Biometric Blockchain-based Multifactor Privacy Perserving Authentication Scheme for VANETs

[1*]Myra Annatasha Umang anak Dineal Gumis, [2]Travis Iran Money, [3]Mohd. Haziq Qayyim bin Safian, [4]Nur Huda Binti Hamka, [5]Zetty Elica Binti Affandi, [6]Mastura Binti Tony and [7]Siti Najihah Binti Sapuan

Faculty of Computer Science and Information Technology (FCSIT), Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

email: [1*]myraannatasha.myr@gmail.com, [2]travismoney.tm@gmail.com, [3]mohdhaziq.kjk@gmail.com, [4]hudahamka77@gmail.com, [5]zettyaffandi@gmail.com, [6]amytony1963@gmail.com, [7]najihahsapuan1998@gmail.com

Date received: 26 August 2021
Date accepted: 22 October 2021
Date published: 22 November 2021

Abstract - *To provide the most suitable or compatible scheme to work against various attack toward vehicular ad hoc networks (VANETs) is very challenging. Not only that the high authentication and communication overhead also became a problem for VANETs. Thus, in this paper we use multifactor authentication that could resist various attack toward VANETs. A biometric blockchain-based multifactor privacy-preserving authentication scheme for VANETs. This scheme is proposed by using a new robust pseudo-identity multifactor VANET scheme based on Physical Unclonable Functions (PUF) and biometric data of the vehicle's authorized user. To calculate the computational cost and the authentication overhead, we compare three of our computational cost and authentication overhead below. From the complexity analysis this proposed scheme has a lower authentication overhead and offers better security level and a low computational cost can be achieved. From the perspective of future, we hope that the cost that involve in this scheme still can be reduce as we offer a high security level. Not only that, but we also hope that this scheme can be implemented practically.*

Keywords: VANET, multifactor authentication, blockchain, biometric, Physical Unclonable Functions.

1 Introduction

One of the most technology that popular recent year is vehicular ad hoc network (VANETs). Due to the huge consumption of fuel, the high number of vehicles use each day, and the number of traffic accident became an important global issue. As we know, traffic accidents are a continuous problem that result in significant loss of property and life (Shrestha et al., 2018). To overcome this issue, VANETs was introduced by an intelligent transportation system. It provides communication link among vehicles as VANETs is a form of mobile ad hoc network (MANET) that can help to reduce the problem (Alazzawi et al., 2019). There are two modes of communication provided in VANETs which are vehicles-to-infrastructure (V2I) and communication between car (V2V). Through the Dedicated Short-Range Communication (DSRC) these two communications are developed to encourage collaboration within vehicles and to exchange useful information (Zheng et al., 2019). The primary goal of VANETs is to achieve successful communication; in general, nodes require specific qualities to acquire information, communicate with neighbours, and then make judgments based on all the data gathered via sensors, cameras, receivers, and omnidirectional antennas (Sheikh et al., 2019). Mutual authentication and specifically multifactor authentication mechanism are not a new research paradigm. Several researchers have proposed several methods to ensure secure authentication mechanisms in any communication protocols (Khan et al., 2021; Khan et al., 2019; Maikol et al, 2020; Balan et al., 2018).

However, one of the biggest challenges that VANETs often face is network security attack. The attack that usually involve in VANETs are impersonation attack, reply attack, DoS attack, man in the middle attack and side-channel attack. Attackers took advantage of the cloud servers used in a conventional centralized approach of VANETs

which result in a single point of failure in data storage, leading to possible leakage of sensitive personal data and information, leads to dangerous scenarios and causing network disruption (Zheng et al., 2019; Malik et al., 2017). Security attack can result in the theft of the real identity of any vehicle, modifications of a valid beacon, impersonation of vehicles to transmit bogus information in the VANETs for personal benefits and eavesdrop the communication among the vehicles. These consequences can reduce the efficiency and performance of the network (Alazzawi et al., 2019). The consequences for the high computational cost are first, deliberately broadcasting many invalid verifications or authentication requests may exhaust the receiver's computing power and network capacity (Malik et al., 2017). Next, the weak authenticator for the puzzle solution is difficult to counterfeit, precompute, or reuse (Malik et al., 2017). Authentication in VANETs has numerous methods for preventing and countering network security attacks while being computationally efficient. Zheng et al. (2019) proposed implementing blockchain technology in the mutual authentication process for VANETs, which helps to build a trust communication environment that retains anonymity without revealing user identities. This is owing to the fact that blockchain offers tamper-resistance, immutability, and decentralization qualities that aid in privacy preservation and the prevention of replay attacks (Zheng et al., 2019). It is also worth noting that the mentioned scheme reduces the dependence on the authority centre as well as the load of vehicle identity authentication, resulting in improved efficiency in computational costs (Zheng et al., 2019). Aside from that, the significant computational costs associated with VANETs can also be handled by using batch signature verification. Feng et al. (2017) proposed a scheme that utilizes batch signature verification in which a revoked user list is implemented to facilitate validation and any expired keys are removed to minimize the list length therefore reduce the computational overhead. To sum up, an efficient and secure mutual authentication scheme is key to overcome VANETs' high computation cost and its vulnerability to security attacks. An efficient scheme for VANETs' authentication protocol is required as it helps reduces the computation cost therefore enabling exchange of information to occur at a faster rate.

