Designing a Secure Vehicular Internet of Things (IoT) Using Blockchain

Atul Lal Shrivastava and Rajendra Kumar Dwivedi

Abstract Smart vehicles are interconnected and deliver a variety of sophisticated services to their owners, transit authorities, automobile manufacturers, and other service providers. Smart cars could be exposed to a number of security and privacy risks, including GPS tracking and remote vehicle hijacking. Blockchain is a game-changing technology that can be used for everything from cryptocurrencies to smart contracts. It may be a viable solution for implementing security in vehicular IoTs. We present a blockchain-based methodology to preserve users' privacy while simultaneously boosting vehicle security in this paper. The proposed model upgrades the services of vehicular IoT.

Keywords Blockchain · Vehicular networks · IoT · Cloud computing

1 Introduction

Automobiles and roadside equipment form self-organizing wireless networks called vehicular ad hoc networks (VANETs) (RSUs). The use of real-time dynamic communication between vehicles and RSUs provides for efficient and long-lasting data transmission. As a result of the broad deployment of VANETs, intelligent transportation systems (ITSs) are now feasible [1, 2]. A varied collection of VANET-based applications, which can be classified as safety or commercial, increases not only driving safety but also driving enjoyment. Safety-related applications include emergency vehicle warnings, traffic management reports, road accident notification, and speed monitoring [3, 4]. Commercially focused applications that provide convenience and entertainment include weather forecasting, broadcasting information from neighboring gas stations and restaurants, navigation, and Internet connectivity.

We present a secure certificateless authentication solution for vehicle ad hoc networks in this paper. Centralized and decentralized networks in the IoT are well described in Fig. 1, and blockchain is well described in Fig. 2.

A. L. Shrivastava (✉) · R. K. Dwivedi
Department of Information Technology and Computer Application, MMMUT, Gorakhpur, India
e-mail: atulsha08@gmail.com

V. Suma et al. (eds.), *Inventive Systems and Control*, Lecture Notes in Networks and Systems 436, https://doi.org/10.1007/978-981-19-1012-8_46

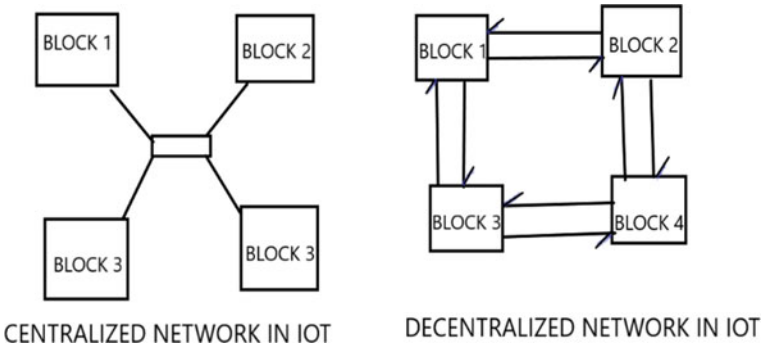

Fig. 1 Centralized and decentralized network in IoT

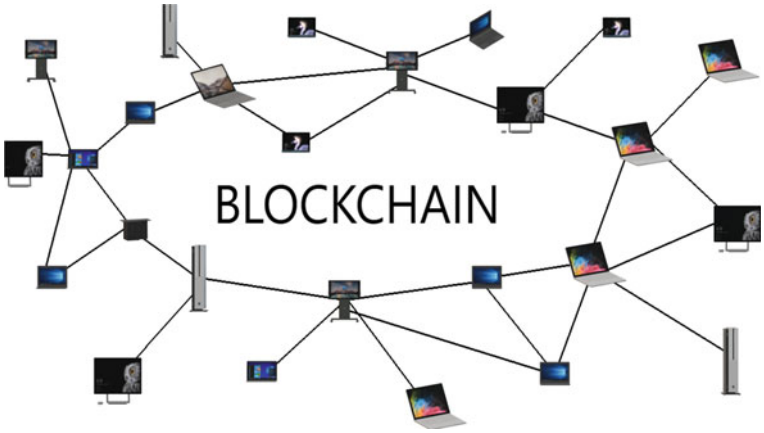

Fig. 2 Blockchain

The following is a breakdown of the paper's structure. The second section is a summary of the survey's findings. The research gap is described in Sect. 3. The model description and preliminaries in vehicle IoT using blockchain are described in Sect. 4. Section 5 outlines a model for bridging the gap, and the tools to be utilized are described in Sect. 6. This paper comes to a close with Sect. 7.

