Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 12. Issue.01, PP. 156-163, June 2024
https://doi.org/10.22555/pjets.v12i1.1054
E-ISSN 2224-2333
P-ISSN 2222-9930

HES: Hash-Based Efficient Secure Model For Vehicular Ad Hoc Network

Qazi Ejaz Ali[1*], Murad Hussain[1], Ibrar Ahmad[1], Waheed Ur Rehman[1], Abdul Haseeb Malik[1], Tabinda Salam[2]

[1] Department of Computer Science, University of Peshawar.
[2] Department of Computer Science, Shaheed Benazir Bhutto Women University Peshawar

[*]Corresponding Author: qaziejazali@uop.edu.pk

Abstract:

Intelligent Transport System (ITS) provides an extensive range of applications, such as road safety, comfort, security, and efficient use of transportation. It is vital to shield reserved facts, and the revocation of harmful vehicles should only occur once malicious activity is observed. Procedures of ITS include Vehicles (Vs), Certification Authority (CA), and Road Side Units (RSUs). It is seemly not to expose the real identity of an ITS station that is a vehicle, during the communication. Through the rapid evolvements in-vehicle technologies, extraordinary throughput satellite communication, cyber-physical systems, the Internet of Things (IoT) and the Internet of Vehicles (IoV) have developed as a substantial research effort for expressive applications in current ages. IoV empowers linked and autonomous vehicles to be involved with ITS environments, covering infrastructure, computing nodes, sensors, and other entities. Vehicular ad hoc networks (VANETs) contribute to developing driving efficiency and security by reducing traffic congestion and avoiding accidents. However, the ad hoc nature of VANETs leads to numerous types of possible attacks, such as modification of beacons, a man in the middle, Sybil, and side-channel attacks. These attacks result in the deprivation of VANETs, abiding malicious vehicles to misinform lawful vehicles for personal gain. To achieve the objectives of VANETs, it is vital to implement strong security measures. Though various techniques have been suggested but face different challenges such as communication delays, computational overheads, and security. This paper suggests an efficient hash-based method to reduce communication delays and computational overheads and prevent the mentioned security attacks. The results show that the proposed technique provides less computational overheads, minimizes communication delays, and provides security.

Keywords: *Internet of Vehicle, Hash, Authentication, Integrity*

I. INTRODUCTION

Intelligent Transport System (ITS) subclass Vehicular Ad hoc Network (VANETs) provides inter Vehicular communication in order to remove accidents, and congestions and improve road wellbeing [1]. Vehicular Communication is positioned for the escaping of bottlenecks and mishaps. In order to provide road safety, intellect should be installed in vehicles [2]. In VANETs, Dedicated Short Range Communication (DSRC) enables vehicles to communicate with each other [2-4]. Another name of DSRC is Wireless Access in Vehicular Environment (WAVE)/IEEE 802.11P [2]. In VANETs, individual vehicles interconnect with one another and likewise over the set-up to attain road protection and traffic productivity [3]. Nevertheless, due to the VANET's wireless linkage, active and passive threats are conceivable, which distress the safety and concealment of automobiles.

In order to prevent different types of attacks, the researcher tried their best to develop different models, in one of which is a hashing technique that guarantees verification and truthfulness [2]. Facts communication among different entities for instance vehicles and Road Side Units (RSUs) through hash function. In order to provide authentication and integrity features, hashing techniques are used, even a slight alteration yields absolutely altered hash, which cannot be verified. In addition, Blockchain technology is expanding hashing systems [3]. A blockchain stores encrypted block of records and chains them collected to produce a true basis of detail in lieu of the records. Nakamoto in 2009 introduced Blockchain technology [4].

In VANETs, the authors of [5] planned a physical-based (PHY-based) verification model, which uses the physical features of mutually received signals and ambient indicators to guard against replay attacks. However, it leads a great computational and communication overheads. In [6], the authors planned a mechanism, in which unidentified communications will be disseminated. However, this technique presents the issue that if a bogus message is disseminated then how the malicious vehicle will be revoked. In [7], the researchers projected a method, which is established on a sole unified database. However, the sole central idea presents internal threats. Ali et al. [8] suggested numerous types of reservation and secrecy threats as well as their possible solutions, though no efficient solutions are designed.