To overcome this problem, we proposed a multifactor authentication by using biometric blockchain-based multi-factor privacy-preserving authentication scheme for VANETs. It combines the use of biometric authentication, registration vehicle and the identity authentication.
Following the proposed biometric blockchain-based multi-factor privacy-preserving authentication scheme for VANETs, our contributions are as the following:

i. We have incorporated the biometric technology by introducing a new authentication phase prior to the vehicle registration phase called the biometric authentication phase, as an added level of security in authentication for VANETs. This phase involves validating the real identity of the vehicle's authorized driver by using the biometric data (fingerprint) of the vehicle's authorized driver for the vehicle to be registered into the VANETs.

ii. We have introduced a new robust pseudo identity for the vehicles that is based on the calculated hash value of the Physically Unclonable Function (PUF) given to them and biometric data of the vehicle's authorized driver. With this new robust pseudo identity, it is impossible be cloned and thus helps to mitigate physical and cloning attacks.

iii. Finally, we have conducted the security analysis, computational and authentication overhead for our proposed scheme. In comparison to the three distinct schemes used as references, our method is practical and easy while maintaining security, and it also offers decentralization, conditional privacy, security authentication, and trusted communication features.

The proposed scheme should be able to mitigate any security attacks that were mentioned that are impersonation attack, reply attack, DoS attack, man in the middle attack and side-channel attack. This scheme also immune to bogus information attack, this attack includes disseminating counterfeit or fake information across a network to cause disruption to guarantee the safety and security of user while vehicles are on the road. User's identity and privacy must be always protected especially when performing authentication. The proposed work can be extended to enhance end to end security mechanism in network intrusion detection system or malware detection system (Ahmad et al., 2021; Dildar et al., 2017; Khan et al., 2021; Khan et al., 2017).

The rest of this project are organized as follow. Section II present the proposed the related work that involve in this project. Section III describe the multifactor authentication of a new robust pseudo-identity multi-factor VANET scheme based on Physical Unclonable Functions (PUF) and biometric data of the vehicle's authorized user with the diagram of proposed scheme in details. Section IV gives the security analysis. Section V presents the complexity analysis of authentication overhead and computational Overhead. Section V conclude the paper and provide the potential for future work.

2 Related Works

There is a various scheme that was developed by researchers where the focus of each scheme is to provide a secure and efficient solution in VANET.

Feng et al. (2017) have discussed the security and privacy issues and solutions for pervasive social networking (PSN). An anonymous authentication scheme based on group signature was proposed by the researchers. Anonymous authentication is used to protect nodes' privacy, which is a property of group signatures (Azam et al., 2021). The scheme also adopts batch verification to verify messages efficiently and able to reduce delay. The author claimed that the proposed scheme could address impersonation attacks and user tracking.

Alfadhli et al. (2020) proposed a lightweight multifactor authentication that employs Physical Unclonable Functions (PUF) and one-time dynamic pseudo-identities as an authentication factor. PUF puts as a second authentication factor in the scheme. PUFs have a built-in physical characteristic that allows them to provide a unique one-way function that is impossible to duplicate. The features of PUF are enabling the scheme to preserve privacy and provide security.

According to Zhang et al. (2017), existing schemes that focus on privacy-preserving are often had a time-consuming operation with a high volume of cryptographic data. Zheng et al. (2017) proposed Distributed aggregate authentication (DAPPA) protocol based on the MTA-OTIBAS technique to mitigate the issue. A vehicle can verify multiple messages at a time, and their signature can be aggregated onto a single message. Therefore, the storage space needed by data collectors or vehicles can be significantly reduced.

The issues are mainly on the security network and privacy problems in VANETs. The security analysis focuses on replay attacks, impersonation attacks, modification attacks, and man-in-the-middle attacks (Cheng et al., 2020). The consequences can result in leaking data, modifying valid beacons, and impersonating vehicles to send bogus information throughout the VANETs. Furthermore, existing schemes suffered from high computation costs, and the vehicle is disseminating false information due to issues raised by PKI-based and ID-based authentication systems. To mitigate the security drawbacks and problems in VANETs, Elliptic Curve Cryptography (ECC) is used in the proposed pseudo-ID-based scheme schemes. Alazzawi et al. (2019) scheme contribute to increased computation cost-effectiveness and resisting network attacks mentioned above.

