INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS

Received: 08-08-2023

Accepted: 30-10-2023

Published: 11-12-2023

Citation: Sajini S, Anita EAM, Janet J (2023) A Block Chain Based Authentication Scheme in VANET for a Secure Data Communication Using SHAH Algorithm. Indian Journal of Science and Technology 16(46): 4291-4299. https://doi.org/10.17485/IJST/v16i46.2010

* **Corresponding author**.

sajinisham13@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

A Block Chain Based Authentication Scheme in VANET for a Secure Data Communication Using SHAH Algorithm

S Sajini[1,2]*, E A Mary Anita[3], J Janet[4]

1 Research Scholar, Anna University, Chennai, Tamil Nadu, India
2 Assistant Professor, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India
3 Professor, Department of Computer Science and Engineering, School of Engineering and Technology, Christ University, Bengaluru, Karnataka, India
4 Professor, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract

Objectives: In Vehicular Ad Hoc Networks (VANETs), ensuring secure data communication is essential to uphold the integrity and reliability of vital vehicular applications. This study presents an innovative authentication scheme based on block chain technology, specifically designed to enhance data exchange security within VANETs. With a successful deployment and integration into our transportation systems, VANETs promise safer roads, reduced traffic congestion, and more efficient traffic management. These networks offer immediate communication of vital information to drivers, such as traffic conditions, accidents, and roadwork, helping to reduce accidents and save lives. VANET can enable intelligent traffic management, making real-time adjustments to traffic signals and routes based on data from the network. This can lead to reduced travel times and improved fuel efficiency, resulting in cost savings and reduced emissions. **Methods:** The scheme utilizes the SHAH (Secure Hash Algorithm with HMAC) Algorithm as a foundational component to safeguard data authenticity and confidentiality. Our proposed block chain-based authentication approach capitalizes on the decentralized nature of block chain technology, establishing a robust and tamper-resistant ledger for authentication purposes. This helps to secure data transmission. **Findings:** A comprehensive analysis of the proposed scheme showcases its efficacy in ensuring secure data communication within VANETs. These findings underscore the significant value of our proposed approach, contributing to a safer and more dependable environment for vehicular communication, thereby enhancing the overall reliability of VANET applications. **Novelty:** As a concluding note, this research not only introduces a unique block chain-based authentication scheme tailored specifically for VANETs but also underscores the indispensable role played by the SHAH Algorithm in achieving data security. The outcomes presented in this study inspire further exploration at the intersection of block chain and VANET technologies, ultimately advancing the state of secure vehicular communication.

Keywords: VANET; Block chain; Authentication; Trusted Authority; RSU

1 Introduction

VANET (Vehicular Ad hoc Network) is a network to communicate with vehicles and broadcast messages to all other vehicles in case of emergency. Distribution of messages such as traffic information, entertainment, and emergency as well as identification messages during its passage to other vehicles essentially many safety problems faced. VANETs provide a pleasurable and impractical driving experience for vehicle drivers.[1] Types of communications, the vehicle-to-vehicle (V2V) communication and the vehicle-to-roadside unit (V2R) communication, are accepted in VANETs to make comfortable between vehicle users and broadcast relevant driving information through the dedicated short-range communication (DSRC) radio[2].

The potential of block chain technology to improve security and trust across different fields has been acknowledged by researchers. The decentralized characteristics and resistance to tampering that block chain offers present an encouraging basis for tackling the security issues within VANETs.[3] Through the integration of block chain into VANETs, a strong authentication system can be established, ensuring the integrity of data shared between vehicles and infrastructure and safeguarding the network from malicious entities.[4,5]. Every vehicle and user information in VANET is maintained on a block chain basis.[6,7]. Additionally, upkeep of the decentralized, unreliable VANET system's dependability and prevention of vehicle users' misconduct are difficult duties[8]. This study is positioned to represent significant progress in enhancing the security of VANETs. It aims to address the deficiencies in current authentication methods by capitalizing on the capabilities of blockchain technology and the SHAH algorithm.