Azam et al. [9] suggested a technique based on software-defined network and blockchain for VANETs verification. The researchers tried to solve the security and privacy problem, but there exist syntactic linking attacks. According to the present research, all of the techniques for VANETs suffer from diverse kinds of active attacks, computational costs, and communication delays.

Therefore, there is a requisite for a trustworthy technique that can efficiently address VANETs security and privacy issues like side channel, phishing, modification and replay attacks, along with high communication overheads, and computational costs. In the suggested research as shown in Figure 1, a technique based on hashing is advised to address the above problems efficiently. The technique based on hashing has the potential to solve numerous of the problems now threatening the ITS environment. One of the most persistent alarms in VANETs is dealing with social concerns, and Hashing method is a pleasant resolution. Intelligent system uses a variety of initiation vehicle statistics as input to generate traffic planning efficiently. Vehicles facts in the input is viewing to malicious threats due to the restricted computing capability in the real time. Perceiving malicious attacks are puzzling. In the proposed research work a hash based technique is incorporated in the current VANETs scheme to guarantee security and privacy meaningfully. During the information communication phases by vehicles and authorities, communication integrity is preserved. The main aim of this paper is to design an efficient technique to address the security issues in VANETs, which will guarantee the following objectives:

- The illegal access of malicious vehicles will be prevented.
- The computational cost in communication generation and verification will be reduced.
- To deliver communication integrity in all the phases.

The rest of the paper is organized as; Section 2 consists of the literature review, Section 3 presents network model, Section 4 presents performance analysis, Section 5 shows conclusion and future work. The introduction must contain Motivation, Related Work, Contribution and Organization.

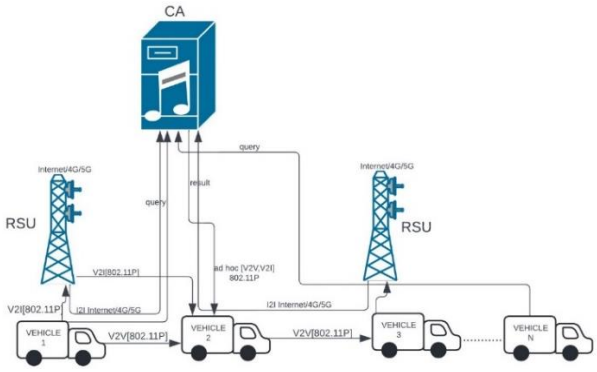

Figure 1: System Model

II. LITERATURE REVIEW

This section describes the literature review and the goal behind the suggested technique. VANETs are the most emerging area of research in the current era. Besides the advantages of VANETs, there exist security attacks that make it vulnerable. Due to the ad hoc nature of VANETs, it develop an easy target of a vehicle for the attackers. Furthermore, it is not appropriate for situations connecting various vehicles and extreme data clues to extensive interruptions or misperception. To address these problems, different analyses have been established with an emphasis on research. Through hash technology, verification and authentication statistics in VANETs can be achieved to begin keys for

recording information. The secrets are easily accomplished by the administrators over certificates. Over a distribution arrangement, the hash method file can be formed and protected by sharp encryption measures, intelligent protocols, and other advanced knowledge.

Lu et al. [5] suggested a technique that depends on the physical features of the received communication to guard against falsification attacks in VANETs. However, this method comes with the drawback of high computational and communication costs. In [6], the authors offered a model including the transmission of unidentified messages. However, this model presents a challenge regarding how to revoke a malicious vehicle if a malicious message is disseminated. In [7], a method based on a single centralized database was suggested. However, the use of a single centralized idea increases the concern of internal attacks.