Blockchain is first proposed by Nakamoto, which consists of decentralized, tamperproof, trustworthy, and anonymity (Feng et al., 2017). Malik et al. (2018) proposed a blockchain-based authentication scheme to reduce reliance on CA for identity verification by introducing a shared blockchain ledger. The scheme also uses Elliptic Curve Cryptography (ECC) to help in providing a high level of security with shorter keys (Feng et al., 2017). Plus, the scheme can reduce overhead while performing revocation of malicious vehicles by prioritizing identifying the vehicle that has been revoked without circulating a whole Certificate Revocation List (CRL).

Alharthi et al. (2021) proposed a biometric blockchain (BBC) framework. The combination on blockchain and biometric feature can provide a reliable data transmission, data exchange tracking and identifying vehicle that involve in sending false messages.

Another example of blockchain-based authentication is by Zheng et al. (2019). Zheng et al. (2019) mentioned that VANETs are prone to a wide range of attacks due to the high mobility and volatility and less efficient authentication, adequate scalability, and adequate distribution. In addition, the potential leading problems can result in data self-tempering, vehicular information leakage, disseminating forged within the network, and impersonate vehicles to send bogus information, potentially leading to an accident. Therefore, for the mentioned issues mentioned above, the authors proposed to implement blockchain technology into VANETs. Using blockchain technology in VANETs, all participant activities, identification authentications, and broadcast of messages will be written into an immutable and unalterable ledger with resistance to tampering and decentralization properties.

3 Proposed Solution

In this paper, we proposed a biometric blockchain-based multifactor privacy-preserving authentication scheme for VANETs. In the proposed scheme, we have incorporated the biometric technology at the initial authentication phase as an added layer of security in authentication for VANETs prior to vehicle registration. In addition, we have also introduced a new robust pseudo identity provided by the CA for the registered vehicles to communicate with other entities in the scheme. This new robust pseudo identity helps to mitigate physical and cloning attacks,

besides providing privacy preservation and traceability. The proposed scheme creates a trust communication environment against internal forced messages while also protecting vehicle identification privacy. Meanwhile, compared to traditional schemes, the decentralized framework is more trustworthy and safer with the participation of blockchain technology, and it also lowers reliance on CA.

3.1 Entities

The entities involved in our proposed scheme is described below:

3.1.1 Certificate Authority

CA oversees issuing certificates for registered vehicles and calculating two specific hash function. Under the supervision of RSUs, the two unique hash functions calculated by CA is to prepare to authenticate vehicles as well as to and trace vehicles.

3.1.2 Roadside Units

Prior to being registered in the blockchain, RSUs will verify all broadcasted messages and transactions. RSUs, as peer nodes in the network of blockchain, are also in charge of authenticating the vehicle identification recorded in each vehicle via V2I communication. Furthermore, RSUs preserve the link between the pseudonym and true identity of the vehicle's in blockchain to ensure CA trustworthiness.

3.1.3 Cloud Server

The cloud server serves two primary purposes. First, it handles the pseudonyms of vehicle given by CA for the identity authentication's convenience. The second on the other hand, in a decentralized manner, it stores the specifics of the transactions declared by vehicles that announces traffic information.

3.1.4 Vehicle

The blockchain is used to power the privacy-preserving authentication system. Vehicles may monitor RSUs by examining the transaction information saved in the cloud server using the unique hash registered in the blockchain. Furthermore, registered vehicles can report harmful members to RSUs for gathering of proof, and the reported vehicles is going to be penalized with the help of the CA and RSUs.

3.1.5 On-Board Units (OBU)

On-Board Units are installed in the vehicles where it contains the real driver's information. The fingerprint scanner will be placed on the On-Board Unit (OBU). Besides that, OBU will be used by the vehicle to connect wirelessly with other entities in the proposed scheme.

3.1.6 Transaction

The transaction involved is meant by the transaction of vehicle identity as well as the traffic announcement's transaction. The latter's hash value is saved in the blockchain, while the particular traffic status information is saved on distributed cloud servers. All the transactions comprise a timestamp and the initiator's signature, but no information that may be linked with the true identity is incorporated in the transaction to protect privacy.

3.1.7 Certificate

Once vehicles register their actual identities into the system, the CA issues them a certificate that contains one pair of public-private keys, two hash values in addition to pseudonyms. However, there is no true identification regarding the vehicle's identity in this certificate to protect the vehicle's privacy.