This paper is organized as follows. Section 2 describes literature review. Section 3 describes the research gaps. Section 4 describes the background and preliminaries in vehicular IoT using blockchain. Section 5 describes system model. Section 6 describes methodology to fill the gap. Section 8 concludes this paper and describes future directions.

2 Literature Review

Security in vehicular Internet of Things (IoT) using blockchain for VANETs has received a lot of attention in recent years. User privacy should be protected, and keys should be updated. For location-based services,

Lu et al. [5] presented a dynamic key management approach (LBSs). The LBS is a non-profit organization dedicated in helping. Each session is broken down into a number of time slots, each with its own set of activities. Following that a vehicular data authentication mechanism [6] is given, including probabilistic verification. For malicious behavior detection, an approach is used. In addition, in order to avoid delays in computing, checking the certificate revocation list (CRL), and group signatures. The authentication code is a hashed message authentication code (HMAC).

Chuang and Lee et al. [7] developed a decentralized authentication security system (TEAM) for V2V communication. It is essential to notice that the findings are improved by using the transitive trust relationship frame. Smart cars could be exposed to a number of security and privacy risks, including GPS tracking and remote vehicle hijacking.

Shen et al. [8, 9] proposed schemes have been created that emphasize privacy preservation and lightweight. VANET verification. public-key cryptography that is based on identity, in particular. For safe certificates, (ID-PKC) [10] has been frequently used. Obtaining proof of efficiency, several authentication methods have recently been introduced.

Zhang et al. [11] proposed VANET management is a term used to describe the process of putting together a virtual Zhang et al. [11] provided an initial hypothesis. Smart vehicles are interconnected and deliver a variety of sophisticated services to their owners, transit authorities, automobile manufacturers, and other service providers. Smart cars could be exposed to a number of security and privacy risks, including GPS tracking and remote vehicle hijacking.

Jung et al. [12] devised a universal re-encryption strategy based on identity. For V2R communications, the batch signature verification scheme. This technique, however, is susceptible to replication [13]. Formal paraphrase An attack Meanwhile, the VANET authentication framework was created as a result of this. [14] offers a new preservation and repudiation model (ACPN). Self-created PKC-based pseudo IDs were designed with this in mind are put into action.

He et al. [15] then devised a successful strategy. The CPPA technique for VANETs is based on identity. It is worth mentioning that bilinear is a term used to describe. As a result of the lack of pairing processes, the results are fairly small. Calculations are cheap. Two more CPPA plans are similar. For VANETs, [1] and [16] were created.

3 Research Gaps

On the basis of the literature survey, we found following research gaps:

- **Proximity:** Because vehicles are mobile and perhaps fast-moving nodes in a network, they would need to change parent nodes frequently. Connections to adjacent peer nodes will be more reliable than connections to distant parent nodes like a cellular tower. A DSRC protocol satisfies the physical range criteria, as indicated in the preceding section [17, 18].
- **Latency:** In vehicles, low latency is crucial given their potential speed. Latency between any two peers will be reduced if nodes interact with one other (or even via each other) using DSRC [3, 19].
- **Decentralization**: When connections are dispersed across different pathways, network traffic bottlenecks are reduced.
- **Fault tolerance**: A network with more connections between nodes is better able to withstand disturbances. This is one of the main advantages of the peer-to-peer (P2P) approach. Because they are not connected to the grid, vehicle peers will be unaffected by power or wired network disruptions [15, 16].

On basis of the identified research gaps, we are using blockchain to create a secure asymmetric cryptographic system. This is commonly used to secure sensitive data and enables public-key encryption. It is especially beneficial when delivering data across an insecure network like the Internet.

4 Background and Preliminaries

This section describes preliminaries of our work as follows.

