Privacy Preserving Blockchain Enabled Metaheuristic Clustering Protocol for Vehicular Adhoc Networks

M. V. B. Murali Krishna M.[1] Dr. C. Anbu Ananth [2] Dr. N. Krishnaraj[3]

[1]Research Scholar, Department of CSE, FEAT, Annamalai University, Chidambaram-608002, Tamil Nadu, India. Email:muralimk786@gmail.com

[2]Associate Professor, Department of CSE, FEAT, Annamalai University, Chidambaram-608002, Tamil Nadu, India. Email:anbu_ananth2006@yahoo.com

[3]Associate Professor, School of Computing, SRM Institute of Science and Technology, Kattankulathur- 603203, Tamil Nadu, India.
Email: drnkrishnaraj@gmail.com

Article Info
Page Number: 977 – 991
Publication Issue:
Vol. 71 No. 3 (2022)

Abstract

Vehicular adhoc networks (VANET) are commonly employed for prompt and efficient communication among vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) to enhance the road safety and efficacy of traffic flow. Owing to the mobile nature of the vehicles and wireless links, the VANET is susceptible to malicious nodes which can get access as to network and perform medium access control (MAC) layer threat. Therefore, it is needed to design effective security based solutions with clustering process for energy efficient and secure VANET. In this aspect, this paper presents a novel chicken swarm optimization based clustering with blockchain technology (CSOC-BT) for privacy preserving VANET. The goal of the CSOC-BT technique is to cluster the vehicles using the CSO algorithm and choose cluster heads (CHs) proficiently in such a way that the load gets balanced throughout the network. The CSOC-BT technique derives a fitness function involving multiple input parameters to select CHs and organize clusters. In addition, blockchain technology is applied to perform secure inter-cluster and intra-cluster communication in the network. To ensure the improved security and energy efficient performance of the CSOC-BT technique, a wide range of simulations take place under the existence of attacks. The experimental results demonstrated the enhanced performance of the CSOC-BT technique over the recent state of art approaches interms of different measures.

Keywords: Blockchain, Energy Efficiency, Clustering, VANET, Metaheuristics, Fitness function

Article History
Article Received: *12 January 2022*
Revised: *25 February 2022*
Accepted: *20 April 2022*
Publication: *09 June 2022*

1. Introduction

Vehicle Adhoc networks (VANET) appeared as subsection of a mobile adhoc network (MANET) application. VANET hasregardedas considerable method to intelligent transportation systems (ITS) [1]. The goal of VANET is for offering inter-vehicle transmission and roadside unit for vehicle transmission for improving local traffic flow and increasing road safety and the efficacy of road trafficswith offered timely and accurate data to road users [2]. There are 2 kinds of transmission in VANET, that is vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) transmissions [3]. The road side unit (RSU) and on-board units (OBU) in VANET found connections between them via dedicated short-range communication (DSRC) in multi-hop/single transmissions. VANET offers several applications and services to the user, mostly they are focused on navigational aid, safety of the drivers, and infotainment. There are 2 kinds of data distributed in VANET: non-safety data (value-added comfort application) and safety (curve warning, vehicle speed warning)[4]. Regardless of the benefit offered by VANET, it comes with problem, particularly depending on the transferred messages and privacy and security of users.

Various protocols are presented for ensuring better performance and management of VANET system. Amongst other cluster based systems is performing better when compared to other systems [5]. In a standard cluster based (CB) method, vehicles from neighbouring regions could create a cluster formation, and one of the vehicles is chosen as Cluster Head (CH) for handling external and internal communications. Standard CB system suffers from traffic hidden node, overloading, and packet dropping problems [6]. But, removing /minimizing the limitations, it is can improve their efficacy. With the increase of Intelligent Transport System (ITS), the application and importance of related methods, such as VANET, are also growing. Several authors have been established, that are targeted for improving the efficiency of the VANET [7]. Since vehicles are moving at higher speeds, it is very difficult for maintaining high throughput, low PDR, better transmission speed, and so on. But, guaranteeing privacy and security of the vehicles are less significant problems.

Although, VANET has to confront identification, authentication, availability, confidentiality, and integrity based attacks and threads [8]. Vehicle authentication is the primary security feature that a VANET should guarantee. Despite low configured computation support in real time and high mobility, authentication is needed for maintaining VANET. As a result of dynamic topology and decentralized structure of VANET, the privacy of the data, vehicles, and users has become very important, as the detection of faulty node/user/malicious wasdeveloped challenging [9]. In VANET, vehicle exchanges sensitive data and traffic alters with one another. But, an absence of authentication of this data might lead to malicious attacks that harm drivers[10].

Malik et al. [11] present an advanced trust management method in VANET with 2 main stages: node trustability prediction and secured message transmission. The privacy guaranteed the message passing is performed by integrating the privacy preservation method under the data sanitization procedure. The key employed to the sanitization procedure is tuned optimally by a novel hybrid model called Sea Lion Explored-Whale Optimization Algorithm, i.e., the integration of WOA and SLOA model, correspondingly. The blockchain technique is aided to manage the key produced by the node.

Akhter et al. [12] present a multilevel blockchain based privacy-preserving authentication method. This study comprehensively describes the development of the key generation processes, authentication centres, and vehicles registration. In the presented framework, a global authentication center (GAC) is accountable to store each vehicle data, whereas Local Authentication Center (LAC) preserves a blockchain for enabling fast handover among internal clusters of vehicles. To offer a secure vehicle transmission amongst vehicles, Kchaou et al. [13] proposed a distributive trust management system for VANET to authenticate the accuracy of the message according to the credibility of message by a CH and controlling of vehicle behaviours by a miner.

In Kadadha and Otrok [14], the present Stackelberg game concept incorporates off-chain QoS-OLSR protocols and developed on-chain smart contract that contains Relay Selection Game Manager (RSGM) for selecting relays and Node Reputation Manager (NRM). The presented architecture contains 1) the on-chain leader profit maximization, 2) the role identification, and 3) the off-chain follower incentive selection. Initially, node identifies their role in the game concept; follower/leader. Next, permits followers (node) to compute incentives for leader (relays) on the basis of off-chain exchanged QoS-OLSR messages including reputation and QoS.