3.2 Assumptions

To construct the proposed authentication scheme for VANETs in this paper, the following assumptions are made:

a. The CA has sufficient space of storage for maintaining the dataset holding the connection involving the pseudonym and true identity of the vehicle.
b. RSUs have more computational capacity as compared to general-purpose computers, allowing them for authenticating and verifying vehicles and check transaction consistency.
c. Hacking greater than half of the blockchain network participants is only beyond the attackers' capacity.

d. The cloud servers are not familiar with one another and have adequate storage space.
e. The OBU's preloaded information (drivers' information) is secured against malicious attack and that the OBU will be used by the vehicle to connect wirelessly with other entities in the proposed scheme.

3.3 Structure of Proposed Scheme

The structure of the proposed scheme is discussed in further detail in this section. The suggested scheme focuses primarily on the first three phases in the authentication involving VANETs, which are biometric authentication, vehicle registration, and vehicle identification authentication. Table 1 lists the notations used in the proposed scheme.

Table 1: Notations Used in Our Scheme

Notation	Definition
V	Set of vehicles
RSU	Set of Roadside Units
S	Set of cloud servers
Di	Driver's information
$Dbio$	Driver's biometric data
$VIDi$	The real identity of *i-th* vehicle
$PIDi$	The pseudonym of *i-th* vehicle
CA	Certificate Authority
H	Hash Function
ECC	Elliptic-curve cryptography
Pki	ECC Public Key
Ski	ECC Private Key
CfT	Cancellable template database
C	Challenge
$cert$	Certificate issue to registered vehicle
th	threshold
ED	Euclidean Distance
PUF	Physically Unclonable Function
R	Unique string of bits called Response R
$Ex()$	Encrypt with x
$Dx()$	Decrypt with x
N_{RSUi}	*i-th* random integer negotiated with RSU
M_{Vi}	Random number selected by *i-th* vehicle
$sig_x()$	Sign with x
Tx_i	*i-th* transaction

3.3.1 Phase 1: Biometrics Authentication

Before the registration of vehicle phase takes place, the real vehicle ID ($VIDi$) together with the driver's information (Di) will be forwarded to the CA. The driver's information will contain the fingerprint data to guarantee the driver's identity. The fingerprint scanner is placed on the On-Board Unit (OBU).

The driver's identification is going to be authenticated via a modified discrete transformation (MDCT). The driver will place his or her fingerprint during biometrics authentication, which is then processed by MDCT to produce a cancellable fingerprint template. The cancellable biometric system then converts the driver's biometric identification and save the cancellable reference template at the cancellable template database (*CfT*) located in the CA and OBU. The *CfT* is used to provide access to VANETs in the second phase that involves the registration of vehicles. Two procedures achieve biometric driver authentication: enrolment and authentication. The vehicle's driver's biometric data *CaT* is registered in the database during the enrollment procedure. Now of authentication, the driver's biometrics are recorded as *CfT** and checked against other reference templates located in the CA database. Based on the similarity, the Euclidean distance (*ED*) has been used to match the collected and reference data. If both sets of data match, the driver will proceed to phase 2 which is the registration of vehicle.

3.3.2 Phase 2: Registration of Vehicle

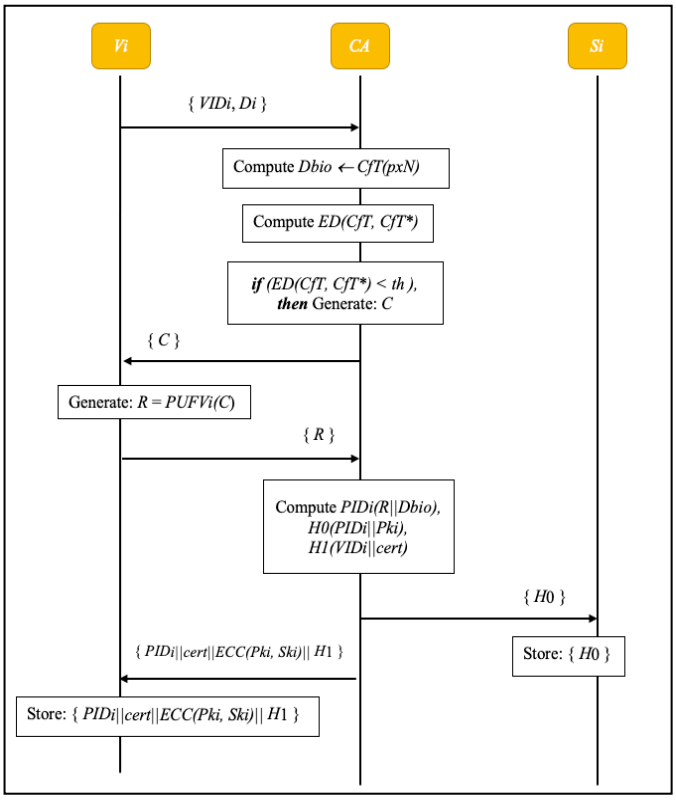

Figure 1: Registration of Vehicle Vi.