In the swiftly changing environment of interconnected cars and intelligent transportation systems, ensuring the safety of data sharing within Vehicular Ad Hoc Networks (VANETs) has become a crucial factor. The trustworthiness, secrecy, and genuineness of data are vital to guarantee the dependability and safety of vehicular uses. Conventional security methods are encountering difficulties in countering new risks, like unauthorized entry and data tampering. Thus, there is a significant requirement for creative strategies that can successfully enhance the protection of data transfer in VANETs. Our proposed algorithm helps to find the different type of attack revolves around generating numerous counterfeit personas (referred to as Sybil nodes) with the intention of obtaining influence over a substantial segment of a blockchain network. In decentralized frameworks like blockchain, where there is no central governing body, malevolent entities find it simpler to fabricate these counterfeit identities, which could ultimately lead to the disturbance of the network's functioning.

2 Methodology

Real-time deployment is difficult to manage at VANET for data like user and vehicle privacy information. Block chain-based authentication is one of the strategies employed by VANET to prevent this kind of security vulnerability.[9] A Privacy Protection Verification (BPPA) system for VANET that uses block chains and transparently and irreversibly records all transactions.[10,11] A decentralized authentication system without a revocation list was offered via block chain-based personal information protection authentication. Only in the event of a disagreement can the ability to establish a link between the certificate and the real ID be revealed; it is encrypted and stored on the block chain.[12] On VSN-backed block chains, effective knowledge sharing is the topic that was envisioned. Effective information sharing uses two mechanisms: an anonymous creation process and an identity-based signature mechanism.[13] Edwards-curve Digital Signature technique is utilized to improve the execution in the authentication process, and Elliptic Curve Diffie Hellman (ECDH) technique is proposed for trustworthy key exchange. Performance study shows how much computation resources are saved by the protocol.[14] Proposed a study based on the block chain technology, a framework for traceable distributed systems that allows for secure data access. It improved the efficiency of vehicle information and driver personal information using block chain technology.[15,16] Proposed a mutual authentication-based improved lightweight secure authentication protocol (ELSAP) that ensures networks' survivability. Calculating communication costs was significantly more accurate. Delegation proof-of-stake consensus algorithm improved for uninterrupted data flow to RSU. For secure data transmission, 5G and block chain were both utilized.[17] Proposed conditional privacy protection is based on Chebyshev polynomials that include group key sharing and authentication for VANET. This technique effectively utilised TA and is utilized to maintain track of the nodes.[18] It was suggested to use the CDSPP algorithm, which uses verified signatures and effective routing protocols to verify vehicles and send data between authenticated nodes. The CDSPP approach boosts packet transmission speed.[19,20] Developed a drone-supporting block chain-based trust mechanism to prevent the reporting of fraudulent data in the IoT.[21] Proposed an ASCII ECC method for a cryptography-based system. Additionally, there is still a problem with how to monitor the misbehavior of entities (such CAs and RSUs) while avoiding frequent online contacts with the certificate services. It's crucial to regularly access node and message trustworthiness using trust models since node trust and event message trust are two of the biggest obstacles to safeguarding communication in the VANET.

2.1 Block Chain-Based Authentication Scheme Architecture

RSU, or vehicle-to-vehicle communication, is crucial to this system. It is advised to use a block chain-based authentication system while delivering secure messages. All messages are sent as blocks using technologies built on the block chain. Figure 1 illustrates how a block chain is a publicly accessible distributed database of all completed digital transactions shared among participating nodes. The majority of network nodes reach a consensus that all events in the block chain database are legitimate. Anyone can join and participate with a public block chain because it is an open network and no central authority is required.

