 ms
Ex_{s}	Time taken for executing a symmetric encryption/decryption operation.	0.271 ms
Ex_{mtp}	Time taken to execute a MapToPoint hash operation associated with bilinear pairing.	0.0992 ms
Ex_{bp-sm}	Time taken to execute a scalar multiplication operation associated with bilinear pairing.	0.694 ms
Ex_{bp-pa}	Time taken to execute a point addition operation associated with bilinear pairing.	0.0018 ms
$Ex_{AES-enc}$	Time required for executing an encryption AES operation.	0.002 ms
$Ex_{AES-dec}$	Time required for executing a decryption AES operation.	0.001 ms

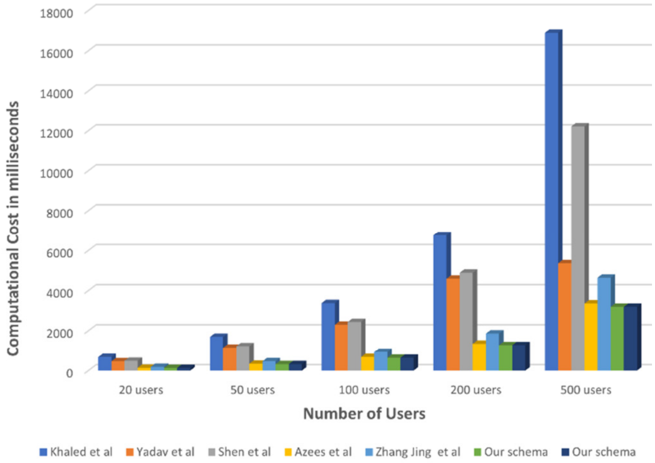


Fig. 3. Computational cost analysis of various schemes.

Comparing the computational cost of the proposed with the other schemes, it was found the scheme in [34] had a lower computational cost. This is due to the absence of a complete vehicle user verification phase, which exposes the system to risks such as car theft, identity theft, and other disasters.

2) Communication Cost

Communication cost is the total size of the message sent throughout the authentication process. For ECC, the size of p is 20 bytes, while for bilinear pairing, it is 64 bytes. Therefore, by multiplying the size of p by 2, the size of the elements in G and $G1$ are as 40 and 128 bytes, respectively. Furthermore, both the timestamp and identity should consist of 4 bytes, while the general hash function's output should consist of 20 bytes. Table III presents a comprehensive evaluation of communication expenditures for the proposed and other schemes.

TABLE II. DURATION FOR VERIFYING AUTHENTICITY ACROSS DIFFERENT METHODOLOGIES.

Scheme	Single OBU and Single RSU Authentication (ms)	*n* user's and *n* RSUs authentication (ms)
[29]	$3Ex_e + 2Ex_{bp-sm} + 5Ex_{bp} + 6 Ex_{mtp} \approx 38.88$	$3nEx_e + 2\text{n}Ex_{bp-sm} + 5\text{n}Ex_{bp} + 6\text{n}Ex_{mtp}$
[30]	$3Ex_e + 4Ex_{bp-sm} + 4Ex_{bp} + Ex_{bp-pa} + 6\ Ex_h \approx 24.4198$	$3nEx_e + 4\text{n}Ex_{bp-sm} + 3\text{n}Ex_{bp-pa} + 6\text{n}Ex_h$
[38]	$8Ex_{ecc-sm} + 4Ex_{bp} + 9Ex_h \approx 22.9274$	$8\text{n}Ex_{ecc-sm} + 4\text{n}Ex_{bp} + 9\text{n}Ex_h$
[32]	$2Ex_{bp} + 5Ex_{ecc-sm} \approx 11.781$	$(1+n)\ Ex_p + 5nEx_m$
[33]	$3Ex_e + 9Ex_{ecc-sm} + 3Ex_{ecc-pa} + 6\ Ex_h \approx 9.29$	$3\text{n}Ex_e + 9\text{n}Ex_{ecc-sm} + 3\text{n}Ex_{ecc-pa} + 6\text{n}Ex_h$
[34]	$4Ex_{ecc-sm} + Ex_{ecc-pa} + Ex_{bp} + 4Ex_h \approx 6.3796$	$4\text{n}Ex_{ecc-sm} + \text{n}Ex_{ecc-pa} + \text{n}Ex_{bp} + 4\text{n}Ex_h$
Proposed scheme	$4Ex_{ecc-sm} + Ex_{ecc-pa} + Ex_{bp} + 6Ex_h + Ex_{AES-enc} + Ex_{AES-dec} \approx 6.3846$	$4\text{n}Ex_{ecc-sm} + \text{n}Ex_{ecc-pa} + \text{n}Ex_{bp} + 6nEx_h + \text{n}Ex_{AES-enc} + \text{n}Ex_{AES-dec}$