Ali et al. [8] placed numerous types of security and privacy threats alongside possible solutions, but the challenge lies in proficiently including those solutions. In [9], the writers labeled a security technique for VANETs. Nevertheless, the centralized environment of this approach increases concerns about internal attacks, showing off a threat to the secrecy of VANETs. The authors of [10] projected a technique for safeguarding VANETs deprived of trusting RSUs. However, the method faces scalability concerns due to its use of proof of work, subsequent in high computational overheads.

In [11], a scheme for VANETs was employed, though this idea raises a reliable communication atmosphere against internal threats, challenges persevere in terms of scalability, high computational overheads, and vulnerability to instillation attacks. The writers of [12] applied obscurity to transfer beacons regarding the broadcast and legitimacy of protection communications. However, the model lacks the revocation process. In [13], researchers planned a technique that depends on Software-Defined Networking and Blockchain for VANET verification. Though striving to address security concerns, the researchers come across a syntactic linking attack, compromising the complete security.

In [14] the researchers presented Conditional Privacy-Preserving Authentication (CPPA) for VANETs that utilize elliptic curve cryptography. The authors revealed that the method is empirically safe against identity attacks and adaptive chosen communication attacks in the random oracle model, but incurs high computational overhead. In [15] the writers designed a blockchain-based verification procedure, though, it is noted that the approach faces scalability issues due to its high computational and communication overheads. The authors of [16] presented a technique that works well in sparse scenarios but does not work well in dense scenarios due to its computational overheads. In [17], the researchers designed a technique, but there are possible weaknesses, for instance, Sybil, Man in the Middle (MIM), and injection attacks. The authors of [18] presented a privacy-preserving method for vehicle security. However, it is disposed to Sybil and MIM attacks. In [19] the authors projected a scalable and privacy-preserving verification protocol for the IoV. However, the recommended method is vulnerable to numerous types of attacks such as MIM and replay attacks. Nie et al. [20] presented an authentication method for V2I communication, which allows for the generation of many messages with signatures when fresh vehicles join VANETs, the effectiveness of verification can be suggestively enhanced through group validation of these signatures. However, it is prominent that the planned technique does not efficiently work in a V2V environment due to a high computational overhead. In [21] the authors offer a forthright tool for privacy preservative confidence assessment. The structure shows stability among trust assessment and secrecy safety though striking nominal overheads. However, probable weaknesses such as side channel and replay attacks are identified. The researchers in [22] presented a multi-zone verification and privacy preservative protocol that unveiled important improvements compared to previous methods, particularly decreasing signature formation time through the use of short bilinear pairing signatures. However, this technique is vulnerable to syntactic linking attacks.In [23] it is projected that the improved certificate less and provably secure conditional privacy-preserving authentication practice, precisely considered for automatic situations. However, it is noted that there are high computational and communication overheads related to this practice.

In [24] the authors presented a technique, which offers a slight, secure, efficient verification and key arrangement scheme to establish secure communication in VANETs. The method employs lightweight treating but is vulnerable to different kinds of attacks such as replay and MIM attacks. In [25] researchers tried to suggest information about an efficient V2I verification system. However, the structure is accompanied by high computational and communication overheads. The authors of [26] suggested a lightweight identity authentication procedure, but the scheme is prone to side-channel attacks. In [27] the authors considered a privacy-preserving lightweight authentication mechanism, but

it is vulnerable to replay, phishing, and MIM attacks. Subsequently detailed investigation, it is highlighted that it is essential to design a technique that addresses VANETs security and privacy issues such as replay, MIM, and phishing attacks with low computational and communication overheads.

III. NETWORK MODEL

This section includes the System model, Design Goals, and Methodology of the proposed research work.