During this registration phase, CA being a trusted third party develops a set of system parameters based on the unique vehicle ID and biometrics data given by the registered vehicle. To protect the vehicle's identity information and communication, the CA assigns a pseudonym to the registered vehicle for communication, which is then kept in the CA's database. The registered vehicle's pseudonym is generated using the computed hash value of both the PUF and biometric data (fingerprint) of the vehicle's authorized driver. The CA, in particular, transmits the hash values to the registered vehicles and cloud servers, correspondingly, to ease authentication process of the vehicle and reduces the communication strain on the CA. As illustrated in Figure 1, the integrated vehicle registration process consists of the following interactive steps:

Step 1: If the biometric authentication for the vehicle's authorized driver is successful, the CA will generate a random challenge called *C* and sends it to the vehicle.

Step 2: When the vehicle receives the challenge *C* from the CA, it extracts the *PUF* output *R = PUFVi(C)* and returns it to the CA.

Step 3: The CA next computes a hash value for the vehicle's pseudonym *PIDi*, where *PIDi = H(R||Dbio).* Finally, the CA creates the certificate, which contains the pseudonym *PIDi*, a pair of *ECC* public-private keys, *Pki* and *Ski*, in accordance with the vehicle's true identity.

Step 4: Two hash functions *H0 = (PIDi||Pki)* and *H1 = (VIDi ||cert)* are then calculated by the CA. These hash functions are used to authenticate the identity of the vehicle and storing information of vehicle in the future.

Step 5: The CA will then transmit the hash value *H0* to the cloud server, to which the cloud server will then store the hash value *H0*.

Step 6: The registered vehicle then obtains from the CA a robust pseudonym *PIDi*, certificate, *H1*, and a pair of Public-Private keys, to which are stored in the On-Board Unit (OBU).

3.3.3 Phase 3: Identity Authentication

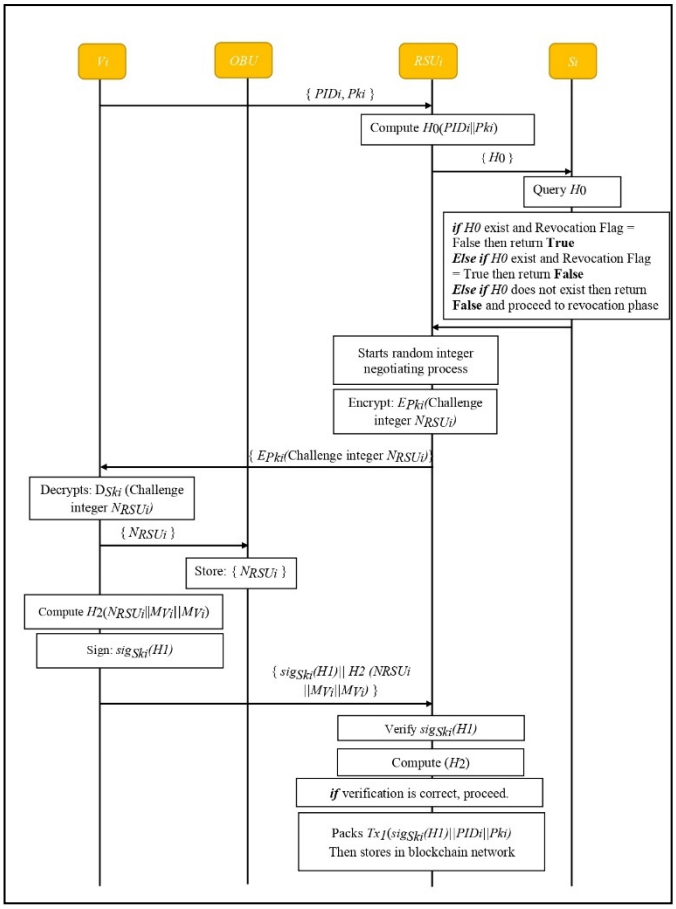

Figure 2: Identity authentication of Vehicle Vi.