Joshi et al. [15] present an effective privacy-preserving data communication which utilizes blockchain technique from cluster based VANET. The clusterbased VANET was utilized for achieving load balancing and minimalizing overhead from the network, whereas the cluster method can be implemented by the ROA model. Ahmedet al. [16], proposed a blockchain-based method, in which one of the blockchain stores the authentication data of the vehicle, and other one distribute and store blockchain services. Research study exposed that the presented blockchain-based protocol is better than the present ones.

This paper presents a novel chicken swarm optimization based clustering with blockchain technology (CSOC-BT) for privacy preserving VANET. The goal of the CSOC-BT technique is to cluster the vehicles using the CSO algorithm and choose cluster heads (CHs) proficiently in such a way that the load gets balanced throughout the network. The CSOC-BT technique derives a fitness function involving multiple input parameters to select CHs and organize clusters. Furthermore, blockchain technology is utilized for secure inter-cluster and intra-cluster communication in the network. For examining the enhanced performance of the CSOC-BT technique, a series of experiments were carried out under the existence of attacks. In short, the paper contribution is summarized as follows.

- Develop a novel CSOC-BT technique for privacy preserving data transmission in clustered VANET.
- Derive a new CSO algorithm to choose CHs from the available vehicles and construct clusters using a fitness function involving distinct input paramters.
- Employ blockchain technology to accomplish secure inter-cluster and intra-cluster communication in VANET.
- The proposed CSOC-BT technique has the ability to attain privacy preserving communication in the clustered VANET.
- Validate the performance of the CSOC-BT technique against recent state of art approaches under varying number of vehicles/ nodes.

The rest of the paper is organized as follows. Section 2 elaborates the working process of the CSOC-BT technique. Section 3 offers the performance validation and section 4 concludes the study.

2. The Proposed Model

In this study, a novel CSOC-BT technique is derived to accomplish privacy preserving communication in clustered VANET. The CSOC-BT technique derives a fitness function involving multiple input parameters to select CHs and organize clusters. Furthermore, blockchain technology is utilized for secure inter-cluster and intra-cluster communication in the network. Fig. 1 illustrates the architecture of proposed system.

.

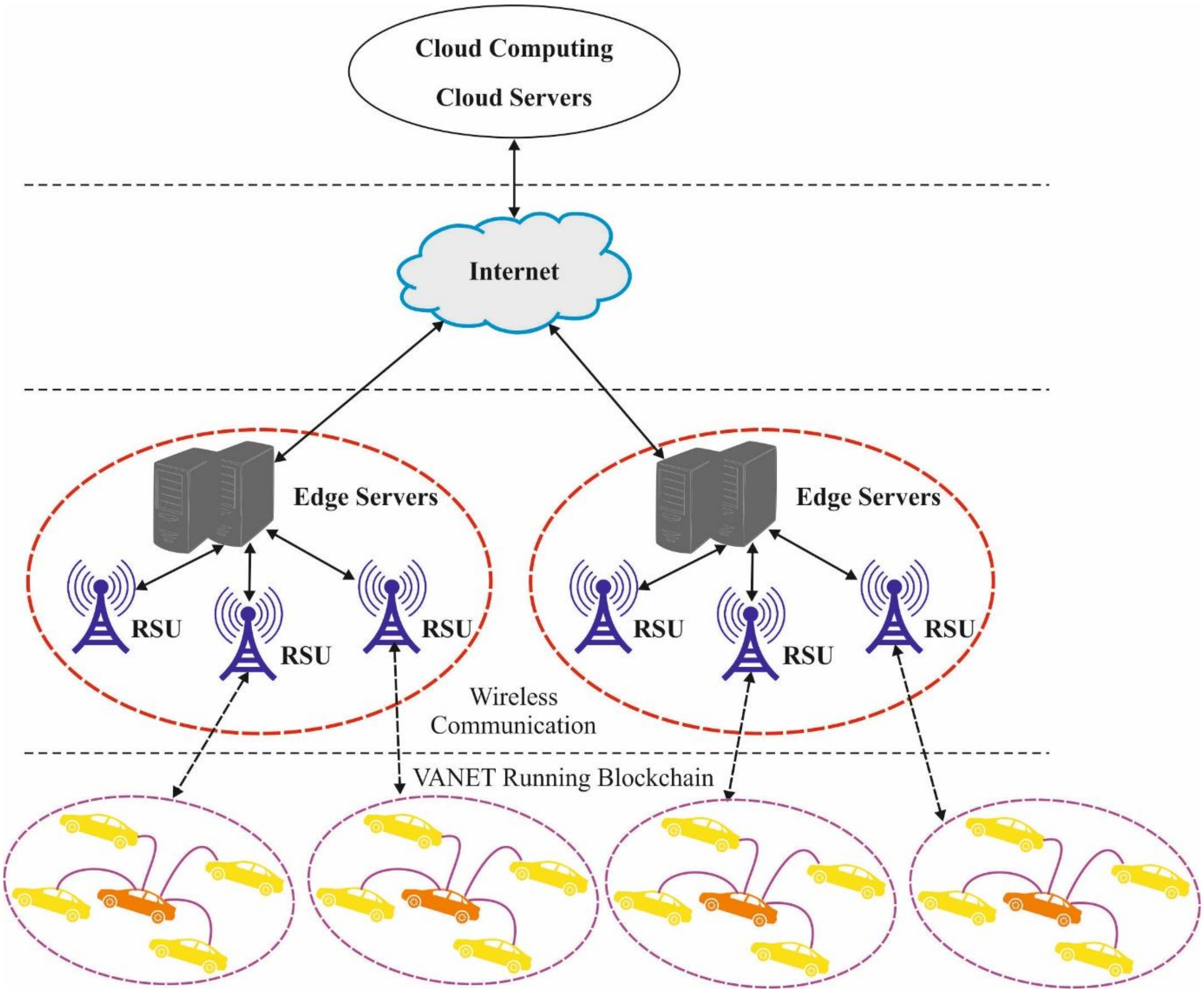

Fig. 1. Proposed System Architecture

2.1. Process involved in CSO based Clustering Technique

At this stage, the CSO-C technique gets executed to pick the CHs and organize clusters. In the fundamental CSO technique, there are 3 types of roles, chick, hen, and rooster, all containing distinct performance conditions. As follows, it provides fundamental conditions to the CSO technique:

(1) The CSO technique separates a chicken swarm into some groups, all that is one rooster, many hens, and small amount of chicks.