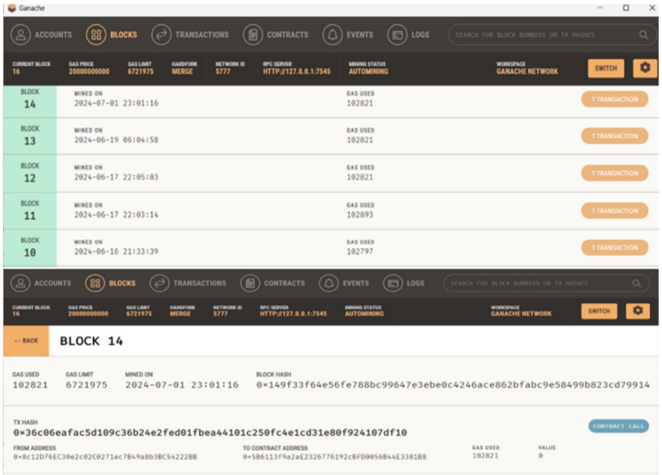
TABLE III. COMPARISON OF COMMUNICATION OVERHEAD

S.no	Scheme	Cost (Bytes)
1	[29]	592
2	[30]	824
3	[38]	184
4	[32]	868
5	[33]	380
6	[34]	408
7	Proposed scheme	544

According to Table III, the proposed scheme is more balanced between communication bytes and security goals than other related works. The other schemes have fewer communication bytes than the proposed one, primarily because they lack a user authentication phase. They rely solely on OBU and RSU authentication, neglecting to verify the user, leaving them vulnerable to vehicle theft and numerous attacks.

3) Gas Cost

Performance evaluation focused on the system's transaction latency, which is important for ensuring a smooth user experience in a secure VANET environment. The tests carried out on the Ganache platform yielded significant data on transaction processing time and related expenses. The latency was determined by the time it took for a transaction to be completed and added to a block, with an average reported time of 20 s. This statistic is essential for real-time applications and represents the level of responsiveness of the VANET system implementation on a blockchain network. On average, the transactions used about 102,821 gas units, as shown in Figure 4, demonstrating a balance between computational accuracy and temporal efficiency. For these particular transactions, the gas price was 0.000287 ETH, and there was no transfer of ETH value. This ensures minimal operating expenses, signifying a cost-effective design.



CURRENT BLOCK 16 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE GANACHE NETWORK

BLOCK	MINED ON	GAS USED
14	2024-07-01 23:01:16	102821
13	2024-06-19 06:04:58	102821
12	2024-06-17 22:05:03	102821
11	2024-06-17 22:03:14	102893
10	2024-06-16 21:33:39	102797

CURRENT BLOCK 16 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE GANACHE NETWORK

BLOCK 14

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
102821	6721975	2024-07-01 23:01:16	0×149f33f64e56fe788bc99647e3ebe0c4246ace862bfabc9e58499b823cd79914

TX HASH
0×36c06eafac5d109c36b24e2fed01fbea44101c250fc4e1cd31e80f924107df10

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×8c12D76EC30e2c02C0271ec7B49a8b3BC54222BB	0×5B6113f9a2aE2326776192cBFD0056B44E3381B8	102821	0

Fig. 4. Transaction gas cost usage overview.

V. CONCLUSIONS

This study proposed a privacy-preserving anonymous multifactor blockchain-based authentication scheme in fog-computing VANETs. It is essential to ensure the physical safety and privacy of users and vehicles, as well as to set up a secure communication system among various VANET components. By integrating fingerprint and QR code authentication, the proposed approach improved system efficiency and reduced potential threats from malicious vehicles and theft offenses. This ability makes it well-suited for use in high-security environments such as oil tankers, money transport, armored vehicles, and police cars. Sophisticated techniques were used to safely verify the authenticity of vehicle users, OBUs, and RSUs using ECC, SHA-256, and AES. Furthermore, the use of blockchain technology enhances decentralization and ensures the security and dependability of the sent data, thus mitigating susceptibility to attacks aimed at modulating communications. Integrating VANETs with fog services improves scalability and provides critical storage and computational assistance for a variety of VANET-based applications. The proposed scheme has a remarkable authentication time of 6.3816 ms for a single user, OBU, and RSU authentication, as well as communication costs of 544 bytes, ensuring a quick procedure. This showcases its exceptional efficacy compared to other systems in terms of computational expenses, communication expenses, and storage expenses. The distinguishing characteristic of the proposed scheme is its comprehensive verification of all system features, including vehicle user validation, which most existing systems lack. This approach demonstrates robustness against a diverse range of possible attacks, including MITM, impersonation, modification, Sybil, DoS, and 51% attacks. To expand the scheme for VANETs, future work will focus on implementing the simulation in the real world, addressing its primary limitations. In addition, the integration of emerging technologies such as 6G and satellite communications should be prioritized to improve the connection in rural areas. Furthermore, the authors plan to investigate the implementation of a blockchain-based vehicular network infrastructure for smart traffic services with a focus on handling large volumes of traffic data.

