Management Journal for Advanced Research
ISSN (Online): 2583-1747
Volume-2 Issue-4 || August 2022 || PP. 35-41 DOI: 10.54741/mjar.2.4.6

Optimized and Efficient Authentication in VANET using Blockchain

Shrinivas Khedkar[1] and Ronik Mahajan[2]
[1]*Assistant Professor, Department of Computer Engineering and IT, VJTI, Mumbai, India*
[2]*M.Tech Student, Department of Computer Engineering and IT, VJTI, Mumbai, India*

[1]*Corresponding Author: sakhedkar@ce.vjti.ac.in*

Received: 03-07-2022 Revised: 14-08-2022 Accepted: 29-08-2022

ABSTRACT

Vehicle ad hoc networks (VANETs) are the most interesting area of research in smart transport systems as they provide convenience and safety information to drivers. However, VANET's unique features make security, privacy and trust management promising issues in the design of VANET's. It is a challenging problem to provide an effective anonymous authentication system in ad hoc vehicle networks (VANETs) with low computational cost. Blockchain technology in VANET provides a decentralized, secure, and reliable database, which is maintained by the network node. Earlier, vehicle authentication is performed whenever the vehicle enters the RSU range. In this paper, authentication will be done if a vehicle fails to travel certain distance. This decreased number of authentications and time required for it leads to increase in efficiency of the system.

Keywords: *vanet, blockchain, manet, authentication*

I. INTRODUCTION

The growing demand for improvements to road safety and the optimization of road traffic has brought widespread interest to Vehicles Ad Hoc Networks (VANET). It's similar to that of Mobile Ad Hoc Networks (MANET), in which vehicles behave as a mobile node. VANETs consists of vehicles, roadside unit (RSUs) and a centralized trusted authority (TA). It is developed for short-range direct communication between vehicles and long-range communication via RSU. In VANET, each vehicle is equipped with On-board-Unit(OBU) which is a tamper-proof device and is used to communicate with other vehicles that is vehicle-to-vehicle(V2V) communication, the vehicle also communicate with roadside units (RSUs) for authentication and providing useful information that is a vehicle-to-RSU (V2R) communication. The vehicles and RSUs are deployed with wireless interfaces within their radio range.

Due to wireless network infrastructure, it is necessary to provide primary security measures such as authentication and privacy preservation. If proper security measures are not taken then various attacks can be possible namely, man-in-middle attack, fake information attack, impersonation attack, etc. VANET is considered as an intelligent transport system which aims to prevent traffic flow and road accidents. However, if data sent/received by vehicle is lost, tampered or delayed with while on road, this will affect driver's or automated car decisions, resulting in deviation from actual route, severe accident or delay in further V2V communications. Proper authentication in minimum amount of time and preserving privacy in an anonymous manner solves the problem. If authentication is not done properly then malicious vehicle may get authenticated further, it may pass fake messages and disturbs the system. Increased authentication time causes delay in response time and quick decision taking capabilities of driver and automated vehicle. Privacy preservation of vehicle in an anonymous manner prevents impersonation and spoofing attacks. Moreover, if legitimate anonymous vehicle turns malicious, then its information should be revoked by Trusted Authority (TA) to all vehicles and RSUs to prevent further damages.

VANET supports broadcasting of messages by RSUs and vehicles into their range. Compared with RSUs, vehicles have shorter range. RSUs broadcast essential messages such as traffic update, location-based messages, speed limit message etc. to remain vehicles updated. Vehicles also send messages such as, its speed and direction, lane change message, etc. The rapid change in VANET topology due to fast moving vehicles limits the communications therefore quick authentications need to be done.

Thus, this paper focuses on reduced and quick authentications using HMAC-SHA256 algorithm based on bilinear pairing for elliptic curve, also necessary messages are prioritized and stored in blockchain using PoA in less time.

PoA- The Proof-of-Authority (PoA) is a replacement for the Proof-of-Work, where the blockchain is protected by only a group of pre-selected authorities called validators. This approach does not utilize nodes to solve difficult mathematical problems, instead it uses a set of validators to add block in blockchain. The main characteristics of a PoA are a low computational power requirement, no communication requirement between nodes to reach consensus, and network continuity is independent of the number of genuine nodes available.