The moment a vehicle on the road appears within the range of the nearest RSU installed, it delivers a request for authentication to the RSU using its very own PID. On top of computing the corresponding outcome of the delivered authentication request, the request's correctness is acquired by the RSU through querying data from the cloud server. Then, the result of the authentication is logged into the blockchain by RSU. The vehicle and the RSU communicates with each other under its own alias during authentication and both the RSU and the cloud server are both unaware of the vehicle's true identity. Figure 2 depicts the proposed mechanism involving the authentication, which is involves seven stages explained below:

Step 1: A request for authentication is vehicle initiated by the vehicle by forwarding a message to a nearby RSU on the lane, to which the RSU obtains the vehicle's pseudonym *PIDi* and public key *Pki*.

Step 2: Once the message of request is received, RSU computes the hash value as per the *H*0 algorithm then returns the corresponding result. To confirm the vehicle's legality, the RSU uses the cloud server to verify result's accuracy. "True" is returned to RSU by the cloud server if the query response fits the calculation result and also if the vehicle is not flagged as revoked, meaning that the vehicle is legitimate. If the query response fits the calculation result but is flagged as revoked, authentication will fail. On the other hand, an unmatched query result and calculation result will result in fail authentication and revocation phase starts.

Step 3: The RSU starts the random integer negotiating process after confirming the validity of the vehicle's identity. It sends the vehicle a random integer *NRSUi* that is encrypted with *Pki*.

Step 4: The ciphertext is received and decrypted by the vehicle using its private key *Ski* before storing the integer *NRSUi* in OBU to be used for future announcement cases.

Step 5: To decide whether or not the integer from the RSU is received by the vehicle and the credibility of the random number, another random number *MVi* must be picked by the vehicle and calculate a hash function *H*2 obtained two integers previously stated. Furthermore, to ensure that the CA is secured from malicious behaviour, the vehicle must sign on *H*1, which is the mapping of true identity and certification, and store it in the blockchain network. Then, RSU finally receives *sigSki*(*H*1)|| *H*2 (*NRSUi*||*MVi*||*MVi)* from the vehicle.

Step 6: The RSU validates the hash value *H*1 with the vehicle's signature and computes the corresponding hash value based on the obtained random integer *MVi* and the *NRSUi* using the vehicle's *Pki*. If the calculated result turns out exactly as *H*2, the received hash value, then that indicates a successful random number negotiation.

Step 7: As a blockchain network peer node, the RSU packages a transaction *Tx*1(*sigSki* (*H*1)||*PIDi*||*Pki*) and saves the respective transaction in the network of the blockchain. All RSUs can then obtain transaction *Tx*1.

As a result of this phase, the RSU now has access to the authenticated vehicle's public key and certificate without having to authenticate it again in the future. The information is not stored in a single location on a single server but is split into several sections and stored in a variety of locations. Whenever the OBU and RSU requires to query or validate details of transaction, the related transaction content can be accessed by means of various servers based on the transaction's unique hash value. The transactions' content is accessed from various servers, that enables the prevention of data leakage, ensuring the integrity of transactions, preventing collusion attacks, and improving cloud storage trust and authentication

4 Security Analysis

In this subsection, we discuss how the proposed biometric blockchain-based multi-factor privacy-preserving authentication scheme meets the security criteria.

4.1 Added Layer of Security in Authentication

As an extra layer of security in authentication for VANETs, we have incorporated the biometric technology by establishing a new authentication phase prior to the vehicle registration phase called the biometric authentication phase. In order for the vehicle to be registered into the VANETs, this phase requires confirming the true identity of the vehicle's authorized driver using biometric data (fingerprint). If the biometric authentication phase fails to validate the true identity of the vehicle's authorized driver, the vehicle will be unable to register in the VANETs.

4.2 Physical and Cloning Attack

In our scheme, each vehicle is embedded with a PUF, hence any physical tampering effort by an adversary will fail to compromise the OBU. Any such activity, however, will alter the behavior of the embedded PUF's and render it unusable. Furthermore, because the PUFs cannot be recreated, they are immune to cloning (Alfadhli et al., 2020), in contrast to (Hakeem et al., 2019) and the majority of the previous related works, which did not contemplate such an attack.

4.3 Privacy-Perserving

Vehicle X utilizes its own CA-issued robust pseudonym PIDi for V2V and V2I communications, with no knowledge of its true identity. In order to strike a balance of both security and privacy, CA stores pairs of identities and pseudonyms with great level of security. It implies that only CA acknowledges the true identity of any provided pseudonym for each vehicle, and only CA has the power to track the harmful vehicle whenever it misbehaves, or broadcasts falsified communications. Furthermore, at the stage of authentication, the mapping of true identity and pseudonym is also stored on blockchain network, and RSUs does not have the capability to acquire the mapping particular information, which significantly increases CA confidence. To protect the privacy of vehicles, no information that may be linked to the true identity is included in the transaction.