(2) The identity of rooster, hen, and chick are defined as its fitness value, the optimum ones are chosen as roosters, the least ones are chicks, and another individual is hen. All the hens arbitrarily elect one rooster as her mating and develop the member of this group, and all the chicks also arbitrarily choose one hen as their mother.

(3) During the entire population, the individual identity, the spouse connections, and mother-children connections continue unaffected to G generation (G implies the iterative cycle), and identity, spouse connection, and mother-children connection are upgraded then G generation.

(4) During all sets of entire populations, the hen follows its spouse rooster for finding food, and it is arbitrarily competing to food with another individual in the group. The individual with optimum fitness values is highly possible for obtaining food.

All the chicken was explained by their place. Assume that CN, MN, RN, and HN implies the amount of chick, mother hen, rooster, and hen correspondingly, and $x_{i,j}^{t}$ refers the place of i^{th} chicken from the j^{th} dimension space on t^{th} iteration, in which $\in \{1,\dots,N\}, j \in \{1,\dots,D\}$, and $t \in \{1,\dots,T\}$ and N, D, and T imply the entire amount of chickens, the dimensional number, and the maximal iteration times correspondingly [17]. The rooster, hen, and chick are its particular place upgrade equations. Fig. 2 depicts the flowchart of CSO technique.

In order to rooster, their recurrent place was determined as:

$$x_{i,j}^{t+1} = x_{i,j}^{t} * \left(1 + Randn(0, \sigma^2)\right) \tag{1}$$

$$\sigma^2 = \begin{cases} 1, if\ f_i \le f_k, \\ \exp\left(\frac{f_k - f_i}{|f_i| + \varepsilon}\right), otherwise\ k \in [1, RN], k \ne i. \end{cases} \tag{2}$$

At this point, $Randn\ (0, \sigma^2)$ signifies the arbitrary number subsequent Gaussian distribution with expectation of zero and variance of σ^2, ε refers the very low constant, k demonstrated the amount of other roosters that are elected arbitrarily, and f_i and f_k stands for the fitness values of i^{th} and k^{th} roosters correspondingly. The recurrent place of hen was determined as:

$$x_{i,j}^{t+1} = x_{i,j}^{t} + C_1 * Rand\ * \left(x_{r_1,j}^{t} - x_{i,j}^{t}\right) + C_2 * Rand\ * \left(x_{r_2,j}^{t} - x_{i,j}^{t}\right), \tag{3}$$

$$C_1 = \exp\left(\frac{\left(f_i - f_{r_1}\right)}{\left(abs(f_i) + \varepsilon\right)}\right), \tag{4}$$

$$C_2 = \exp\left(f_{r_2} - f_i\right). \tag{5}$$

At this point, C_1 and C_2 signifies the learning factor, $Rand$ stands for the arbitrary number subsequent uniform distribution from the scope of zero and one, r_1 refers the index of rooster which is spouse of i^{th} hen, r_2 denotes the amount of rooster or hen that was chosen arbitrarily, and $r_1 \ne r_2$.

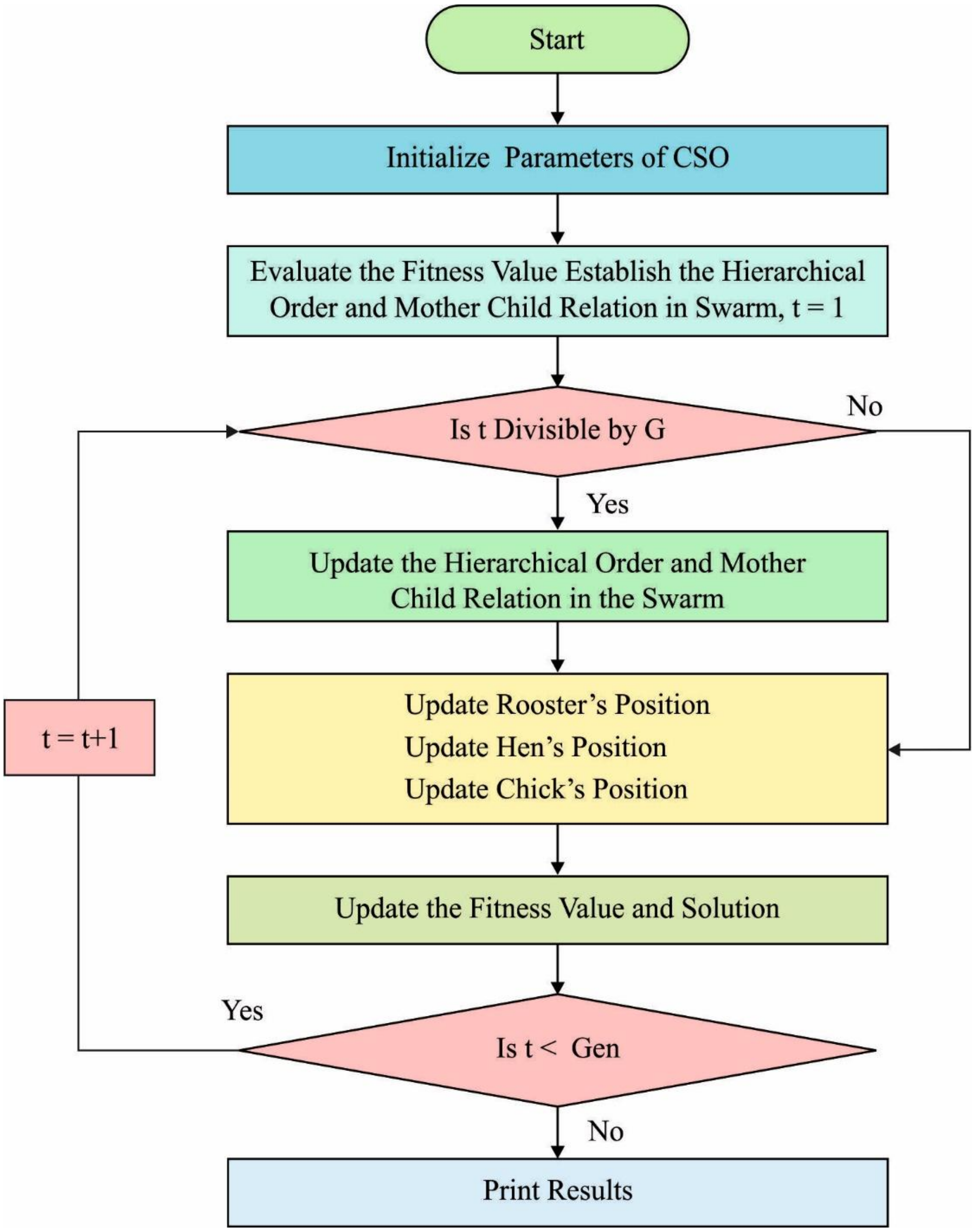
Start
Initialize Parameters of CSO
Evaluate the Fitness Value Establish the Hierarchical Order and Mother Child Relation in Swarm, t = 1
Is t Divisible by G
No
Yes
Update the Hierarchical Order and Mother Child Relation in the Swarm
Update Rooster's Position
Update Hen's Position
Update Chick's Position
t = t+1
Update the Fitness Value and Solution
Yes
Is t < Gen
No
Print Results