A. Our Contributions

Based on the observed conflicts and challenges, the main contributions of this paper are summarized as follows.

In order to reduce authentication time, we optimized number of reauthentications to increase efficiency of the system with high security and privacy.

The computational cost of adding block in blockchain is also reduced by using PoA.

To minimize emergency message loss, the messages are priotized and authenticated based on the type of message sent by vehicles.

B. Roadmap of This Paper

Rest of this paper is organized as follows: Section II represent surveyed related works. Section III explains the existing system and states its advantages and limitations. Section IV details the system overview. Section V describes the proposed schema. Section VI is performance analysis. Section VII concludes the conclusion

II. RELATED WORK

The main aim of VANET is to provide safety warnings and emergency messages to comfort drivers in the vehicular environment. Later research focus on privacy preservation of vehicles and security. The pseudonym-based approaches effectively protect the privacy of vehicles, while preserving the privacy of vehicles the research work lead to reducing authentication time for vehicles so that quick response will be taken by vehicles. The security of vehicles immessages is done by using blockchain.

An efficient conditional privacy preserving protocol based systems are proposed in [1-4, 6, and 15]. In these schemas, whenever vehicle enters into the range of RSU, RSU provides multiple anonymous short-term keys to a vehicle so that it is prevented from being traced. Due to short-term keys the storage of keys problem is solved but the latency of different keys generation at RSU is increased. If the requester is an RSU, it is usually possible for the RSU with the private key to work locally. On the other hand, if the requester is an OBU, when requesting short-time anonymous public key certificates, the OBU may use the private key to authenticate itself. The main limitation of ECPP it that, the RSUs suffers from high latency in pseudonym generation. Also, the vehicle has to wait to receive pseudonyms from RSU to carry further communications. The pseudonyms need to be informed to TA before issuing it to vehicles which again increases time delays between request-response of vehicles and RSU. Fengzhong et.al.[5] and Lu et. Al. [14] has given a review on security and privacy of VANETs.

In [7], an effective Pseudonymous Conditional Privacy Protocol (PACP) for VANETs is proposed. In this schema, prior when vehicle submit its documents to TA such as driving license, Aadhar card, vehicle information, etc., after verification based on that documents a long-term pseudonym named as ‘ticket’ is generated and is assigned to the vehicle which is then further used to obtain ‘tokens’ from RSUs. Using this token, the vehicle generates a pseudonym for further anonymous V2V and V2R communications. The PACP protocol tries to overcome the drawbacks of ECPP protocol but it suffers from some limitations. First, it is not efficient due to two reasons: 1. It has relatively high latency for RSUs to produce pseudonym keys. and 2. It needs the omnipresence of RSUs to assist vehicles in deriving their pseudonyms and corresponding keys at any given position on the route. Secondly, the RSUs gives corresponding mapped tokens with provided ticked without knowing any information about vehicles. In addition, RSUs need to provide multiple tokens to increase vehicle anonymity.

In [8] the DSSCB, the RSU is a preselected Node (PSN) and the vehicle is sensing node (SN). PSNs have granted the right to write data and participate in the consensus whereas, the SN can access and synchronize replicas, but it does not participate in the consensus. Whenever SN enters the range of PSN the sensed data is uploaded to PSN after verifying the identity and request information and after certain period of time the collected data is signed and broadcasted to entire network then all PSNs engage in consensus process to compete for the permission for data writing in blockchain. The limitations of this schema are that, the authentication process requires more time as it sequentially process the following authentication phases: Signature request. parameters generation, pseudonym generation module, Signature key generation, message signing and message verification. Moreover, the computational cost of the system increases as all PSNs engage in competing among themselves to add block in blockchain also, all messages are stored despite of storing only essential messages which unnecessarily increase storage.

