Secure Internet of Vehicles (IoV) with Decentralized Consensus Blockchain Mechanism

Shanshan Tu *Member, IEEE*, Haoyu Yu, Akhtar Badshah Muhammad Waqas *Senior Member, IEEE*, Zahid Halim *Senior Member, IEEE* and Iftekhar Ahmad, *Senior Member, IEEE,*

[1]

***Abstract*—The Internet of vehicles (IoV) is increasingly being used to realize the vision of intelligent transportation systems with the rapid development of computation and communication technologies. However, numerous IoV applications rely on a central unit for storing and processing information and mediators for wireless transmission. This can lead to the leakage of sensitive data and high costs and delays. To address these issues and improve the efficiency of data storage, processing, and sharing in the IoV, we propose a vehicle-based secure blockchain consensus (VBSBC) algorithm. Our VBSBC algorithm overcomes the limitations and drawbacks of state-of-the-art approaches by leveraging blockchain technology and a consensus algorithm to ensure secure communication between vehicles. In addition, the algorithm includes an authentication process and a key distributing and request process, illustrated during vehicles' movement between different zones. In simulation results, our proposed VBSBC algorithm demonstrated high performance compared to existing approaches in terms of authentication delay, key processing time, attack detection rate, throughput, and packet loss rate.**

***Index Terms*—Blockchain, Internet of vehicles, security, authentication, key processing.**

I. Introduction

A. Motivation

Blockchain, originating from Bitcoin, enables parties involved in a transaction to build trust among untrusted entities through decentralization. The triumph of Bitcoin has sparked heightened interest in blockchain, leading researchers to investigate its potential applications across multiple industries [1], [2]. As vehicles become more intelligent and autonomous, the Internet of vehicles (IoV) concept has emerged. The IoV concept aims to create an interconnected infrastructure for smart vehicle information and resource exchange, which will facilitate the development of an intelligent transportation system (ITS) [3]. Through IoV, ITS will involve an increasing number of connected and intelligent automobiles and enable continuous connectivity among vehicles, roadside infrastructures, and pedestrians [4]. This interconnected infrastructure will bring benefits, including enhanced road safety, safer driving, more efficient traffic flow, better parking management, and expanded use of multimedia services. Implementing IoV is expected to bring ITS to fruition in the coming years, meeting the growing demands for ITS with the vehicle-to-everything (V2X) concept. The ultimate aim is to create a standardized, intuitive, interconnected infrastructure for smart vehicle information and resource exchange [5].

The growth in smart vehicles is expected to result in a massive data exchange, boosting traffic flow thanks to vehicle-based applications and services. To handle the expansion of IoV, the data exchange and storage platform in IoV needs to be decentralized, adaptable, flexible, and capable of scaling [4]. However, using typical cloud-based concurrent control and processing methods would present significant challenges for IoV due to its high speed, low latency, contextual complexity, and diversity features [6]. Additionally, ensuring robust compatibility and interoperability among IoV entities from multiple service operators is crucial. There is a question about whether all vehicles should be allowed to participate in the IoV or only certain trusted vehicles. Unauthorized vehicles can violate privacy and pose risks to the system. Furthermore, the system is distributed and decentralized and more vulnerable to threats. Therefore, it is critical to ensure the confidentiality, anonymity, and reliability of IoV [7]. Therefore, this article puts forth a secure and low-latency authentication scheme for vehicles utilizing blockchain security. The concept is based on decentralized authentication with a zone-based architecture to improve authentication latency, attack detection rate, and key processing time in ITS.

The main contribution of our proposed work is outlined in the following subsection. Here, we explain how our proposed low-delay authentication scheme will enhance the security of the IoV by addressing the challenges and concerns mentioned in existing research. In addition, we leverage blockchain technology's decentralized, immutable, and transparent nature and a zone-based architecture to ensure faster authentication, attack detection, and key processing time.

Corresponding Author: Muhammad Waqas, engr.waqas2079@gmail.com)

S. Tu and H. Yu are with the Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China. (emails: sstu@bjut.edu.cn, yuhaoyu@emails.bjut.edu.cn)

S. Tu and H. Yu are with the Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China. (emails: sstu@bjut.edu.cn, yuhaoyu@emails.bjut.edu.cn)

A. Badshah is with the Department of Software Engineering, University of Malakand, Dir Lower, Pakistan. (email: akhtarbadshah@uom.edu.pk)

M. Waqas is with the Computer Engineering Department, College of Information Technology, University of Bahrain, 32038, Bahrain and also with the School of Engineering, Edith Cowan University, WA 6027, Australia. (email: engr.waqas2079@gmail.com)

Z. Halim is with the Faculty of Computer Science and Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi 23640, Pakistan. (email: zahid.halim@giki.edu.pk)

I. Ahmad is with the School of Engineering, Edith Cowan University, Perth WA 6027, Australia (e-mail: i.ahmad@ecu.edu.au)