Fig. 2. Flowchart of CSO technique

The recurrent place of chick was determined as:

$$x_{i,j}^{t+1} = x_{i,j}^{t} + FL * \left(x_{m,j}^{t} - x_{i,j}^{t}\right), \tag{6}$$

where $x_{m,j}^{t}$ implies the mother hen of chicks and FL refers the random factor from the scope of zero and two.

The CSOC-BT approachobtains a FF with use of three input variables as distance to neighbours, energy to CH selection, and trust level.

Distance to neighbors: It can beappropriateto choose CH with minimal distance amongneighbouring vehicles. While the intra cluster broadcast process, sensor vehicle power utilization to CH transmission. If the neighbouring vehicle distance was decreased, afterward the power of intra cluster transmission is also minimalized.

Objective 1: Minimalize

$$f_1 = \sum_{j=1}^{m} \frac{1}{l_j} \left(\sum_{i=1}^{l_j} dis(CH_j, s_i) \right) \tag{7}$$

Trust factor (TF): To begin with, the complete vehicle was explained that TF is one. The value of TF was decreased by abnormal forecast module if the vehicle procedures the anomalous tasks and vehicle is called a malicious vehicle.

Objective 2: Maximalize

$$f_2 = \sum_{j=1}^{m} \frac{1}{m} (TF_j) \tag{8}$$

Energy: It can be count of power utilization likeCHs to RE of CHs. If the CH utilizes minimal power usage like process, sense, and broadcast process also with maximum RE is collected as minimum energy ratio. Therefore lower as energy ratio, the CH selective enhances further feasibility.

Objective 3: Minimalize

$$f_3 = \sum_{j=1}^{m} \frac{E_c(CH_j)}{E_R(CH_j)} \tag{9}$$

During the presented CSOC-BT approach, it could be essential for decreasing the linear integration of objective function. Therefore, the potential energy function of SHPC-SEMD manner was executed by:

$$Minimize\ Potiential\ energy\ function = \alpha_1 \times f_1 + \alpha_2 \times f_2 + \alpha_3 \times f_3 \tag{10}$$

Where $\alpha_1 + \alpha_2 + \alpha_3 = 1, \alpha_2 \geq (\alpha_1 + \alpha_3). Also$ $0 < f_1, f_2, f_3 < 1$.

2.2. Blockchain Enabled Secure Transmission

A blockchain is a collection of blocks. All the blocks contain 4 sections: hash value of previous block, data about the transaction (ethereum, bitcoin), the timestamp, and current block. Also, blockchain is determined as a distributed common electronic ledger i.e., utilized for saving the transaction data with different perspectives. The transaction could be recorded by cryptographic hash values i.e., tested by each miner. It can be held with related values in the comprehensive ledger and is made up of blocks of each transaction, as shown in Fig.3. The blockchain offers the capacity to share ledger information in a secure form [18].