The Efficient Anonymous Authentication with Conditional Privacy-Preserving (EAAP) Scheme focus on authentication of vehicles based on conditional privacy preserving protocol in an anonymous manner. The RSUs continuously authenticates and verify messages whenever vehicles enter the range of RSUs and also before providing Location Based Safety Information (LBSI) messages. This schema tries to anonymously authenticate with low certificate and signature verification costs which are most essentially required in the VANET applications. In case of any malicious vehicle the RSU reports TA but, it does not store vehicles information and its messages for verification and tracking of messages also, it authenticates vehicle in First Come First Serve (FCFS) manner due to that emergency messaged vehicles get delayed.[9].

In [8, 10, 11, 13, and 16] has proposed Blockchain based VANETs to solve the issues such as identity, authenticity, validity and message reliability the bilinear pairing for elliptic curves is used to ensure the reliability and integrity when transmitting data to a node. Wherein consortium blockchain technology i.e. proof-of-work (PoW) provides a decentralized, secure, and reliable database.

In [12] a decentralized model is proposed using the group signature concept for authentication. This model provide threshold authentication with traceability and linking of messages for processing a batch of messages.

III. EXISTING SYSTEM

The existing system consists of registration, key generation, signature generation, verification and tracking. The flow of the system is as follows:

Registration: The vehicles and RSU nodes need to be registered in the TA before network deployment. The vehicle owners directy goes to TA and submit information such as aadhar card, mobile number, driving license, license plate number, etc. The TA will generate pseudonym and keys for each user and store it in vehicles device and also in its database for further tracking. Each RSUs location and keys also get stored in TA's database.

Key Generation: Whenever vehicle enters into the range of RSU, it selects random number as a temporary short-term private key and using that computes corrosponding short-term public key.

Signature Generation: To authenticate and preserve integrity of message, the vehicle produce short-term anonymous signature using short time anonymous keys and send that to RSU.

Verification: After reciving the message form vehicle the RSU authenticate vehicle and verify message. If everything seems to be correct it accepts the message and sends confirmation message to vehicle otherwise it discards the message and reports to TA for further tracking.

Tracking: In case of any dispute from RSU or vehicle, TA track the real identity from its datatbase and revels it to all RSUs and vehicles which revoke the privacy of the malicious vehicle user or RSU from causing any further damage.

Advantages:

The advantages of existing system are given as follows:

- The system uses bilinear pairing for elliptic curve for authentications, which is considered most secure.
- Blockchain PoW technology is used, which stores the data in most secure way.
- The tracking mechanism tracks malicious vehicle and revokes its identity to all other vehicles to prevent future damage.
- Each vehicle privacy is preserved by using pseudonyms for them.

Limitations:

The limitations of existing system are as follows:

- Every time when a vehicle enters the range of RSUs it gets authenticated, which effectively increases load on RSUs and waiting time for vehicles.
- All messages that are sent from vehicles to RSUs are treated same hence, in this fast-moving vehicle environment there is delay for emergency messages.
- High computational cost is required at all RSUs as complex operations are performed to add block in blockchain.

IV. SYSTEM OVERVIEW

In this section, the system model, bilinear pairing, elliptic curve cryptosystem and HMAC-SHA256 algorithm, which are used in the proposed method, are demonstrated below.

4.1 System Model

In VANETs, each vehicle is equipped with an on-board unit (OBU) which permits it to communicate with other vehicles and this type of communication is vehicle-to-vehicle (V2V) communication. Moreover, the vehicles can also communicate with roadside units (RSUs), which is as vehicle-to-RSU (V2R) communication. Through V2V and V2R communications, VANETs improve driving safety and convenience with safety messages as well as traffic messages. VANETs consist of three major components namely, OBU, RSU and TA.

OBU: An OBU is equipped in every vehicle as a transceiver to communicate with other vehicles' OBUs and RSUs. Each OBU has a tamper-proof device (TPD) to store the sensitive information such as authentication key received from TA, Sensors such as Global Positioning System (GPS) to provide the location, and event data recorder (EDR) to record information about vehicle crashes.