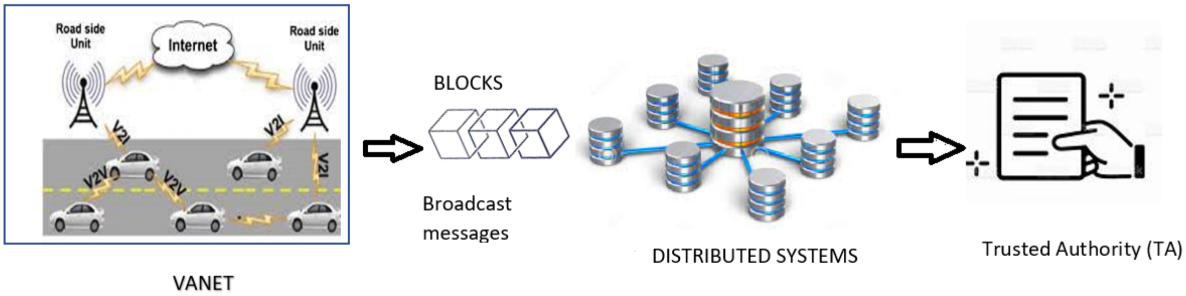

Fig 1. VANET Architecture

The structure of each block contains the block header and the block body. The block header consists of a hash, a nonce, a timestamp of the previous block, and a Merkle root, as illustrated in the Figure 2. The block content comprises a list of transactions and some additional data, depending on the requirements of the block chain.

We propose a blockchain-based authentication system in VANETs, where all nodes use an authentication scheme to communicate with all other nodes in a secure way. This system purely depends on security which shows in Figure 3. The hash function's encryption is employed to store information in a link, and the data becomes malicious and recognizable. Once a piece of data has been verified and recorded in the blockchain, it cannot be changed or removed from the network.

2.2 Registration Phase

All cars must be registered during the registration phase. Only registered vehicles are permitted to operate across the whole network. For authorised cars, registration serves as identity. All required personal information, including the users' name, address, phone number, and email address, must be provided by users of the vehicle. The TA selects a random number UniID$_i \in K^{*}_{Rand}$ and also compute public key based on it PubK=n1$^{\text{UniIDi}}$ after the private information is correctly provided

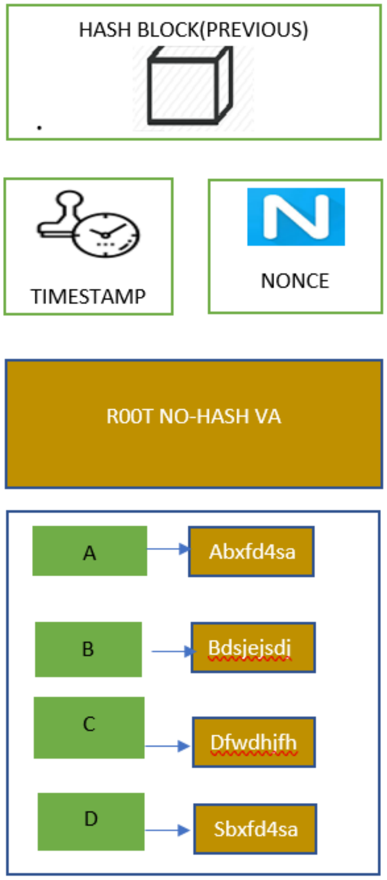

Fig 2. Block header format

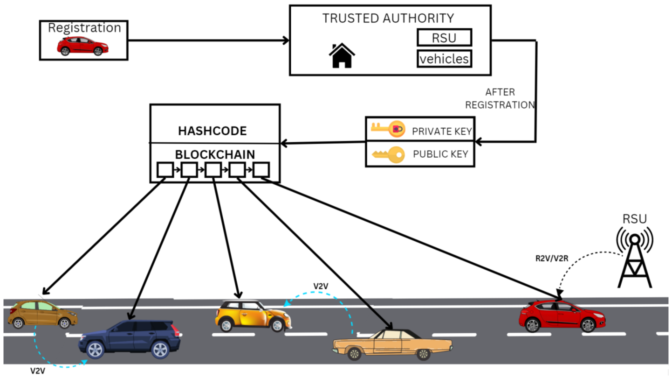

Fig 3. Proposed Methodology

and approved by the TA, it will compute a new hash value and update it in database to track vehicles if required. Each vehicle needs vehicle identification (VehI$_{de}$) and a number that will be chosen at random by the Trusted Authority (T$_{ARN}$) in order to produce a private/unique key.