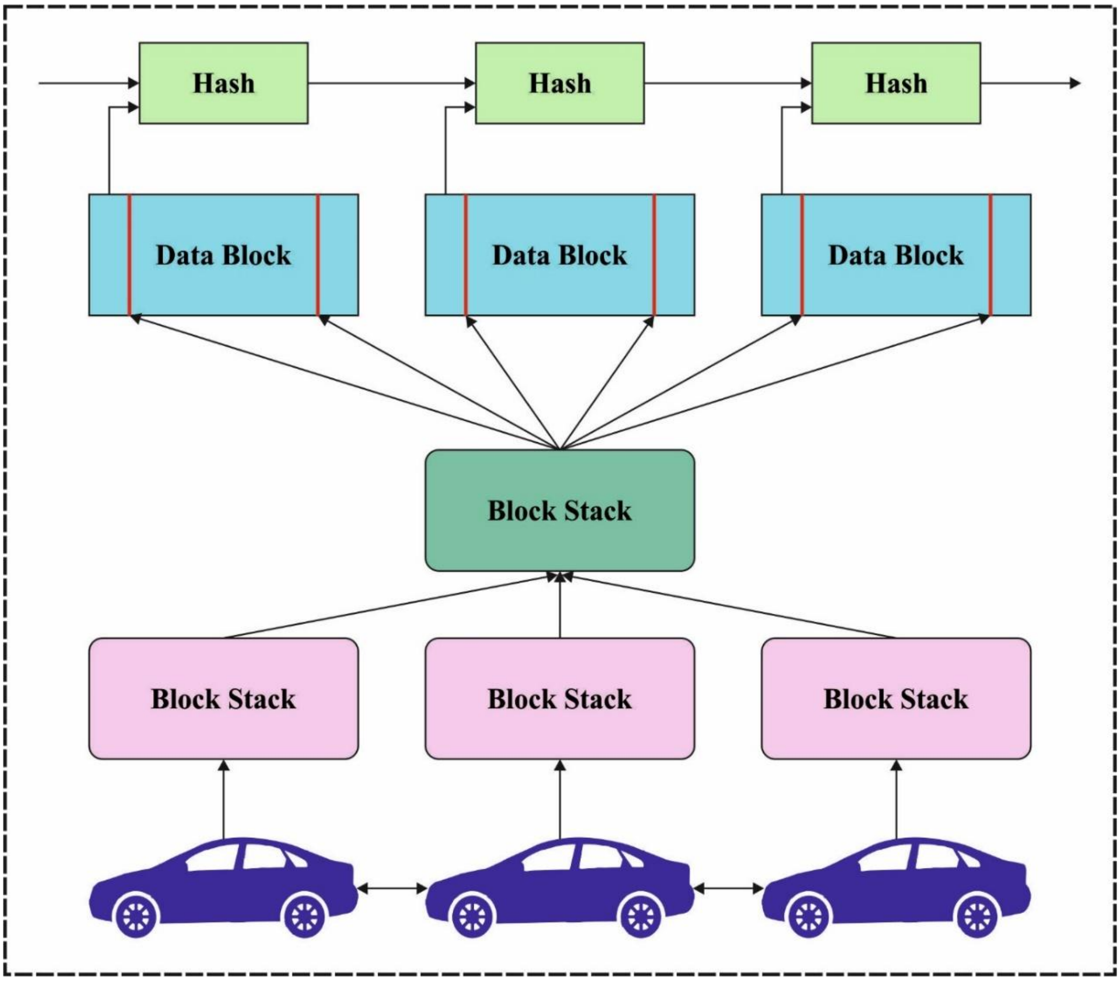

Fig. 3. Blockchain structure

It must be considered that vehicles communicate with each other via V2V and V2X transmission, and these vehicles could interconnect to the Internet efficiently. Also, considered that each vehicle is indispensable namely GPS, OBUs, and sensors. Furthermore, the amount of legitimate RSUs is greater than susceptible RSUs. It can be considered that critical event message is distributed inside an ROI. Also, the total number of messages is indispensable to ensure that the message and event are accurately recognized. A novel kind of blockchain is required, as standard blockchain could not be employed for these purposes. A conventional blockchain employed is cryptocurrency, when we want a blockchain which handles safety event messages without utilizing crypto-coins. It can be single blockchain which can be supervised and balanced independently for recording the transported information. Each vehicle broadcast its position using beacon messages. Each vehicle requires an LC to accept its location concurrently.

The problem of timeliness and scalability in the earlier blockchain becomes insurmountable for realtime VANET applications. Hence, a novel blockchain method is needed. From this autonomous blockchain, each miner mines new blocks as per the event message and transmits each recently minted block to the local blockchain networks. Next, a vehicle could enquiry its safety level, if necessary, by using the blockchain.

3. Experimental Validation

The performance validation of the CSOC-BT technique is performed under varying numbers of vehicles/nodes [19]. Fig. 4 and Table 1 demonstrate the PDR analysis of the CSOC-BT manner with recent methods. The results reported that the CSOC-BT technique has reached increased PDR under all nodes. For instance, under 20 nodes, the CSOC-BT approach has attained higher PDR of 0.97 but the STBBA, ASC, LAKAP, and HEPPA approaches have obtained lower PDR of 0.94, 0.70, 0.76, and 0.84 correspondingly. In addition, under 100 nodes, the CSOC-BT technique has offered increased PDR of 0.79 while the STBBA, ASC, LAKAP, and HEPPA approaches have gained decreased PDR of 0.75, 0.57, 0.53, and 0.57 correspondingly. The results also revealed that the PDR gets reduced with a rise in node count.

Table 1 PDR analysis of CSOC-BT technique with existing approaches

Packet Delivery Ratio					
Number of Nodes	**CSOC-BT**	**STBBA**	**ASC**	**LAKAP**	**HEPPA**
20	0.97	0.94	0.70	0.76	0.84
40	0.89	0.86	0.68	0.63	0.73
60	0.85	0.81	0.64	0.58	0.70
80	0.83	0.79	0.64	0.57	0.67
100	0.79	0.75	0.57	0.53	0.57

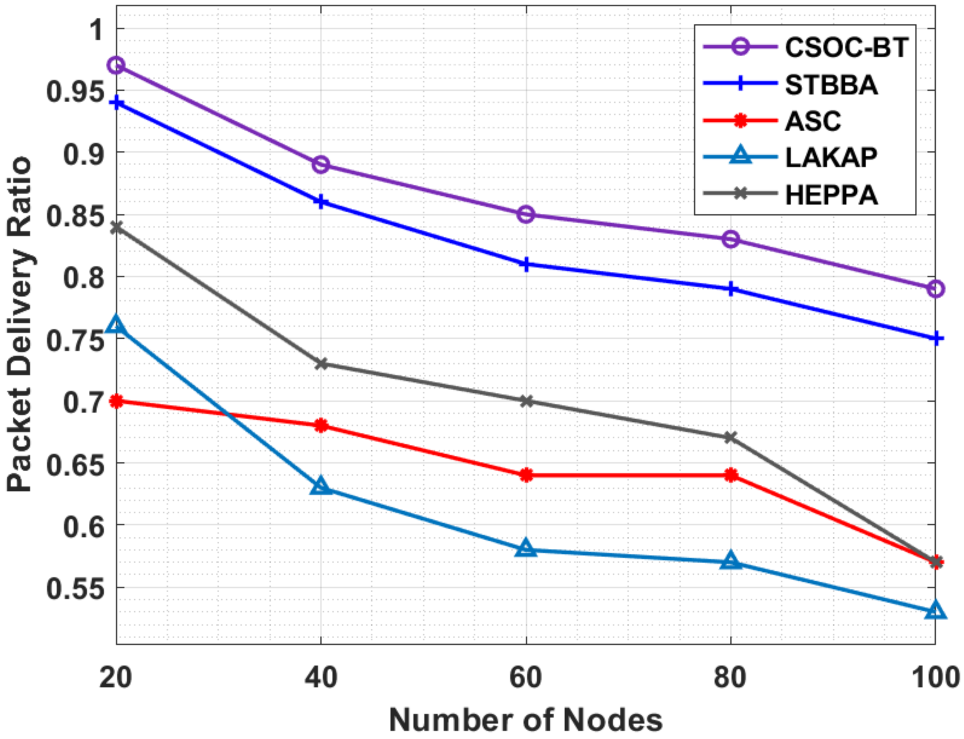

Fig. 4. PDR analysis of CSOC-BT technique under count of nodes

Fig. 5 and Table 2 offered a detailed ETED analysis of the CSOC-BT and other techniques. The figure exhibited that the CSOC-BT technique has produced effective outcome with the minimum ETED under all nodes. For instance, with 20 nodes, the CSOC-BT algorithm has resulted in minimal ETED of 0.079s but the STBBA, ASC, LAKAP, and HEPPA methods have exhibited maximal ETED of 0.094s, 0.131s, 0.122s, and 0.277s respectively. Likewise, with 100 nodes, the CSOC-BT technique has accomplished least ETED of 0.121s whereas the STBBA, ASC, LAKAP, and HEPPA approaches have got increased ETED of 0.131s, 0.350s, 0.523s, and 0.466s respectively. The results also discovered that the ETED seems to be increased with a rise in node count.