RSU: The RSUs are stationary devices deployed along the road or at dedicated locations such as at intersections or parking lots. The RSUs have network devices for dedicated short-range communication (DSRC) as well as authentication key stored received from TA. The main functions of RSUs are, authenticating vehicle, storing important messages in blockchain, maintaining private ledger which consists of all vehicle information and their authentication status, communicating with neighboring RSUs and vehicles in their range and reporting malicious activity to TA.

TA: TA is responsible for maintaining the trust and security of all VANETs including registering vehicles and RSUs. It maintains master database for vehicle information and local database for storing vehicles and RSUs authentication key. These databases are referred while tracking malicious vehicle or RSU.

4.2 Bilinear Pairing

Bilinear pairing is a pairing between elements of two multiplicative cyclic groups to a third group. Consider three multiplicative cyclic groups G1, G2, and GT with same order q, where q is a large prime. Let's consider g1 be a generator of G1, g2 be a generator of G2, and ψ be an isomorphism from G2 to G1 such that ψ (g2) = g1. The bilinear map $e : G1 \times G2 \rightarrow GT$, satisfies the following three properties.

1) Bilinearity: The mapping $e : G1 \times G2 \rightarrow GT$ is said to be bilinear if e (aP,bQ) e (abP,Q) = e (P,abQ) where ∀ a, b € Z*q and P,Q € G_T

2) Non-degeneracy: e (g1, g2) ≠ 1GT .

3) There exists an efficient algorithm to easily compute the bilinear map $e : G1 \times G2 \rightarrow GT$.[4]

4.3 Elliptical Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is a public key generation technique based on an elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

An elliptic curve is the set of points that satisfy a specific mathematical equation. The equation for an elliptic curve looks like this y2 = x3 + ax + b. ECC uses the mathematical properties of elliptic curves to produce public key cryptographic systems. ECC is based on mathematical functions that are simple to compute in one direction, but very difficult to reverse. In this, with ECC (Elliptic Curve Cryptography), large private number (x) is taken, and a point on the elliptic curve (G), and then multiply them together to produce public key, P = x*G.

4.4 HMAC-SHA256 Algorithm

HMAC-SHA256 is a type of keyed hash algorithm built from the SHA256 hash function and is used for vehicle authentication and message authentication. In HMAC method message is combined with secret key and hashes the result with the SHA256 hash function, the obtained result is again combined with the secret key, and then the SHA256 hash function is applied a second time to obtain output hash length of 256 bits.

V. PROPOSED SCHEMA

In VANET, the communication between vehicles is considered crucial to avoid road accidents and traffic jams. Later on, to preserve the integrity and authenticity of the message more focused is on security and privacy. In V2V communication, it is not necessary to maintain the confidentiality of each message because the vehicles are only able to send the message only after it gets authenticated by RSU. Thus, authenticating vehicles in less amount of time becomes a challenging task so that, vehicle do not remain idle at the time it wants to communicate with other vehicles.

Various systems have been proposed which focuses on reducing authentication time at each RSUs keeping security and privacy of vehicle constant. The vehicle needs to be authenticated each time so that, no malicious vehicle enters the system also, by keeping vehicle authenticated forever creates problems. Thus, in proposed system, the number of authentications is reduced to some extend so that, there won't be much delay in authentication and communication with other vehicles.

In order to obtain vehicle message passing record, blockchain's Proof of work technology is considered but it requires high computational cost at each RSUs as it compete among RSUs to add block in blockchain. Thus, in proposed schema, blockchain's Proof of authority technology is used to reduce computational cost. Also, to minimize storage only essential vehicles messages are stored in blockchain. Some of the emergency vehicles such as ambulance, fire brigade, etc. carries emergency message also, some vehicles pass messages of accident and traffic jam information therefore, based on the type of message the vehicles are prioritize and authenticated at RSU.