REFERENCES

[1] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, Jan. 2017, https://doi.org/10.1016/j.vehcom.2017.01.002.

[2] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A Lightweight Privacy-Preserving Authentication Protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, Sep. 2020, https://doi.org/10.1109/JSYST.2020.2991168.

[3] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, and M. A. Saleem, "Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12158–12167, Aug. 2021, https://doi.org/10.1109/TVT.2021.3118892.

[4] M. A. Al Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang, and J. Ma, "Two-Factor Privacy-Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14253–14266, Apr. 2024, https://doi.org/10.1109/JIOT.2023.3340259.

[5] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, Jul. 2019, https://doi.org/10.1109/JIOT.2019.2902840.

[6] F. B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay, and A. ur R. Khan, "Vehicular Ad Hoc Network (VANET) Localization Techniques: A Survey," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3001–3033, Jun. 2021, https://doi.org/10.1007/s11831-020-09487-1.

[7] M. A. Alazzawi, K. Chen, A. A. Yassin, H. Lu, and F. Abedi, "Authentication and Revocation Scheme for VANETs Based on Chinese Remainder Theorem," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Zhangjiajie, China, Aug. 2019, pp. 1541–1547, https://doi.org/10.1109/HPCC/SmartCity/DSS.2019.00212.

[8] I. M. Hassan and K. R. Hassan, "Vehicular Social Networks and Vehicular Ad-hoc Networks, Applications, Modelling Tools and Challenges: A Survey," *International Journal of Computer Applications*, vol. 176, no. 25, pp. 32–38, May 2020.

[9] R. Mohan, G. Prabakaran, and T. Priyaradhikadevi, "Seagull Optimization Algorithm with Share Creation with an Image Encryption Scheme for Secure Vehicular Ad Hoc Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 13000–13005, Feb. 2024, https://doi.org/10.48084/etasr.6786.

[10] W. Othman, M. Fuyou, K. Xue, and A. Hawbani, "Physically Secure Lightweight and Privacy-Preserving Message Authentication Protocol for VANET in Smart City," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12902–12917, Sep. 2021, https://doi.org/10.1109/TVT.2021.3121449.

[11] P. Wang and Y. Liu, "SEMA: Secure and Efficient Message Authentication Protocol for VANETs," *IEEE Systems Journal*, vol. 15, no. 1, pp. 846–855, Mar. 2021, https://doi.org/10.1109/JSYST.2021.3051435.

[12] M. A. Alazzawi, M. T. Almalchy, A. Al-Shammari, A. S. Al-Khaleefa, and H. M. Albehadili, "LSKA-ID: A lightweight security and key agreement protocol based on an identity for vehicular communication," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 4, pp. 784–796, Aug. 2023, https://doi.org/10.12928/telkomnika.v21i4.24388.

[13] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular Adhoc Network with Fog Computing," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Ottawa, Canada, May 2015, pp. 1202–1207, https://doi.org/10.1109/INM.2015.7140467.

[14] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of

Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5403–5415, Feb. 2020, https://doi.org/10.1109/TVT.2020.2977829.

[15] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain Based Data Integrity Service Framework for IoT Data," in *2017 IEEE International Conference on Web Services (ICWS)*, Honolulu, HI, USA, Jun. 2017, pp. 468–475, https://doi.org/10.1109/ICWS.2017.54.

[16] S. M. Umran, S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry," *Internet of Things*, vol. 24, Dec. 2023, Art. no. 100969, https://doi.org/10.1016/j.iot.2023.100969.

[17] N. Sapra, I. Shaikh, and A. Dash, "Impact of Proof of Work (PoW)-Based Blockchain Applications on the Environment: A Systematic Review and Research Agenda," *Journal of Risk and Financial Management*, vol. 16, no. 4, Apr. 2023, Art. no. 218, https://doi.org/10.3390/jrfm16040218.

[18] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, https://doi.org/10.1109/ACCESS.2019.2896108.

[19] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[20] T. Gao, Y. Li, N. Guo, and I. You, "An anonymous access authentication scheme for vehicular ad hoc networks under edge computing," *International Journal of Distributed Sensor Networks*, vol. 14, no. 2, Feb. 2018, Art. no. 1550147718756581, https://doi.org/10.1177/1550147718756581.