Table 2 ETED analysis of CSOC-BT technique with existing approaches

End to End Delay (s)					
Number of Nodes	**CSOC-BT**	**STBBA**	**ASC**	**LAKAP**	**HEPPA**
20	0.079	0.094	0.131	0.122	0.277
40	0.083	0.108	0.212	0.177	0.297
60	0.107	0.124	0.242	0.272	0.327
80	0.110	0.131	0.320	0.376	0.435
100	0.121	0.131	0.350	0.523	0.466

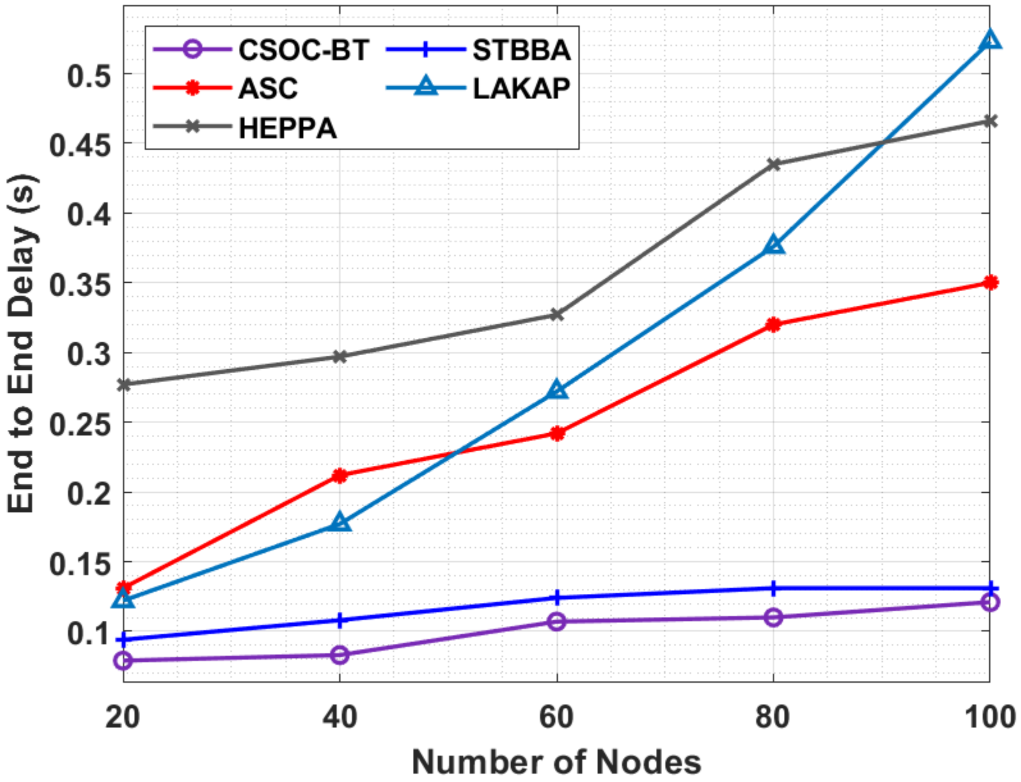

Fig. 5. ETED analysis of CSOC-BT technique under count of nodes

Fig. 6 and Table 3 provided a detailed PL analysis of the CSOC-BT and other techniques. The figure portrayed that the CSOC-BT manner has produced effective outcomes with the lower PL under all nodes. For instance, with 20 nodes, the CSOC-BT technique has resulted in lesser PL of 5.26% whereas the STBBA, ASC, LAKAP, and HEPPA methods have demonstrated superior PL of 5.99%, 24.04%s, 30.19%, and 16.23% correspondingly. Similarly, with 100 nodes, the CSOC-BT technique has accomplished least PL of 22.54% whereas the STBBA, ASC, LAKAP, and HEPPA approaches have got increased PL of 25.72%, 47.50%, 43.22%, and 43.03% correspondingly. The results also discovered that the PL clear that improved with an increase in node count.

Table 3 Packet loss analysis of CSOC-BT technique with existing approaches

Packet Loss (%)					
Number of Nodes	**CSOC-BT**	**STBBA**	**ASC**	**LAKAP**	**HEPPA**
20	5.26	5.99	24.04	30.19	16.23
40	10.71	13.81	37.08	32.61	27.02
60	15.18	19.58	41.73	35.77	30.00
80	17.62	20.32	42.85	36.52	32.42
100	22.54	25.72	47.50	43.22	43.03