In dense network, as number of vehicles increases the load on RSUs also increases, making the system slow. The proposed schema reduces load on RSUs by reducing number of authentications and uses a PoA consensus algorithm to optimize the increasing time and make the system comparatively faster. The detailed explanation of the flow of the above framework is given as follows:

Registration: The vehicle users first directly goes to the TA and submits information such as Aadhar card details, phone number, driving license number, vehicle number, etc which is stored in master database of TA. Using this information TA generates necessary unique keys for each user vehicle using key generation process, it includes generation of original user identity (OID), dummy user id (DID) and random number which is stored in Local database. The mapping from original identities to dummy identities is done in TA only. After that, Authentication key which consists of dummy identity and random number is stored in vehicles Tamper Proof Device (TPD). The dummy identity protects vehicle privacy. The master database and local database is referred further while tracking particular vehicle.

Each RSU details such as location and dummy identity is stored in local database and the same is stored in RSUs in form of authentication key to identify malicious activity and physical damage at particular location.

Key Generation: As shown in Fig.1, the RSUs have their own private ledgers which maintains details received from neighbouring RSUs such as vehicle's pseudonym, its message, authentication status and timestamp. The timestamp goes on decreasing and as it reaches zero, the authentication status of that vehicle becomes unauthenticated. As vehicle enters the RSU range, RSU will check whether or not vehicle is authenticated. If the vehicle is not autenticated, RSU requests for authentication parameters else 'authentication successful' status is passed.

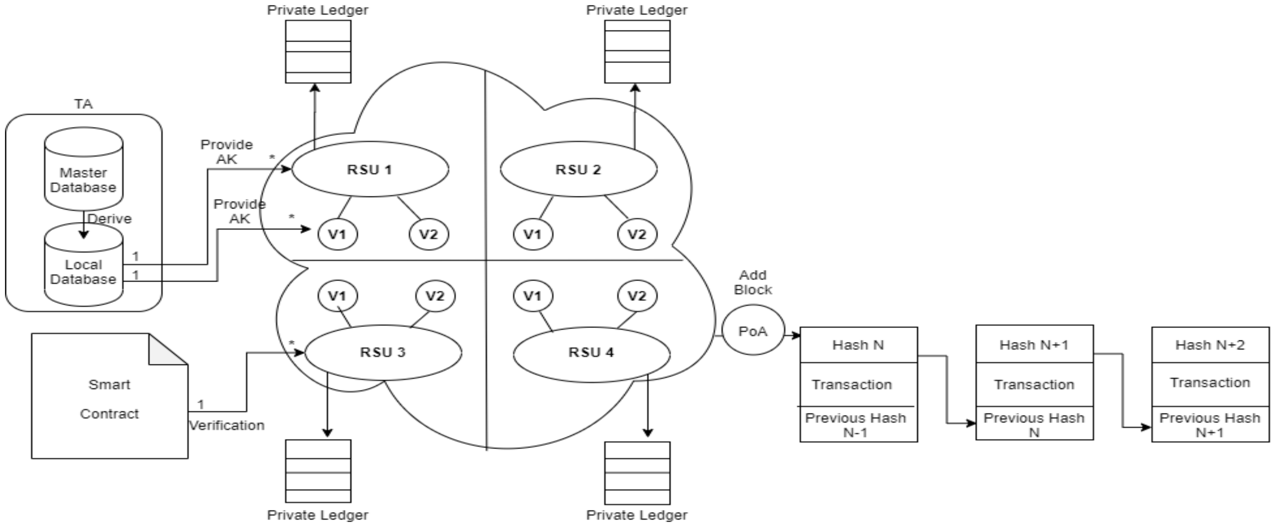

Figure 1: VANET using Blockchain

The authentication parameters are generated using bilinear pairing for elliptic curves. In which, the vehicle first selects random number as the temporary short time private key(x) and then takes a point on the elliptic curve (G) using that computes corresponding temporary short time public keys(P) as: P = x*G

Signature Generation: In order to preserve integrity of message M, vehicle generate short time anonymous signature using HMAC-SHA256 algorithm and private key. The vehicle first calculates hash of the message using HMAC-SHA256 algorithm and then map the hash value to a point on an elliptic curve as H(M). The signature of the message is then computed as, S = x*H(M)

Prioritazation, Verification and reducing authentications: The vehicle sends message, signature and public key to RSU as msg = (M || S || P), the msg is prioritize depending on the type of message M. Types of messages sent to RSUs are:

Message from ambulance and fire brigade.
Accident message from particular vehicle.
Traffic jam message.
Normal authentication message.
In which, 1 has highest priority while 4 has lowest priority.