A. System Model

There are three main performers in the proposed model, which are Authentication Server (AS), Road Side Unit (RSU), and Vehicles (V). The AS and RSU are assumed to be entirely trustworthy, while the vehicles are presumed to be completely devious. Each vehicle contains an On Board Unit (OBU) with storage and processing capabilities that communicate with the AS, RSUs, and other vehicles. Furthermore, in VANETs, the communication channels are insecure. Therefore, a hacker can launch attacks. In order to avoid the attacks and make VANETs trustworthy, the proposed system model is shown in Figure 1. The proposed model consists of CA, RSU, and V. Each V communicates with CA, and RSUs through 4G/5G, while up to 1000 meters range with other Vs through DSRC/ WAVE [2]. A CA can originate valued information from validly established communications. In addition, CA manages VANETs and supports RSU to confirm the vehicle. It gets and permits information from a vehicle within its range. The initial hash is installed in the V OBU, which guarantees authentication and integrity of the messages during Vehicle to Vehicle (V2V) communication.

B. Design Goals

The following are the design goals of the proposed work:

Communication Integrity: One of the most vital apprehensions in the plan process is communication integrity which means that any deviations made to a communication should be perceived by the receiving vehicle.

Communication Confidentiality: If an attacker gets a message, it provides no information to the attacker.

Stampede Strategy Privacy: If any RSU is attacked, the real identity of the vehicle cannot be assumed.

Drive Partaking Secrecy: In communication, RSU and other vehicles cannot know the actual identity of the V.

C. Methodology

The proposed technique, which is shown in Figure 2 will be implemented in MATLAB [28]. The system, which is used for the implementation of the proposed model is core i5 with 8GB RAM. The following steps are involved in the proposed HES model:

Step 1: Vehicle requests from CA for registration.

Step 2: CA calculates the hash of the V wish and directs the preliminary pseudonym to the vehicle beside the hash.

Step 3: CA informs RSU regarding the V hash.

Step 4: The V requests RSU for communication pseudonyms.

Step 5: Once confirmation of hashes, RSU issues pseudonyms for communication to the V.

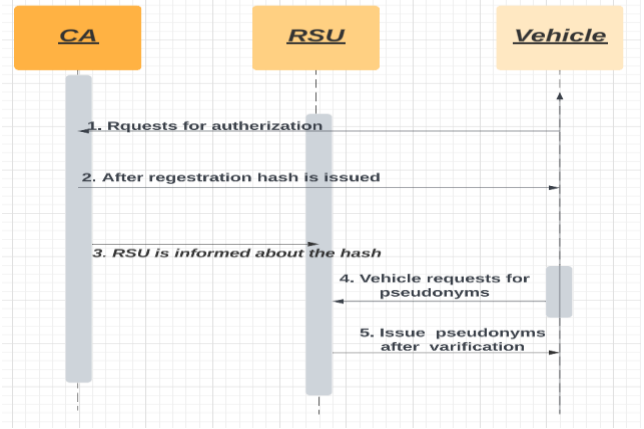

Figure 2: Proposed Methodology

In incident of a malicious action, hash will be demanded sideways with the communication. The CA will be presented with the hash with the pseudonym of the attacked vehicle. In this technique, the malicious vehicle will be repealed from the ITS network. The proposed HES process as shown in Algorithm 1 is implemented in the designed technique. The notations of the suggested technique are given in Table 1.

$Algorithm\ 1\ HES\ protocol$

$1: V \rightarrow CA: KCA[(Vid \,||\, Vinfo)]$
$2: CA \rightarrow V: KV[H(Vid \,||\, CAid) \,||\, P1 \,||\, LT1]$
$3: CA \rightarrow RSU: KRSU[H(Vid \,||\, CAid) \,||\, P1]$
$4: V \rightarrow RSU: KRSU[H(Vid \,||\, CAid) \,||\, P1)]$
$5: RSU \rightarrow V: KV[P2, P3, P4, LT2]$

Table 1: Notations

Notation	Description
V	Vehicle
V_{id}	Vehicle Identification
RSU	Road Side Unit
CA	Certification Authority
CA_{id}	Certification Authority Identification
K_{CA}, K_{RSU}	Secret key of CA and RSU
K_v	Secret key of Vehicle
P_1	Pseudonym 1
H	Hash
||	Concatenation

IV. PERFORMANCE ANALYSIS

In this section, the proposed model is analyzed to check its robustness. This section includes Overhead ratio, Computational cost analysis, and Attack model. The simulation parameters are given in Table 2.