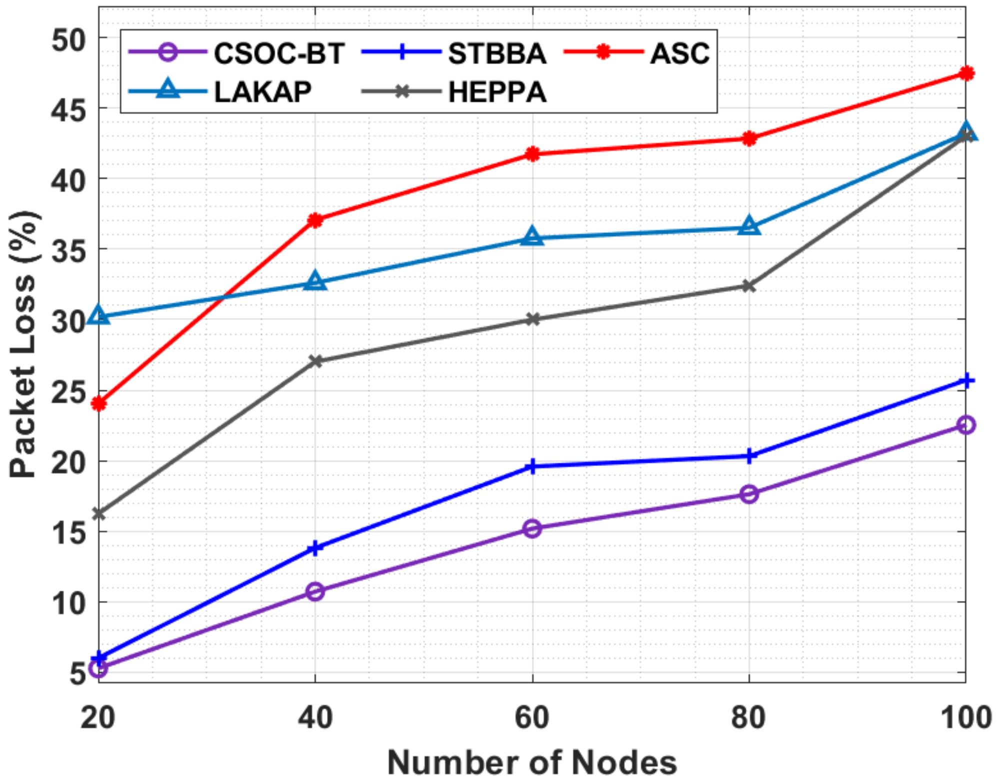

Fig. 6. Packet loss analysis of CSOC-BT technique under count of nodes

Fig. 7 and Table 4 presented a comprehensive TOH analysis of the CSOC-BT and other manners. The figure showcased that the CSOC-BT technique has produced effective outcomes with the lower TOH under all nodes. For instance, with 20 nodes, the CSOC-BT system has resulted in minimal TOH of 1.369kB whereas the STBBA, ESPA, and SPACF methods have demonstrated maximum TOH of 1.847kB, 3.607kBs, and 3.287kB respectively. Along with that, with 100 nodes, the CSOC-BT technique has accomplished least TOH of 4.429kB whereas the STBBA, ESPA, and SPACF approaches have got increased TOH by 5.128kB, 20.734kB, and 12.651kB correspondingly. The outcomes also exposed that the TOH appears that maximum with a rise in node count.

Table 4 Transmission overhead analysis of CSOC-BT technique with existing approaches

Transmission Overhead (kB)				
Number of Nodes	**CSOC-BT**	**STBBA**	**ESPA**	**SPACF**
20	1.369	1.847	3.607	3.287
40	2.227	2.887	6.328	5.768
60	2.781	3.287	10.410	7.449
80	3.335	3.767	15.532	8.569
100	4.429	5.128	20.734	12.651

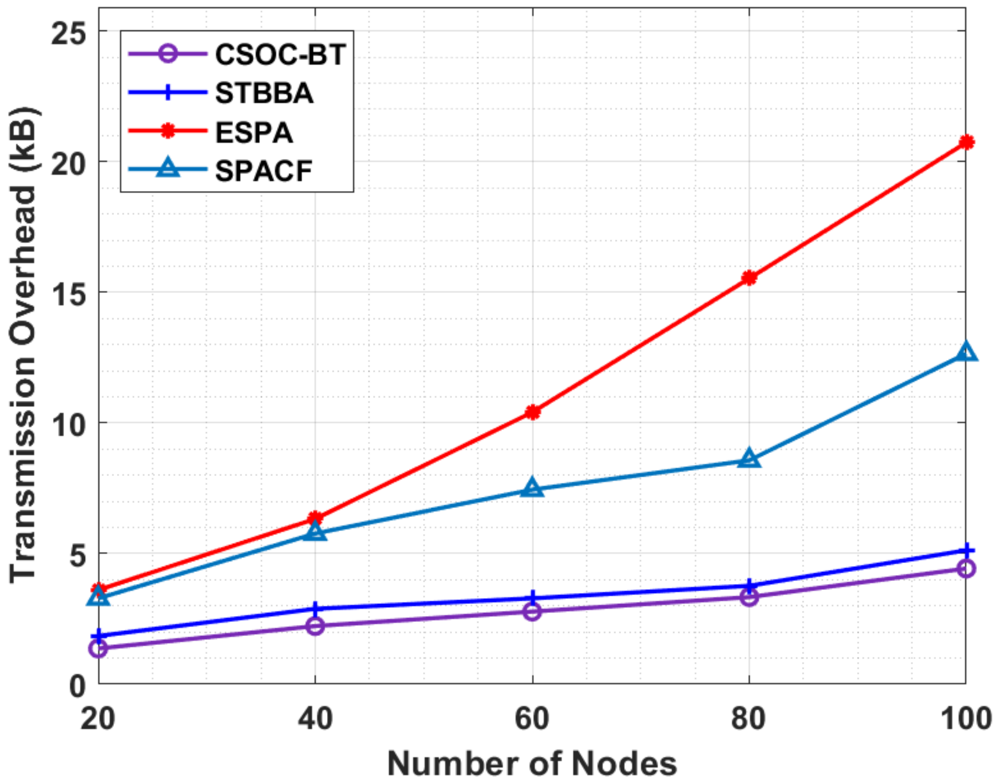

Fig. 7. TOH analysis of CSOC-BT technique under count of nodes

Fig. 8 and Table 5 accessible a brief CC analysis of the CSOC-BT and other approaches. The figure outperformed that the CSOC-BT manner has produced effectual outcomes with the minimal CC under all nodes. For instance, with 20 nodes, the CSOC-BT system has resulted in less CC of 0.087ms whereas the STBBA, ASC, LAKAP, and HEPPA methods have outperformed maximal CC of 0.119ms, 0.253mss, 0.426ms, and 0.349ms correspondingly. Followed by, with 100 nodes, the CSOC-BT technique has accomplished least CC of 0.326ms whereas the STBBA, ASC, LAKAP, and HEPPA approaches have got increased CC of 0.373ms, 0.558ms, 844ms, and 0.716ms correspondingly. The outcomes also revealed that the CC seems to be enhanced with increase in node count.