The vehicle is authenticated at RSU if e(G,S) = e(P,H(M)) holds true else it is a malicious vehicle and is reported to TA by RSU. The integrity of message is also checked using HMAC-SHA256 algorithm. All this verification code is in the smart contract.

Consider a vehicle V1 in the range of RSU1 and is intended to travel towards RSU2. The vehicle is authenticated at RSU1 and is assigned with timestamp based on highest distance required to travel its neighbouring RSUs i.e. RSU2, RSU3 and RSU4 along with some time delay due to external factors. The vehicle information is then broadcast to its neighbouring RSUs. If the vehicle is able to travel the distance in the given timestamp into the range of RSU2, it is not authenticated again. The RSU2 just pass the message to the vehicle that it is an authenticated vehicle and there is no need of authentication again. But if the vehicle fails to travel the distance within the given timestamp into the range of RSU2, the RSU2 will send authentication request to vehicle and the vehicle will be authenticated again.

Tracking: The useful messages are stored by RSU in blockchain by using PoA in the form of a transaction. In case of dispute, TA track real identity by looking into its local database and blockchain database. After tracking the real identity, the TA revoke the privacy of the malicious vehicle or RSU from causing any further damage.

IV. PERFORMANCE ANALYSIS

Fig.2 shows the comparison between time at which authentication of nth vehicle is completed by existing system and proposed system. For existing system, as number of vehicles at particular RSU increases, the authentication time increases linearly. When vehicles enter the range of RSU, they are queued at RSU to complete authentication process. Each vehicle is treated the same hence, emergency vehicles such as ambulance, fire brigade, etc. and emergency message such as accident message get delayed. As fixed time is required to authenticate the vehicle, the graph is linear and time delay increases as number of vehicles increases. In proposed system, if a vehicle is authenticated at one RSU and it covers distance to another RSU in given time then, the RSU will send authentication successful message to vehicle hence, there is no need of re-authentication and queuing at RSUs. If vehicle fails to cover certain distance in given time then it will be queued and re-authenticated at RSU also, the emergency vehicles are prioritized based on message received at RSU.