Table 2: Simulation Parameters

Parameters	Value
Vehicle speed	50 miles/hour = 22.35 meters/second, Smax = 70
Safety distance (Ds)	10 meters
Vehicle acceleration	a_min= 0 meters/seconds, a_max = +(-) 5 meters/seconds
Miles/hour	31.29 meters/second
Vehicle Arrival rate/Departure rate	0.833
Road Traffic Volume	vol = 3000 vehicles/hour/lane
Minutes	2
Road Traffic Density	100-500 vehicles/lane
Range	50

A. Overhead ratio

The overhead ratio of the HES and without HES is shown in Table 3. The simulation results shown in Table 3 regularly reveal similar developments through sparse and dense scenarios. Therefore, the proposed methodology has no effect on the overhead ratio.

Table 3: Overhead Ratio with HES and Without HES

Number of Vehicles	With HES	Without HES
2	3.107ms	0.402ms
3	0.074ms	0.006ms
4	1.658ms	0.061ms
5	0.987ms	0.044ms
6	0.441ms	0.136ms
7	0.033ms	0.030ms
8	0.028ms	0.010ms
9	0.026ms	0.002ms
10	0.282ms	0.146ms
11	0.213ms	0.008ms
12	0.026ms	0.004ms
15	0.209ms	0.007ms
15	0.188ms	0.006ms
15	0.897ms	0.394ms
16	0.186ms	0.002ms
20	0.037ms	0.004ms
10	0.282ms	0.146ms
43	1.471ms	1.186ms

B. Computational Cost Analysis.

The computational cost is evaluated and is specified in Figures 3, and 4 respectively, the message generation time is very low, though the message verification time is also low. In Figures 3 and 4, the number of vehicles is shown on the x-axis, though the time delay is shown on the y-axis. Intensifications in transportation size will certainly outcome in greater delays. In the case of a single vehicle request, there is less delay. Due to several requests received at a time, the vehicles are experiencing delays. However, the delay in the case of HES and without HES has no significant differences in sparse and dense scenarios. In Figure 5, the number of Vs is shown on the x-axis, while operational cost is shown on the y-axis. As the vehicles increase the operative cost increases. However, there are no significant differences between HES and without HES scenarios.

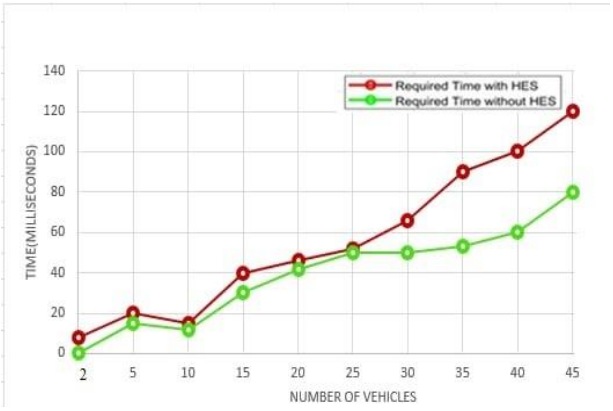

Figure 3: Time for V2V Communication

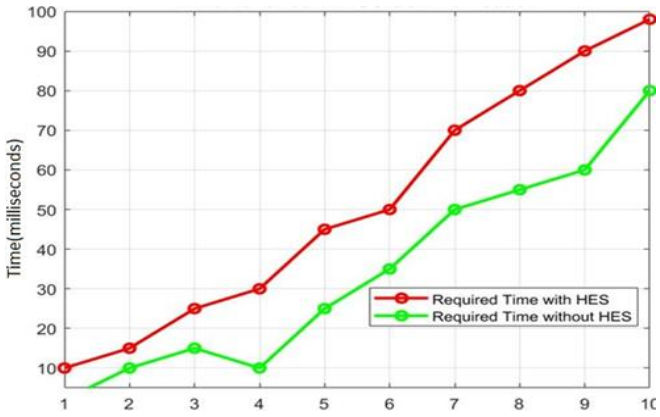

Figure 4: Time for Vehicle to RSU Communication

The communication cost of the HES is a little bit high than without HES, which is a tradeoff between security and without security parameters that is depicted in Figure 6.