4.1 Elliptic Curve Cryptography (ECC)

Let F_p be a finite field of order p and $p > 3$ be a prime number. $4a^3 + 27b^2 + 6 = 0$ must be satisfied by F_p. An elliptic curve E_p (a, b) over a finite field F_p is described by the equation:

$$y^2 = x^3 + ax + b$$

Key Generation: Select a no. 'd' within range 'n'

$$Q = d * P$$

where d = within range (1 to $n - 1$).
Q = public key, d = private key.

Encryption:

The agreement on a common integer (the key) lies at the heart of all encryption. The agreed number is then used to encrypt a message by shifting the characters.
s_1 and s_2 two ciphertext will be generated.

$$s_1 = k * P \tag{1}$$

$$s_2 = M + k * Q \tag{2}$$

Decryption:

The agreement on a common integer (the key) lies at the heart of all encryption. The agreed number is then used to encrypt a message by shifting the characters and then to return to the receiving end to decrypt it. The ECC is a way for securing the agreement of a key.

$$M = s_2 - d * s_1 \tag{3}$$

4.2 Hash Function

If a one-way hash function fits the following criteria, it is deemed secure [20]. (1) Given any length message x, it is simple (x) to compute a message digest with a fixed length output h. (2) Calculating $x = h_1$ given y is tricky (y). (3) Given x, it is computationally impossible to compute $\times 0 = \text{x}$ such that $h(\times 0) = h(x)$.The Chinese remainder theorem (CRT) assume that $k_1, \ldots, k_n$ are positive integer pairs that are approximately prime. The system of congruence [21] exists for any given set of numbers $a_1, \ldots, a_n$. There is only one solution to the modulo $g = Q_n\ i = 1\ k_i, \times a_i$ mod k_{ii} [1–n]. The solution is $C = X_n\ i = 1$ iii mod ki, where $I = g\ ki$ and $I\ I = 1$ mod ki. The speed of the time sequences can vary. The DTW method is frequently used to calculate the distance or similarity between time series automatically.

4.3 Dynamic Time Warping (DTW)

The approach of dynamic time warping (DTW) [22] is effective for obtaining the best alignment between two time-dependent sequences (time series). It is important to keep in mind that the length and collected and forwarded to TA for analysis.

TA also stores the sensitive keys assigned to RSUs and vehicles. TA is believed to have sufficient storage and processing capabilities in this situation. Furthermore, because TA is the only valid verifier for the whole VANET, all participating autos must first be confirmed. The fast growth of cloud computing, in particular, makes it easier to connect traditional VANETs to cloud servers. As a result, vital information and sensitive user data can be stored on various cloud servers. Meanwhile, TA's calculation capabilities could be improved. In recent years, cloud-assisted VANET research has attracted a lot of attention [23, 24].

5 System Model

The three main components of VANETs system are described in this section. The design of the projected VANETs system is seen in Fig. 2.

5.1 Trusted Authority (TA)

The dependable authority is the VANETs system's dependable command and control center (TA). TA is in charge of verification vehicle registration, key management, and other major activities. We believe TA is always truthful and trustworthy. As seen in Fig. 1, TA provides a variety of programs to authorized cars, Internet access, including weather forecasts, navigation and, meanwhile, vehicle data, such as traffic congestion statistics.

5.2 Road-Side Unit (RSU)

The RSU is a one-of-a-kind facility that acts as the only connection between TA and on-the-road vehicles. The RSU's job is to communicate with approaching vehicles via short-range communication technologies (DSRC). In real-world settings, RSUs are stationed in remote places far from TA, with some of them in dangerous environments. As a result, if these RSUs are not regularly maintained, they can easily be compromised or deactivated, resulting in data leakage from the affected vehicles. Malicious attackers may be able to obtain sensitive vehicle data by storing corrupted RSUs. RSUs were designed as semi-trusted entities with limited access to vehicle data to account for this. The TA will harvest and process the vehicle data and other crucial information.

5.3 Vehicles

Vehicles are meant to collect data as well as receive VANET services. Each vehicle has an on-board device (Board unit) that allows it to communicate with road-side units as well as other vehicles. In our system concept, the vehicle plate number is recognized as a unique identifying provided by TA, each of which is clearly linked to a single driver. The driver's fingerprint/certificate card is also utilized for further protection, guaranteeing that the driver and the connected vehicle are linked each time the driver starts his or her vehicle. For the sake of clarity, we regard the driver and the vehicle as a single entity in this research. Security in vehicular IoT using blockchain is shown in Fig. 3.