[21] Y. Ming and H. Cheng, "Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs," *Mobile Information Systems*, vol. 2019, no. 1, 2019, Art. no. 7593138, https://doi.org/10.1155/2019/7593138.

[22] M. A. Alazzawi, H. Lu, A. A.Yassin, K. Chen, "Robust Conditional Privacy-Preserving Authentication based on Pseudonym Root with Cuckoo Filter in Vehicular Ad Hoc Networks," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 12, Dec. 2019, https://doi.org/10.3837/tiis.2019.12.018.

[23] A. Bhargava and S. Verma, "DUEL: Dempster Uncertainty-Based Enhanced- Trust Level Scheme for VANET," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15079–15090, Sep. 2022, https://doi.org/10.1109/TITS.2021.3136548.

[24] Q. Xie, Z. Ding, W. Tang, D. He, and X. Tan, "Provable Secure and Lightweight Blockchain-Based V2I Handover Authentication and V2V Broadcast Protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 15200–15212, Sep. 2023, https://doi.org/10.1109/TVT.2023.3289175.

[25] Q. Tao, H. Ding, T. Jiang, and X. Cui, "B-DSPA: A Blockchain-Based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad Hoc Networks," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1385–1397, Jan. 2024, https://doi.org/10.1109/JIOT.2023.3289057.

[26] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, Mar. 2021, https://doi.org/10.1109/TDSC.2019.2904274.

[27] L. Wei, J. Cui, H. Zhong, I. Bolodurina, C. Gu, and D. He, "A Decentralized Authenticated Key Agreement Scheme Based on Smart Contract for Securing Vehicular Ad-Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 4318–4333, Feb. 2024, https://doi.org/10.1109/TMC.2023.3288930.

[28] S. J. Payattukalanirappel, P. V. Vamattathil, and M. Z. C. Cheeramthodika, "A Blockchain-assisted lightweight privacy preserving authentication protocol for peer-to-peer communication in vehicular ad-hoc network," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 4013–4032, Nov. 2024, https://doi.org/10.1007/s12083-024-01784-x.

[29] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, "Privacy-Preserving Route Reporting Schemes for Traffic Management Systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2703–2713, Mar. 2017, https://doi.org/10.1109/TVT.2016.2583466.

[30] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure Real-Time Traffic Data Aggregation With Batch Verification for Vehicular Cloud in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 807–817, Jan. 2020, https://doi.org/10.1109/TVT.2019.2946935.

[31] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, Phoenix, AZ, USA, Apr. 2008, pp. 246–250, https://doi.org/10.1109/INFOCOM.2008.58.

[32] A. S. Rajasekaran, A. Maria, F. Al-Turjman, C. Altrjman, and L. Mostarda, "ABRIS: Anonymous blockchain based revocable and integrity preservation scheme for vehicle to grid network," *Energy Reports*, vol. 8, pp. 9331–9343, Nov. 2022, https://doi.org/10.1016/j.egyr.2022.07.064.

[33] J. Zhang, H. Fang, H. Zhong, J. Cui, and D. He, "Blockchain-Assisted Privacy-Preserving Traffic Route Management Scheme for Fog-Based Vehicular Ad-Hoc Networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2854–2868, Sep. 2023, https://doi.org/10.1109/TNSM.2023.3238307.

[34] A. Maria, A. S. Rajasekaran, F. Al-Turjman, C. Altrjman, and L. Mostarda, "BAIV: An Efficient Blockchain-Based Anonymous Authentication and Integrity Preservation Scheme for Secure Communication in VANETs," *Electronics*, vol. 11, no. 3, Jan. 2022, Art. no. 488, https://doi.org/10.3390/electronics11030488.

[35] "miracl/MIRACL." MIRACL, Nov. 13, 2024, [Online]. Available: https://github.com/miracl/MIRACL.

[36] M. Luo and Y. Zhou, "An Efficient Conditional Privacy-Preserving Authentication Protocol Based on Generalized Ring Signcryption for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 10001–10015, Sep. 2022, https://doi.org/10.1109/TVT.2022.3179371.

[37] M. A. Shawky *et al.*, "Blockchain-based secret key extraction for efficient and secure authentication in VANETs," *Journal of Information Security and Applications*, vol. 74, May 2023, Art. no. 103476, https://doi.org/10.1016/j.jisa.2023.103476.

[38] A. K. Yadav, M. Shojafar, and A. Braeken, "iVFAS: An Improved Vehicle-to-Fog Authentication System for Secure and Efficient Fog-Based Road Condition Monitoring," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 9, pp. 12570–12584, Sep. 2024, https://doi.org/10.1109/TVT.2024.3390607.