$$U_{ID} = Hh(VehI_{den} + T_{ARN}) \tag{1}$$

2.3 Authentication Phase

In this setup, every vehicle in the VANET is assigned a distinct digital identity that is stored within a block chain. This identity undergoes encryption using a private key, and the corresponding public key is retained within the block chain. When a vehicle intends to communicate with another, it shares this digital identity. The transaction occurring between these vehicles is logged in a block, which is then verified and appended to the block chain, guaranteeing the security and immutability of the transaction. To make data storage and transfer secure, regardless of the original data's length, hashing is utilized to convert data into a fixed-size hash. Hashing also enables efficient searching and comparison within extensive datasets, as it can quickly match the hash of desired data to its counterpart in the dataset. Despite its simplicity, requiring no advanced technical expertise, it's important to acknowledge that present hashing techniques have their own limitations and drawbacks.

One major drawback is that the hash functions used in modern hashing algorithms are deterministic, meaning that given the same input, they will always produce the same output. This means that attackers can use precomputed hash tables to quickly reverse engineer hashed passwords, making it easier to break into systems. Additionally, current hash functions are vulnerable to brute force attacks, in which an attacker attempts to guess the input data that produced a given hash. To address these limitations and improve the security of hashed data, custom hashing techniques are often used. Custom hashing techniques can be designed to provide better security and more efficient processing than standard hashing algorithms. They can also incorporate additional security features such as Salting and Key-based hashing algorithm (SKBH).

```
Algorithm
Define the private and public keys :
private_key = generate_private_key()
public_key = generate_public_key()
Convert a given string into a hash using the keys:
function custom_hash(string):
Split the string into individual characters
characters = split(string)
Generate a random number using the private key
random_number = generate_random_number(private_key)
```

2.4 Verification Phase

The verification phase can also involve checking the validity of the certificate associated with the digital identity. This can be done by verifying the digital signature on the certificate using the public key stored in the blockchain. The use of the verification phase ensures that only authorized vehicles are allowed to communicate in the VANET, preventing any malicious attacks on the network. The verification phase is a crucial step in the authentication scheme in VANETs. It involves verifying the authenticity of the digital identity and the associated certificate, ensuring that only authorized vehicles are allowed to communicate in the network.

```
Multiply each character's ASCII value by the random number
values = []
for each character in characters:
    value = ASCII(character) * random_number
    values.append(value)
Concatenate the resulting values and take the modulus of the product with a large prime number
product = concatenate(values)
modulus = product % large_prime
Add the public key to the result to obtain the final hash
hash = modulus + public_key
return hash
```

2.5 Clustering and Cluster Head (CH) selection

The first step in clustering is to define the criteria for grouping the vehicles into clusters. This can be based on factors such as proximity, speed, direction, or communication requirements. Once the criteria are defined, vehicles within a certain range of each other are grouped into a cluster, with a CH selected for each cluster. The CH is responsible for managing communication within the cluster, including data aggregation, routing, and forwarding. The selection of the CH can be done based on various criteria, such as communication range, connectivity, network traffic, battery level, or reliability. The CH is responsible for coordinating communication within the cluster and forwarding data to other clusters or the internet. The CH can also perform data aggregation, where data from multiple vehicles is combined into a single message to reduce the amount of traffic in the network. Following the selection of cluster heads, the distance between cluster centroids and nodes (vehicles) is calculated using the Euclidean distance formula.

$$Dist_i = \sqrt{\sum_{i=1}^{n} \left((CP)_i - (AV)_n\right)^2} \tag{2}$$

Based on the equation mentioned above, the similarity between all nodes present in the network architecture and the selected centroid values is calculated. If a node is selected, it is left as it is, but if not, the distance calculation is continued. This involves scanning the list of unselected points to find the ungrouped node that has the maximum distance from the selected points. Then, a point is removed from the unselected points list and added to the end of the selected points sequence. Once the clusters are created, the Cluster Head (CH) is selected based on several factors such as the location, speed, velocity, and equipment of the vehicles. This selection is done using the Equation (3) mentioned below.

$$Fact = \sum \left(L_{veh}, S_{veh}, V_{veh}, E_{veh}\right) \tag{3}$$

The cluster node selects the node that meets the threshold value specified by Equation (3) as the Cluster Head (CH). Clustering and CH selection can help improve network scalability, reduce network congestion, and improve overall network performance in VANETs.