6 Methodology to Fill the Gap

The capacity of blockchain is to incorporate consensus procedures and peer-to-peer computing. Blockchain has developed a decentralized and safe platform for sharing information. Indeed, digital encryption technologies are integral to blockchain technology, propelling blockchain cryptography to the forefront. Blockchain can use cryptographic technique such as RSA encryption algorithm.

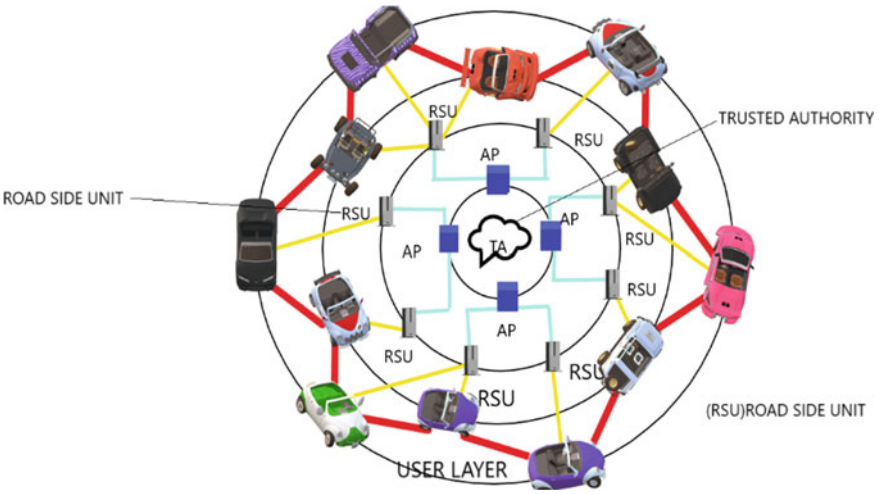

Fig. 3 System model

6.1 Proposed Algorithm

RSA algorithm to produce public and private keys, the RSA algorithm is used the steps of this algorithm are as below:

p and q are two huge prime numbers. Multiply these numbers to produce $x = p \times q$, where x is the modulus of encryption and decryption.

Select an integer e smaller than x such that a is close to $(p-1) \times (q-1)$. It means that, except for 1, e and $(p-1) \times (q-1)$ have no common factor. Select "e" in such a way that $1e\ (x)$, e is prime to (x), and gcd $(e, d\ (x)) = 1$.

If $x = p \times q$, then $e, x>$ is the public key. The public key $e, x>$ is used to encrypt a plaintext message y. The following formula is used to generate ciphertext C from plain text: me mod $n = C$.

y must be less than x in this case. A message of a length more than x is handled as a collection of messages, each of which is encrypted separately.

We use the following formula to compute the d in order to determine the private key:

Demonstrate that $(p-1) \times (q-1) = 1$ or $(p-1) \times (q-1) = 1$.

De mod (x) = 1 de mod (x) = 1 de mod (x) = 1 de mod (x) d , x > is the private key. The private key d , x > is used to decrypt a ciphertext message c . The following formula is used to calculate plain text y from ciphertext c.

mod cd $x = y$.

6.2 Simulation Tool

Ethereum is a completely decentralized blockchain network. Due to the liveliness and responsiveness of its community, as well as the abundance of its documentation, the blockchain promises that goods will become completely autonomous and belong to themselves. They will be able to utilize code: In exchange for money (a type of code), the door will release its access (through code) for the duration of the specified time.

Ethereum is a blockchain network that is decentralized. The blockchain promises that things will become entirely autonomous and belong to themselves as a result of the community's liveliness and reactivity, as well as the volume of data available. They will be able to use code: In exchange for money (a form of code), the door will grant them access (through code) for a set amount of time.

7 Result

The proposed methodology outlined in the paper totally eliminates the inefficiency, as well as the security and privacy of data created in traditional automotive IoT. The suggested framework does a fantastic job of establishing a fully secure vehicular IoT. When it comes to vehicle data study, the most important consideration is the data's trustworthiness or authenticity. When data are generated and stored using the blockchain framework, we can always be sure that the data are genuine because it was joined to the chain by various stakeholders rather than a single controlling body.