C. Attack Model

In order to realize determined restricted anonymity and concealment, the subsequent diverse kinds of risk scenarios are measured in the proposed model.

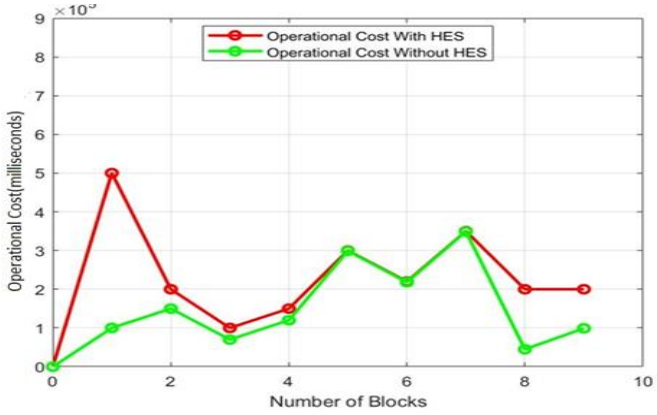

Figure 5: Operational Cost

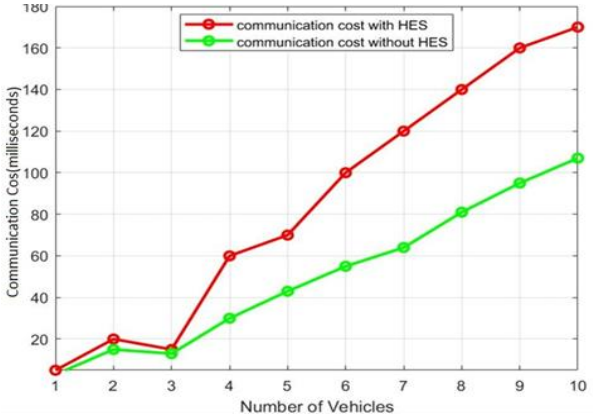

Figure 6: Communication Cost Comparison

- Communication between V2V and V2I are hash protected. Therefore, it is difficult for an opponent to alter the communication, which guarantee the integrity feature.
- An attacker cannot get the real identity of the V during communication, as it is pseudonymized.
- If any RUS is attacked, the attacker cannot get the actual information of the vehicles.
- Likewise, the database of the CA holds coded materials, therefore, attacked of the CA database reveal no beneficial evidences to any attacker.

V. CONCLUSION AND FUTURE WORK

In VANETs, the experiments of sporadic connectivity and dynamic topology rise severe alarms about security and privacy. The proposed model HES addresses these concerns efficiently. This approach prevents the association between pseudonyms and actual identities through illegal ways. Even during a wicked vehicle revocation level, HES safeguards the protection of actual identity by safeguarding it from RSUs. HES reveals efficiency in complex situations, removing the opportunity of replay and MIM attacks. The results specify a reliable growth in delivery ratio, convoyed by a decrease in overhead ratio, and operational costs. HES, when together with lively secrecy, emerges as one of the utmost real methods in minimizing computational costs. In future, HES will be implemented and evaluated through mathematical model with several RSUs and finally it will be combined with the cloud setting to make Internet of Vehicles.

REFERENCES

[1] Zhou, X. Luo, M. Vijayakumar, P. Peng, C. & He, D. Efficient certificateless conditional privacy-preserving authentication for VANETs. IEEE Transactions on Vehicular Technology. (2022), 71(7), 7863-7875.

[7] Jan, S. A.; Amin, N. U.; Othman, M., Ali, M., Umar, A. I., & Basir, A. A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues. IEEE Access. 2021, 9, 153701-153726.