2.6 Secure Data Communication

Secure data communication in VANET involves the use of various techniques and protocols to ensure the confidentiality, integrity, and availability of data transmitted between vehicles or between vehicles and roadside infrastructure. Ensuring secure data communication in VANET is critical to maintaining the safety and reliability of the network. Secure data Communication using SKBH algorithm is based on ASCII characters and is a public key encryption method that can generate faster, smaller, and more efficient cryptographic keys. However, in a standard ECC algorithm, the private key is chosen randomly, which may not provide sufficient security. To address this issue, in this proposed method, the private key is selected by multiplying a random number with the ASCII value of the OBU password. This approach enhances the security of the private key.

2.7 Security Analysis

In this subsection, the attacks, which are mitigated in the proposed model, are given below.

- **DoS attacks** can interfere with communication in VANETs by inundating the network with excessive traffic or excessively taxing the resources of the vehicles. Employing blockchain technology can prevent DoS attacks by implementing a consensus mechanism capable of recognizing and barring malicious nodes from engaging in the network.
- **Sybil attacks** occur when multiple fake identities are generated to manipulate the network. The use of blockchain technology can avert Sybil attacks by offering a tamper-proof record-keeping mechanism that can expose and block the generation of counterfeit identities.
- **Repaly attack** to prevent replay attacks in VANETs that use blockchain technology, various methods such as digital signatures, timestamps, and consensus mechanisms can be employed. These techniques can confirm the distinctiveness and legitimacy of every message, ensuring the VANET's dependability and security. This, in turn, can lower the chances of malicious attacks, strengthening the trust shared among the nodes in the network.

3 Result and Discussion

The efficacy of the suggested methods is confirmed through experimental evaluation when compared to the current approaches.

3.1 Performance Analysis

Performance of the proposed model is analyzed for the following. VANETs utilize multiple hashing techniques, among which are cryptographic hash functions like SHA-1, SHA-256, and MD5 in Figure 4. These hash functions are created to resist different attacks such as pre-image attacks and collision attacks. Measuring different metrics such as throughput, delay, packet loss, and network lifetime is essential to assess network performance.

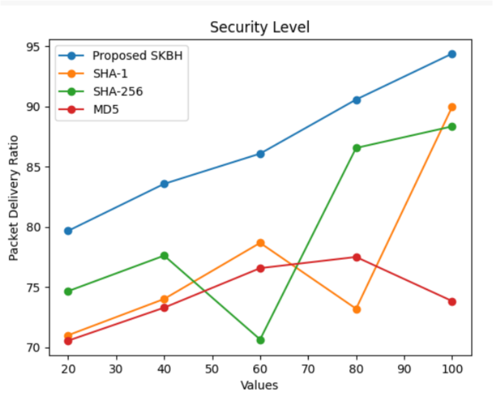

Fig 4. Security

In a controlled simulation, a virtual vanet system was set up where all 4 algorithms were assigned with same amount of packets that is transferred. The data received from this experimental simulation is plotted as a graph from which we can easily infer that the proposed SKBH has the highest packet delivery ratio compared to all 3 other algorithms used in this simulation. Throughput is a fundamental metric in VANET performance analysis, which refers to the volume of data that can be transmitted through the network during a specific time period. This metric is influenced by factors such as packet size, network congestion, and channel bandwidth. Figure 4 shows the Security level graph comparing the proposed method with existing methods. The SHA-1 method Computation cost of 5.625, while the other methods 6.465,20.974,14.54. During Data Communication, it is important to have a security and this is achievable with the proposed method. The proposed method is more effective in achieving secured DC with less collision and higher security level.