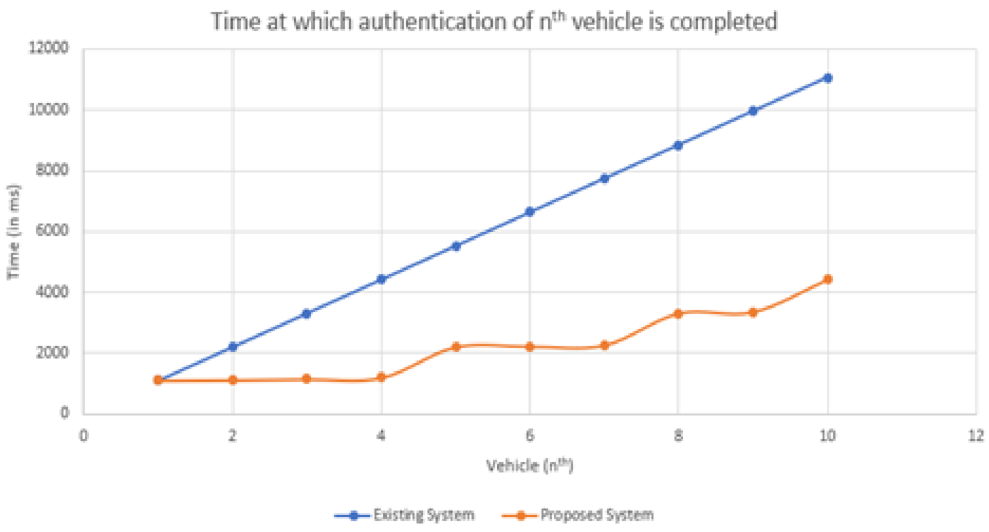

Figure 2: Time at which authentication of nth vehicle is completed

In existing system, after authentication completion of one vehicle, next vehicle's authentication begins. While authenticating certain vehicle, by that time no other vehicle can be authenticated. In the graph, the point represents time at which authentication of nth vehicle is completed while, the line represents authentication is in process. Hence, the graph is linear. For proposed system, as private ledger stores the information from neighboring RSUs of already authenticated vehicles and their timestamp, while authenticating 2nd vehicle, 3 vehicles arrives in that time which are already in private ledger and within timestamp then that vehicles receives authentication successful message at the time at which they enters into the range of RSU. So, there is no need of queuing and reauthentication for that 3 vehicles and hence, for 2nd vehicle after completing the authentication process it is authenticated as 5th vehicle. In this way, the number of authentications is reduced.

V. CONCLUSION

In this paper, we have proposed a new approach to optimize and reduce authentication time of vehicles and store messages using PoA which effectively increases efficiency of the system. In the proposed schema, initially vehicle's message, signature and public key is generated and passed to RSU. Later, RSU prioritise messages and authenticate vehicles. The essential data is then added in blockchain and authenticated vehicle's information along with timestamp is passed to adjacent RSU's which decides authenticity of vehicle based on arrival time of particular vehicle. The proposed schema provides better efficiency in terms of authentication and adding block in blockchain than the previously reported schemes. In future research, we will authenticate vehicles simultaneously using multicore and improve the efficiency of our proposed solution.

REFERENCES

1. Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, & Xuemin. (2008). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. *IEEE Conference on Computer Communications*.
2. Zhi-chi Liu, Ling Xiong, Tu Peng, Dai-Yuan Peng, & Hong-Bin Liang. (2018). A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access.*
3. X. Lin, X. Sun, P.-H. Ho, & X. Shen. (2016). GSIS: A secure and privacy preserving protocol for vehicular communications. *IEEE Transportation Vehicle Technology.*
4. Lei Zhang, Qianhong Wu, & Josep Domingo-Ferrer. (2017). Distributed aggregate privacy preserving authentication in VANETs. *IEEE Transactions on Intelligent Transportation Systems*.
5. Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, & Woong Cho Santamaría. (2016). A security and privacy review of VANETs. *IEEE Transactions On Intelligent Transportation Systems*.
6. A. Wasef, & X. Shen. (2016). Privacy preserving group communications protocol for vehicular ad hoc networks. *IEEE ICC.*
7. Dijiang Huang, Satyajayant Misra, & Guoliang Xue. (2011). PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Transactins on Intelligent Transportation Systems, 12*(3).
8. Xiaohong Zhang, & Xiaofeng Chen. (2019). Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access.*
9. Maria Azees, Pandi Vijayakumar, & Lazarus Jegatha Deboarh. (2019). EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Transactins on Intelligent Transportation Systems, 18*.
10. Lixia Xie, Ying Ding, Hongyu Yang, & Xinmu Wang. (2019). Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs. *IEEE Access*.
11. Youcef Yahiatene, & Abderrezak Rachedi. (2018). Towards a blockchain and software-dened vehicular networks approaches to secure vehicular social network. *IEEE Conference on Standards for Communications and Networking*.
12. Jun Shao, Xiaodong Lin, Rongxing Lu, & Cong Zuo. (2016). A threshold anonymous authentication protocol for VANETs. *IEEE Transactions on Vehicular Technology, 65*(3).
13. Pradip Kumar Sharma, Seo Yeon Moon, & Jong Hyuk Park. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of Information Processing System, 13*(1).
14. Zhaojun Lu, Gang Qu, & Zhenglin Liu. (2018). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems.*
15. Hong Liu, Yan Zhang, & Tao Yang. (2017). Distributed aggregate privacy-preserving authentication in VANETs. *Security and Privacy of Connected Vehicular Cloud Computing*.
16. Hong Liu, Yan Zhang, & Tao Yang. (2018). Blockchain-enabled security in electric vehicles cloud and edge computing. *Security and Privacy of Connected Vehicular Cloud Cmputing.*