4.4 Traceability

A signature for each broadcasted message is generated by Vehicle X using its private key, and RSU may verify the signature using that vehicle's public key. In the meantime, the other vehicles forwarding the message must

insert their own pseudonym and signature on the messages before they are distributed. Once the malicious vehicle with forged message is detected, the system tracks it down and obtain the vehicle's true identity with help of the CA and RSUs. The need to record the mapping of the malicious vehicle's pseudonym and actual identity on the blockchain makes it difficult for CA, as a trusted institution, to interfere with the relevance of the malicious vehicle's real identity and pseudonym. At the same time, a report is forwarded to the cloud servers to cancel the malicious vehicle's identification information while pursuing the malicious cars' responsibility.

5 Complexity Analysis

5.1 Authentication Overhead

The proposed authentication overhead will be compared with (Zheng et al., 2019), (Malik et al., 2017), and (Zhang et al., 2017). Zheng et al. (2019) proposed the scheme that both the client and the server must have digital certificate where a link can be establish in a mutual authentication process only if the client and server exchange, verify, and trust each other's certificate. The Certificate Authority (CA) issues a set of Elliptic-curve Cryptography (ECC) Public-Private keys (Pki and Ski), Pseudo ID, certificate, hash function H0 to the registered vehicle, and where the vehicle stores it in the OBU. For the proposed scheme in (Malik et al., 2017), the roadside unit (RSU) will be broadcast the RTA's public keys pkc to all vehicles within its range on a regular basis, to validate the message's validity, together with its ID-based signature of the current time interval and a nonce value of freshness. Then the vehicles within the RSU's range will use pkc and others private details to update or generate new pseudonym. As for the proposed scheme in (Zhang et al., 2017), DAPPA is the authentication protocol. The scheme proposes that every vehicle be outfitted with a working TPD, in the sense that the TPD's secrets must be changed before an intruder can extract enough data from it. The system settings and master secret are generated by the root TA in DAPPA.

As for the proposed scheme, the biometric blockchain-based multifactor privacy-preserving authentication scheme has an OBU have the fingerprint scanner where the information will contain the fingerprint of the driver to ensure the identity. The authentication of the driver's identity will be done using MDCT. The RSU now has access to the authenticated vehicle's public key and certificate without having to authenticate it again in the future. The information is not stored in a single location on a single server but is split into several sections and stored in a variety of locations. Compared with the proposed scheme from (Zheng et al., 2019), (Malik et al., 2017), and (Zhang et al., 2017), this proposed scheme has a lower authentication overhead and offers better security level.

5.2 Computational Overhead

The proposed computational overhead will be compared with (Alazzawi et al., 2019), (Malik et al., 2017), and (Vasudev et al., 2020). The proposed scheme in (Alazzawi et al., 2019), the computational cost of the proposed scheme is compared in terms of BGS, SVOB, and BVMB. The proposed scheme has a 0.4422ms faster computing time for BGS, computes SVOB in 0.8859ms, and BVMB computing time for 25 beacons is 1.6528ms. For the proposed scheme in (Malik et al., 2017), the communication delay is measured, and it is defined as the amount of time the RSU take to decrypt the message received, fetch the pointer information and PID from the relating transaction and produce the challenge message, while using the public key of the PID for encryption. The delay between RSU and OBU is observed to be approximately 45ms for up to 5 nodes or vehicles. The communication delay increases with nodes advancing from 5 to 10 then recorded a value of around 68ms to 75ms for 10 to 50 nodes. Proposed by Vasudev et al. (2020), the hash function and symmetric cryptographic (encryption / decryption) are the two components that contributes to computation cost. For example, the researcher assuming that time is the expense takes to carry out computation. Let say the individual operations take the time such as Ch $\approx$ 0.0020ms, Cm $\approx$ 0.0268ms and Cse/Csd $\approx$ 0.01000ms, Cpe takes 4.4063ms, Csd takes 7.7613ms, and Ce takes 0.0399ms. Thus, the total cost of the proposed protocol of 17Ch since it only uses hash functions.

As for the proposed scheme has no pairing operations because it mainly needs one encryption-decryption operation involving the ECC along one signature with verification operation. The authors simulated vehicle registration, authentication, and announcement in order to evaluate the efficacy of the proposed mechanism. The number of vehicles ranged from one to fifty, with average values received for every five vehicles. The Physically Unclonable Function (PUF) send to the vehicle from the CA. The vehicle then extracts the PUF and send it back to the CA. Furthermore, there is biometric authentication prior to the vehicle registration. The pseudonym for the vehicle is generated using the hash value of the PUF and the biometric data of the driver. This will lead to a lower computational cost and efficient for the authentication compared with the schemes from (Alazzawi et al., 2019), (Malik et al., 2017), and (Vasudev et al., 2020).