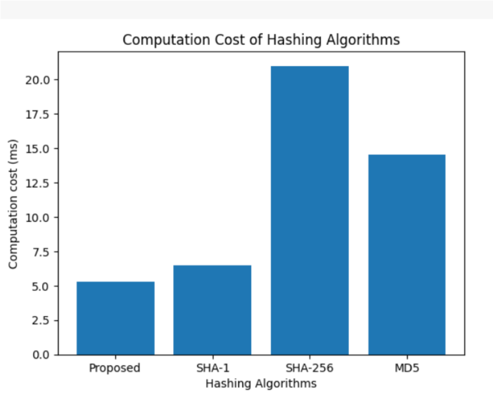

Fig 5. Computation cost

Computation cost of various algorithms shows in Figure 5. The above graph analysis is bench marked on this system with following specs: intel i5 11th gen, 8gb ram, gtx 1660 GPU. Delay is another vital metric in VANET performance analysis, which measures the time taken for a packet to travel from the source to the destination. Secure data communication can help in avoiding transmission delays. Packet loss is a metric that counts the number of packets lost or dropped during transmission, which can be caused by various factors such as signal interference, network congestion, and more. High packet loss can lead to increased network overhead and decreased QoS. Overall, SHAH algorithm for improvement to enhance its performance and efficiency. The experiments are carried in a simulated environment. The Proposed SKBH algorithm is developed and ran locally on the machine for testing and evaluation. All analysis and comparisons are made locally on simulated environment to make detailed analysis and capability of the system.

3.2 Drawbacks

These VANET networks enable vehicles to communicate with each other and with roadside infrastructure in real-time, sharing crucial information about traffic conditions, accidents, and even driver behavior. While the potential benefits are vast VANET come with their set of drawbacks and challenges. In this era of increasing digital connectivity, Connectivity remains a concern, as the effective operation of VANET relies heavily on uninterrupted and efficient data exchange, which can be hampered by network congestion, interference, or inadequate coverage in remote areas. Scalability is a concern as well, as these networks need to accommodate an ever-growing number of vehicles. Another major drawback would be the cost, Deploying VANET infrastructure, such as roadside units (RSU) and onboard units (OBU), can be costly. The deployment and maintenance of these devices require a significant investment, which might not be feasible in some regions. It is important to explore and understand these limitations to develop effective solutions that can harness the full potential of VANET systems while mitigating their shortcomings.

4 Conclusions

The critical role played by the SHAH Algorithm in this scheme underscores its importance in establishing strong security measures. The findings highlight the value of this unique approach, serving as a catalyst for further exploration at the intersection of block chain and VANET technologies. This progress ultimately paves the way for a more secure future in vehicular communication. This research stands as a crucial step forward in enhancing the overall reliability and trustworthiness of VANETs, contributing to the evolution of secure data exchange in our interconnected world.