The change from manual to remote monitoring and environment control is always seen as a more guided and successful approach. A tip-to-tip monitoring was not possible in the traditional method, and it may lead to many discrepancies. As a result, a remote network capable of detecting all connected data and alerting vehicles in the event of an irregularity could be considered one of the best alternatives.

8 Conclusion and Future Directions

The possibility of employing blockchain for autonomous vehicle networks was examined in this article, and a blockchain model was proposed. The decentralized approach provides a number of advantages not present in traditional client–server architectures. While not the ideal application for blockchain technology, examining prospective applications is nevertheless beneficial. As more powerful ITS systems are built for real-world application, a disruptive technology like blockchain will almost certainly find its way into multiple components, even if it is not a core function.

The proposed architecture suits a broader range of applications for future research direction such as improvement in proximity, latency, decentralization, and fault tolerance.

References

1. Lo N-W, Tsai J-L (2016) An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans Intell Transp Syst 17(5):1319–1328
2. Horng S-J, Tzeng S-F, Huang P-H, Wang X, Li T, Khan MK (2015) An efficient certificateless aggregate signature with conditional privacy preserving for vehicular sensor networks. Inf Sci 317:48–66
3. Shen J, Zhou T, Liu X, Chang Y-C (2018) A novel latin-square-based secret sharing for M2M communications. IEEE Trans Ind Informat 14(8):3659–3668
4. Liu B, Jia D, Wang J, Lu K, Wu L (2017) Cloud-assisted safety message dissemination in VANET-cellular heterogeneous wireless network. IEEE Syst J 11(1):128–139
5. Lu R, Lin X, Liang X, Shen X (2012) A dynamic privacy-preserving key management scheme for location-based services in VANETs. IEEE Trans Intell Transp Syst 13(1):127–139
6. Molina-Gil J, Caballero-Gil P, Caballero-Gil C (2014) Aggregation and probabilistic verification for data authentication in VANETs. Inf Sci 262:172–189

7. Chuang M-C, Lee J-F (2014) TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE Syst J 8(3):749–758
8. Zhang L, Wu Q, Domingo-Ferrer J, Qin B, Hu C (2017) Distributed aggregate privacy-preserving authentication in VANETs. IEEE Trans Intell Transport Syst 18(3):516–526
9. Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y (2018) Cloudaided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J Netw Comput Appl 106:117–123
10. Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Advances in cryptology. Springer, Berlin, Germany, pp 47–53
11. Zhang C, Lu R, L Xin, Ho P-H, Shen X (2008) An efficient identitybased batch verification scheme for vehicular sensor networks. In: Proceedings of 27th conference on computer communications (INFOCOM), pp 246–250
12. Jung CD, Sur C, Park Y, Rhee K-H (2009) A robust and efficient anonymous authentication protocol in VANETs. J Commun Netw 11(6):607–614
13. Lee C-C, Lai Y-M (2013) Toward a secure batch verification with group testing for VANET. Wireless Netw 19(6):1441–1449
14. Li J, Lu H, Guizani M (2015) ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans Parallel Distrib Syst 26(4):938–948
15. He D, Zeadally S, Xu B, Huang X (2015) An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans Inf Forensics Secur 10(12):2681–2691
16. Sun J, Zhang C, Zhang Y, Fang Y (2010) An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans Parallel Distrib Syst 21(9):1227–1239
17. Gao T, Deng X, Wang Y, Kong X (2018) PAAS: PMIPv6 access authentication scheme based on identity-based signature in VANETs. IEEE Access 6:37480–37492
18. Tan H, Chung I (2018) A secure and efficient group key management protocol with cooperative sensor association in WBANs. Sensors 18(11):3930
19. Jiang Q, Huang X, Zhang N, Zhang K, Ma X, Ma J (2019) Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist worn devices. IEEE Internet Things J 6(3):5618–5630
20. Tan H, Gui Z, Chung I (2018) A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs. IEEE Access 6:74260–74276
21. Dwivedi RK, Kumari N, Kumar R (2020) Integration of wireless sensor networks with cloud towards efficient management in IoT: a review. In: Part of the lecture notes in networks and systems book series (LNNS), vol 94, Springer Singapore, pp 97–107
22. Haoxiang W, Smys S (2019) QoS enhanced routing protocols for vehicular network using soft computing technique. J Soft Comput Paradigm (JSCP) 1(02):91–102
23. Zhu X, Jiang S, Wang L, Li H (2014) Efficient privacy-preserving authentication for vehicular ad hoc networks. IEEE Trans Veh Technol 63(2):907–919
24. Khattak HA, Islam SU, Din IU, Guizani M (2019) Integrating fog computing with VANETs: a consumer perspective. IEEE Commun Stand Mag 3(1):19–25
25. Tan H, Choi D, Kim P, Pan S, Chung I (2018) An efficient hash-based RFID grouping authentication protocol providing missing tags detection. J Internet Technol 19(2):481–488
26. Khan AA, Abolhasan M, Ni W (2018) '5G next generation VANETs using SDN and fog computing framework. In: Proceedings of 15th IEEE annual consumer communications & networking conference (CCNC), pp 1–6
27. Ullah A, Yaqoob S, Imran M, Ning H (2019) Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing. IEEE Access 7:1570–1585
28. Song J, He C, Zhang L, Tang S, Zhang H (2014) Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs. China Commun 11(9):93–103
29. Tan H, Choi D, Kim P, Pan S, Chung I (2018) Secure certificateless authentication and road message dissemination protocol in VANETs. Wireless Commun Mobile Comput 2018:1–13