6 Conclusions

In this paper, we have designed multifactor authentication framework by using Physical Unclonable Functions (PUF) and biometric data of the vehicle's authorized user with the participant of blockchain technology. The vehicles use the pseudonym to disclose the vehicle information to communicate to other entities. This scheme contains 3 phase that are Biometric authentication phase, Registration Vehicle phase and Identity authentication phase, these phases are needed as the unique ID of the vehicle and the biometric data of the user is used to make this scheme work. The result shown in security analysis and complexity analysis prove that secure registration is need by using signature keys to provide strong security. Not only that, the authentication and computational overhead also can be reduced to achieve high efficiency by using the proposed .

Acknowledgements

The authors would like to thank Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak to support this research work. This work is carried out as a short-term research-based class project.

References

Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network Intrusrion Detection System: A Systematic Study of Machine Leanring and Deep Learning Approaches. *Transactions on Emerging Telecommunications Technologies, 32*. doi:10.1002/ett.4150

Alazzawi, M. A., Lu, H., Yassin, A. A., & Chen, K. (2019). Effecient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad-Hoc Network. *IEEE Access, 7*, 71424-71435.

Alfadhli, S. A., Lu, S., Chen, K., & Sebai, M. (2020). MFSPV: A Multi-Factor Secured and Lightweight Privacy-Preserving Authentication Scheme for VANETs. *IEEE Access*, 142858-142874.

Azam, F., Yadav, S. K., Priyadarshi, N., & Padmanaban, S. (2021). A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. *IEEE Access, 9*, 31309-31321.

Balan, K., & Khan, A. S. (2018, December 12). RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks. *International Journal of Advanced Computer Science and Applications (IJASCA), 9*, 298-304.

Cheng, H., & Liu, Y. (2020). An Improved RSU-based Authentication Scheme for VANET. *Journal of Internet Technology*, 1137-1150.

Dildar, M. S., Khan, N., Abdullah, J. B., & Khan, A. S. (2017). Effective Way to Defend the Hypervisor Attacks in Cloud Computing. *2nd International Conference on Anti-Cyber Crimer (ICACC)*, 154-159.

Feng, W., Yan, Z., & Xie, H. (2017). Anonymous Authentication on Trust in Perversive Social Nerworking based on Group Signature. *IEEE Access*, 6236-6246.

Hakeem, S. A., El-Gawad, M. A., & Kim, H. (2019). A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks. *IEEE Access*, 119689-119705.

Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. A. (2021). A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. *IEEE Access*, 87079-87093.

Khan, A. S., Balan, K., Javed, Y., Abdullah, J., & Tarmizi, S. (2019). Secure Trust-based Blockchain Architecture to Prevent Attacks in VANET. *Sensors(Switzerland), 19*(22).

Khan, A. S., Javed, Y., & Abdullah, J. (2021). Trust-based Lightweight Security Protocol for Device to Device Multihop Cellular Communication (TLwS). *Journal of Ambient Intelligence and Humanized Computing*. doi:10.1007/s12652-021-02968-6

Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending Malicious Script Attacks Using Machine Learning Classifiers. *Wireless Communications and Mobile Computing, 2017*. doi:10.1155/2017/5360472

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L., & Petrus, C. (2020). A Novel Authentication and Key Agreement Scheme for Countering MITM and Impersonation Aattack in Medical Facilities. *International Journal of Integrated Engineering, 13*, 127-135.

Malik, N., Nanda, P., Arora, A., He, X., & Puthal, D. (2017). Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks. *2018 17th IEEE International Conference on Trust, Security and Privacy in ComputingAnd Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, 674-679.

Sheikh, M., & Liang, J. (2019). A Comprehensive Survey on VANET Security Services in Traffic Management System. *Wireless Communications and Mobile Computing, 2019*, 1-23.

Shrestha, R., Bajracharya, R., & Nam, S. (2018). Challenges of Future VANET and Cloud-Based Approaches. *Wireless Communications and Mobile Computing , 2018*(5603518), 1-15.

Vasudev, H., Deshpande, V., Das, D., & Das, S. K. (2020). A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. *IEEE Transactions on Vehicular Technology*, 6709-6717.

Zhang, L., Wu, Q., Domingo-Ferrer, J., & Qin, B. H. (2017). Distributed Aggregate Privacy-Preserving Authentication in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 516-526.

Zheng, D., Jing, C., Guo, R., Guo, S., & Wang, L. (2019). A Traceable Blockchain-Based Access Authentication System with Privacy Perservation in VANETs. *IEEE Access, 7*, 117716-117726.