References

1) Maria A, Pandi V, Lazarus JD, Karuppiah M, Christo MS. BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs. *Security and Communication Networks*. 2021;2021:1–11. Available from: https://doi.org/10.1155/2021/6679882.
2) Jia X, Hu N, Yin S, Zhao Y, Zhang C, Cheng X. A2 Chain: A Blockchain-Based Decentralized Authentication Scheme for 5G-Enabled IoT. *Mobile Information Systems*. 2020;2020:1–19. Available from: https://doi.org/10.1155/2020/8889192.
3) Ahmed W, Di W, Mukathe D. Privacy-preserving blockchain-based authentication and trust management in VANETs. *IET Networks*. 2022;11(3-4):89–111. Available from: https://doi.org/10.1049/ntw2.12036.
4) Khedkar S, Mahajan R. Optimized and Efficient Authentication in VANET using Blockchain. *Management Journal for Advanced Research*. 2022;2(4):35–41. Available from: https://dx.doi.org/10.2139/ssrn.4203801.
5) Dwivedi SK, Amin R, Vollala S, Khan MK. B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs. *IEEE Transactions on Network Science and Engineering*. 2023;10(6):3491–3504. Available from: https://ieeexplore.ieee.org/document/10107443.
6) Patil AN, and SVM. Integrated Blockchain Manufacturing Design for Distributed Authentication, Validation and Secure Sharing of Events in VANETe-commerce. *Journal of Machine and Computing*. 2023;03(01):017–026. Available from: https://doi.org/10.53759/7669/jmc202303003.
7) Yavari M, Safkhani M, Kumari S, Kumar S, Chen CM. An Improved Blockchain-Based Authentication Protocol for IoT Network Management. *Security and Communication Networks*. 2020;2020:1–16. Available from: https://doi.org/10.1155/2020/8836214.
8) Feng X, Cui K, Jiang H, Li Z. EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network. *Symmetry*. 2022;14(6):1–22. Available from: https://doi.org/10.3390/sym14061230.
9) Maria A, Pandi V, Lazarus JD, Karuppiah M, Christo MS. BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs. *Security and Communication Networks*. 2021;2021:1–11. Available from: https://doi.org/10.1155/2021/6679882.
10) Chukwuocha C, Thulasiraman P, Thulasiram RK. Trust and scalable blockchain-based message exchanging scheme on VANET. *Peer-to-Peer Networking and Applications*. 2021;14:3092–3109. Available from: https://doi.org/10.1007/s12083-021-01164-9.
11) Jiang Y, Shen X, Zheng S. An Effective Data Sharing Scheme Based on Blockchain in Vehicular Social Networks. *Electronics*. 2021;10(2):1–17. Available from: https://doi.org/10.3390/electronics10020114.
12) Lu Z, Wang Q, Qu G, Zhang H, Liu Z. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* . 2019;27(12):2792–2801. Available from: https://ieeexplore.ieee.org/document/8784413.
13) Ouaissa M, Ouaissa M, Houmer M. Secure Hierarchical Infrastructure-Based Privacy Preservation Authentication Scheme in Vehicular Ad Hoc Networks. In: Opportunistic Networks. CRC Press. 2021. Available from: https://doi.org/10.1201/9781003132585-4.
14) Zheng D, Jing C, Guo R, Gao S, Wang L. A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs. *IEEE Access*. 2019;7:117716–117726. Available from: https://ieeexplore.ieee.org/document/8808923.
15) Nandy T, Idris MYI, Noor RM, Das AK, Li X, Ghani NA, et al. An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network. *Computer Communications*. 2021;177:57–76. Available from: https://doi.org/10.1016/j.comcom.2021.06.013.
16) Cui J, Ouyang F, Ying Z, Wei L, Zhong H. Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain. *IEEE Transactions on Intelligent Transportation Systems*. 2022;23(7):8857–8867. Available from: https://ieeexplore.ieee.org/document/9457110.
17) Yang J, Deng J, Xiang T, Tang B. A Chebyshev Polynomial-Based Conditional Privacy-Preserving Authentication and Group-Key Agreement Scheme for VANET. *Nonlinear Dynamics*. 2021;106:2655–2666. Available from: https://doi.org/10.21203/rs.3.rs-550221/v1.

18) Saravanan M, Kumar SM. Improved authentication in vanets using a connected dominating set-based privacy preservation protocol. *The Journal of Supercomputing*. 2021;77(12):14630–14651. Available from: https://doi.org/10.1007/s11227-021-03911-4.

19) Li T, Liu W, Liu A, Dong M, Ota K, Xiong NN, et al. BTS: A Blockchain-Based Trust System to Deter Malicious Data Reporting in Intelligent Internet of Things. *IEEE Internet of Things Journal*. 2022;9(22):22327–22342. Available from: https://ieeexplore.ieee.org/document/9444338.

20) Zheng D, Jing C, Guo R, Gao S, Wang L. A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs. *IEEE Access*. 2019;7:117716–117726. Available from: https://ieeexplore.ieee.org/document/8808923.

21) Sajini S, Anita EAM, Janet J. Improved Security of the Data Communication in VANET Environment Using ASCII-ECC Algorithm. *Wireless Personal Communications*. 2023;128(2):759–776. Available from: https://doi.org/10.1007/s11277-022-09974-7.