[8] Ali, Q. E.; Ahmad, N.; Malik.; A. H, Ali, G, & Rehman.; W. U. Issues, challenges, and research opportunities in intelligent transport system for security and privacy. Applied Sciences. .2018, 8(10), 1-24.

[9] Azam, F.; Yadav, S. K.; Priyadarshi, N.; Padmanaban, S.; & Bansal, R. C. A comprehensive review of authentication schemes in vehicular ad-hoc network. *IEEE access*. 2021, *9*, 31309-31321.

[10] Chen, Z.; Li, J.; Wang, J.; Wang, S.; Zhao, J.; & Li, J. Towards hybrid gait obstacle avoidance for a six wheel-legged robot with payload transportation. Journal of Intelligent & Robotic Systems. 2021,102(3), 1-21.

[11] Manikandan, D.; Moni, S. S.; & Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs). Vehicular Communications. 2020, 25, 1-18.

[12] Mohamed, T. M.; Ahmed, I. Z.; & Sadek, R. A. Efficient VANET safety message delivery and authenticity with privacy preservation. PeerJ Computer Science. 2021, 7, 1-16.

[13] Martinez, C. M.; Heucke, M.; Wang, F. Y.; Gao, B.; & Cao, D. Driving style recognition for intelligent vehicle control and advanced driver assistance: A survey. IEEE Transactions on Intelligent Transportation Systems. 2017, 19(3), 666-676.
[14] L. Wu *et al.*, "An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular Ad Hoc network," IEEE Access. 2019, 7, 55050–55063.
[15] S. Tangade and S. S. Manvi, "Scalable and privacy-preserving authentication protocol for secure vehicular communications," 2016 IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2016, 2017, 1-16.
[16] S. J. Yu *et al.*, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," Appl. Sci. 2020, 10, 1-5.
[17] S. Ansari, J. Ahmad, S. Aziz Shah, A. Kashif Bashir, T. Boutaleb, and S. Sinanovic, "Chaos-based privacy preserving vehicle safety protocol for 5G Connected Autonomous Vehicle networks," Trans. Emerg. Telecommun. Technol. 2020, 31, 1–16, .
[18] M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles," IEEE Internet Things J. 2021, 8, 1123–1139.
[19] H. H. Nie, Y. P. Li, and Q. H. Wu, "A privacy-preserving V2I authentication scheme without certificates," J. Inf. Sci. Eng. 2017, 33, 4, 1025–1040.
[20] Z. Liu *et al.*, "LPPTE: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications," Inf. Fusion. 2021, 73, 144–156.
[21] T. M. Mohamed, I. Z. Ahmed, and R. A. Sadek, "Efficient VANET safety message delivery and authenticity with privacy preservation," PeerJ Comput. Sci. 2021, 7, 1–21.
[22] P. C. Science, "Conditional Privacy-Preserving Authentication Protocols for Vehicular Ad Hoc Networks Dissertation," 2019.
[23] Y. Zhou, S. Liu, M. Xiao, S. Deng, and X. Wang, "An Efficient V2I Authentication Scheme for VANETs," Mob. Inf. Syst. 2018, 2018, 1-25 .
[24] Y. Liu, W. Guo, Q. Zhong, and G. Yao, "LVAP: Lightweight V2I authentication protocol using group communication in VANETs," Int. J. Commun. Syst. 2017, 30, 1–11.
[25] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in internet of vehicles," IEEE Trans. Veh. Technol. 2020, 69, 6709–6717.
[26] Mahmood, J.; Duan, Z.; Xue, H.; Yang, Y.; Berwo, M. A.; Khan, S. A., & Yassin, A. A. K. A. Secure message transmission for V2V based on mutual authentication for VANETs. Wireless Communications and Mobile Computing. 2021, 1-16.
[27] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," IEEE Access. 2021, 15633–15642.
[28] AkbarZadeh, O.; Khosravi, M. R.; & Alex, L. T. Design and MATLAB simulation of Persian license plate recognition using neural network and image filtering for intelligent transportation systems. ASP Transactions on Pattern Recognition and Intelligent Systems. 2022, 2(1), 1-14.