30. Gayathri N, Thumbur G, Reddy PV, Ur Rahman MZ (2018) 'Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks. IEEE Access 6:31808–31819
31. Zheng D, Jing C, Guo R, Gao S, Wang L (2019) A traceable blockchain based access authentication system with privacy preservation in VANETs. IEEE Access 7:117716–117726
32. Madhusudhan R, Hegde M, Memon I (2018) A secure and enhanced elliptic curve cryptography-based dynamic authentication scheme using smart card. Int J Commun Syst 31(11):e3701
33. Tan H, Chung I (2019) Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. IEEE Access 7:151459–151474
34. Malip A, Ng S-L, Li Q (2014) A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks. Secur Commun Netw 7(3):588–601
35. Jiang Q, Ma J, Yang C, Ma X, Shen J, Chaudhry SA (2017) Efficient end-to-end authentication protocol for wearable health monitoring systems. Comput Electr Eng 63:182–195
36. Tan H, Choi D, Kim P, Pan S, Chung I (2018) Comments on 'dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks.' IEEE Trans Intell Transp Syst 19(7):2149–2151
37. Ming Y, Shen X (2018) PCPA: a practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks. Sensors 18(5):1573
38. Jiang S, Zhu X, Wang L (2016) An efficient anonymous batch authentication scheme based on HMAC for VANETs. IEEE Trans Intell Transport Syst 17(8):2193–2204
39. Luo G, Yuan Q, Zhou H, Cheng N, Liu Z, Yang F, Shen XS (2018) Cooperative vehicular content distribution in edge computing assisted 5G-VANET. China Commun 15(7):1–17
40. Xie L, Ding Y, Yang H, Wang X (2019) Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access 7:56656–56666
41. Zhang X, Wang D (2019) Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain. IEEE Access 7:97281–97295
42. Butt TA, Iqbal R, Salah K, Aloqaily M, Jararweh Y (2019) Privacy management in social Internet of vehicles: review, challenges and blockchain based solutions. IEEE Access 7:79694–79713
43. Tan H, Song Y, Xuan S, Pan S, Chung I (2019) Secure D2D group authentication employing smartphone sensor behavior analysis. Symmetry 11(8):969
44. Lu Z, Liu W, Wang Q, Qu G, Liu Z (2018) A privacy-preserving trust model based on blockchain for VANETs. IEEE Access 6:45655–45664
45. Al-Riyami SS, Paterson KG (2003) 'Certificateless public key cryptography. In: Advances in cryptology. Springer, Berlin, Germany, pp 452–473
46. Dhaya R, Kanthavel R (2021) Bus-based VANET using ACO multipath routing algorithm. J Trends Comput Sci Smart Technol (TCSST) 3(01):40–48