Table 5 Computational cost analysis of CSOC-BT technique with existing approaches

Computational Cost (ms)					
Number of Nodes	**CSOC-BT**	**STBBA**	**ASC**	**LAKAP**	**HEPPA**
20	0.087	0.119	0.253	0.426	0.349
40	0.135	0.172	0.334	0.584	0.449
60	0.189	0.228	0.419	0.660	0.539
80	0.291	0.341	0.479	0.746	0.618
100	0.326	0.373	0.558	0.844	0.716

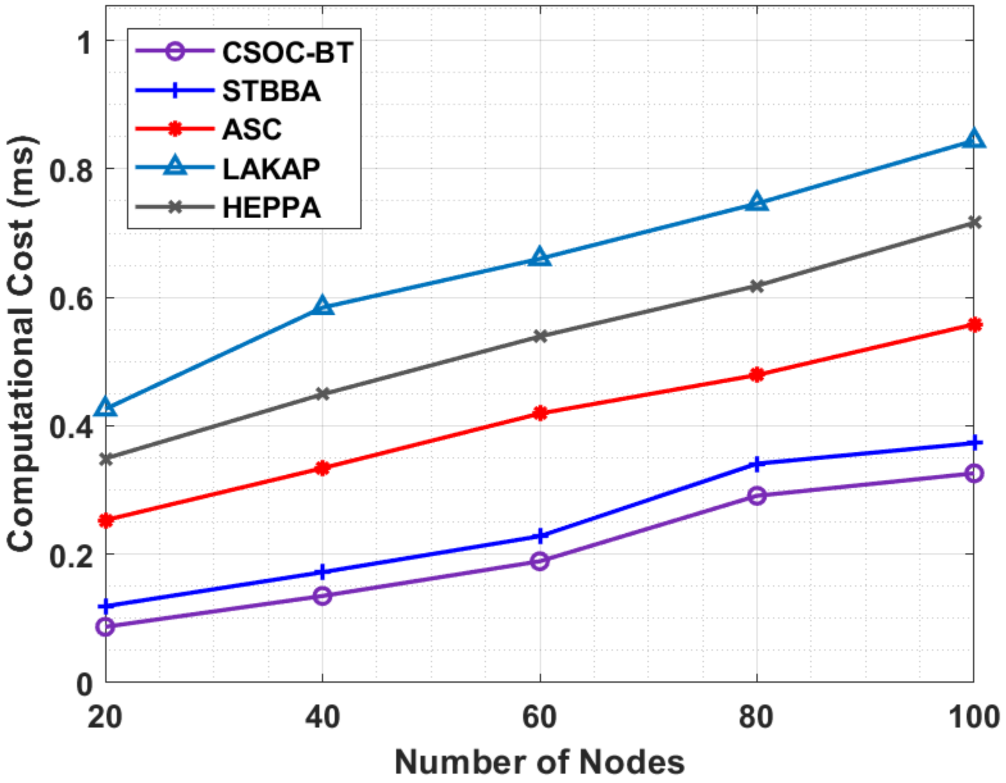

Fig. 8. Computational cost analysis of CSOC-BT technique under count of nodes

4. Conclusion

In this study, a novel CSOC-BT technique is derived to accomplish privacy preserving communication in clustered VANET. The CSOC-BT technique derives a fitness function involving multiple input parameters to select CHs and organize clusters. Furthermore, blockchain technology is utilized for secure inter-cluster and intra-cluster communication in the network. For examining the enhanced performance of the CSOC-BT technique, a series of experiments were carried out under the existence of attacks. The experimental results outperformed the enhanced performance of the CSOC-BT technique over the recent state of art approaches interms of different measures. In future, the performance of the CSOC-BT technique can be boosted by the design of multihop routing techniques.

References

[1] Ghori, M.R.; Zamli, K.Z.; Quosthoni, N.; Hisyam, M.; Montaser, M. Vehicular ad-hoc network (VANET): Review. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development ICIRD, Bangkok, Thailand, 11–12 May 2018.

[2] Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. 2012, 50, 217–241.

[3] Abbasi, I.A.; Khan, A.S. A review of vehicle to vehicle communication protocols for VANETs in the urban environment. Future Int. 2018, 10, 14.

[4] Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. Comput. Commun. 2014, 44, 1–13.

[5] Ostermaier, B.; Dotzer, F.; Strassberger, M. Enhancing the security of local dangerwarnings in vanets—A simulative analysis of voting schemes. In Proceedings of the 2nd International Conference on Availability, Reliability and Security, Vienna, Austria, 10–13 April 2007; pp. 422–431.

[6] Patel, N.J.; Jhaveri, R.H. Trust based approaches for secure routing in VANET: A survey. Procedia Comput. Sci. 2015, 45, 592–601.

[7] Rajput, U.; Abbas, F.; Eun, H.; Oh, H. A hybrid approach for efficient privacy-preserving authentication in VANET. IEEE Access 2017, 5, 12014–12030.

[8] Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A secure privacy-preserving authentication scheme for VANET with CUCKOO Filter. IEEE Trans. Veh. Technol. 2017, 66, 10283–10295.

[9] Ying, B.; Nayak, A. Anonymous and lightweight authentication for secure vehicular networks. IEEE Trans. Veh. Technol. 2017, 66, 10626–10636.

[10] Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. IEEE Internet Things J. 2019, 6, 8076–8094.

[11] Malik, N., Nanda, P., He, X. and Liu, R.P., 2020. Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. Wireless Networks, 26(6), pp.4207-4226.

[12] Akhter, A.F.M., Ahmed, M., Shah, A.F.M., Anwar, A. and Zengin, A., 2021. A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET. Sustainability, 13(1), p.400.

[13] Kchaou, A., Abassi, R. and Guemara, S., 2018, August. Toward a distributed trust management scheme for vanet. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-6).

[14] Kadadha, M. and Otrok, H., 2021. A blockchain-enabled relay selection for QoS-OLSR in urban VANET: A Stackelberg game model. Ad Hoc Networks, 117, p.102502.

[15] Joshi, G.P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T. and Ibrahim, A., 2020. Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), p.1358.

[16] Ahmed, M., Moustafa, N., Akhter, A.S., Razzak, I., Surid, E., Anwar, A., Shah, A.S. and Zengin, A., 2021. A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET. IEEE Transactions on Intelligent Transportation Systems.

[17] Wang, Z., Qin, C., Wan, B., Song, W.W. and Yang, G., 2021. An Adaptive Fuzzy Chicken Swarm Optimization Algorithm. *Mathematical Problems in Engineering*, *2021*.

[18] Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. Digit. Commun. Netw. 2020, 6, 177–186.

[19] Khan, A.S., Balan, K., Javed, Y., Tarmizi, S. and Abdullah, J., 2019. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors*, *19*(22), p.4954.