B. Related Work

Blockchain technology can address numerous problems effectively in vehicle management systems, particularly in relation to centralized smart parking. These issues include the requirement to expose personal data, such as destination details, when searching for and reserving available parking and the vulnerabilities of a centralized architecture, including the potential for accessibility attacks and data leakages. To address these issues, Amiri *et al*. [8] proposed a privacy-preserving smart parking system using blockchain and private information retrieval. Their proposed system uses a consortium blockchain and private information retrieval to enable drivers to privately retrieve real-time parking information and authenticate anonymously for reserving parking slots. Evaluation results showed that the proposed system effectively preserves drivers' privacy with low communication and computation overheads. In fact, the alliance chain is just a semi-decentralized system. As long as most of the organizations in the alliance reach a consensus, the block data can be changed.

Xiao *et al*. [9] proposed a platoon-driving model for autonomous vehicles to improve traffic and reduce accidents. The model uses smart contracts for payments and demonstrates superior performance for fuel consumption, platoon head revenue, and platoon member charges compared to alternative approaches. However, their proposed mechanism is based on smart contracts, which may be difficult to be adopted widely.

The authors of the article presented in [10] proposed a practical and secure approach for blockchain to facilitate information sharing between vehicles. This approach includes a unique key negotiation scheme with transparency and verification features intended to effectively address data protection, surveillance, and reliability issues. However, the process of key agreement may still present potential security risks.

To enable rapid and dynamically executed key agreements in vehicular networks, the proposed approach provides automatic key agreements based on fixed or variable protocols [11], [12]. The networking challenges, such as establishing trust while maintaining the confidentiality and anonymity of participants, can be addressed through blockchain.

The authors of the article presented in [13] proposed a wireless channel transmission method based on a link fingerprint (LF) to generate blocks, while [14] proposed an improved security algorithm to make the fingerprint generation process more lightweight. However, the model relies on the cloud as the central server for transaction assurance, rather than using it as a node in the blockchain. As a result, it is not practical to use the blockchain for verification in this way. The authors of the article presented in [15] proposed a blockchain-assisted resource-sharing solution for IoV. They used a consortium blockchain and proposed a lighter-weight consensus protocol to establish trust and reduce the computationally intensive mining process.

The majority of existing works on blockchain technology have focused on improving only a few of its properties, such as scalability, decentralization, delays, and security. For example, proof-of-work systems without permission offer decentralization and security but suffer poor scalability [16]. Likewise, central block processing mechanisms prioritize scalability but sacrifice decentralization of block producers [17]. Meanwhile, multi-chain systems achieve scalability and decentralization at the expense of increased risk [18].

This paper proposes an efficient method for building a blockchain-enabled IoT network that addresses these issues. We also present an overview of existing efforts to evaluate the efficiency of blockchain systems. In [19], the authors compared the performance of different isolated blockchains in terms of time delay, but their evaluation was based on simulation and did not provide quantitative results. Gencer *et al*. [20] compared the decentralization of Bitcoin and Ethereum using various metrics such as provisioned bandwidth, network structure, mining power distribution, mining resource usage, and fairness. Still, their approach only applies to proof-of-work systems and does not provide clear quantification of variables. Finally, in [20] and [21], the authors quantitatively measured the decentralization, security, and delays of proof-of-work blockchains by evaluating the number of blocks, producers, likelihood, and transmission time, respectively. While these studies offer some insights into the implementation of blockchain systems, they are not comprehensive and lack generalizability. This also encourages us to develop a comprehensive procedure for evaluating blockchain systems to optimize their performance.

C. Research Contributions

Based on the problems mentioned above, we propose an efficient scheme to illustrate the effectiveness of blockchain-enabled IoV in a decentralized manner. Our significant contributions are as follows:

- We investigate the security aspect of the IoV by incorporating blockchain technology and a consensus algorithm to overcome the data leakage problem and ensure the effectiveness of handling gigantic data in the IoV.
- We propose a vehicle-based secure blockchain consensus (VBSBC) algorithm to address the limitations and drawbacks of existing state-of-the-art solutions. Additionally, we illustrate the authentication process, key distribution, and request process during the movement of vehicles among different zones.
- Simulation results demonstrate that our proposed VBSBC algorithm outperforms existing state-of-the-art solutions regarding authentication delay, key processing time, attack detection rate, throughput, and packet loss rate.

The remaining sections of the paper are organized as follows: In Section II, we propose a system architecture. Section III explains the concept of a blockchain-based controller. The authentication process, key distribution, and the requesting process are covered in Section IV and Section V, respectively. The procedures for migration and authentication are discussed in Section VI. In Section VII, we present simulation results. Finally Section VIII concludes the paper and summarize our findings.

II. Proposed System Architecture

Vehicles are divided into various zones in our proposed system architecture, as illustrated in Fig. 1. Each zone has

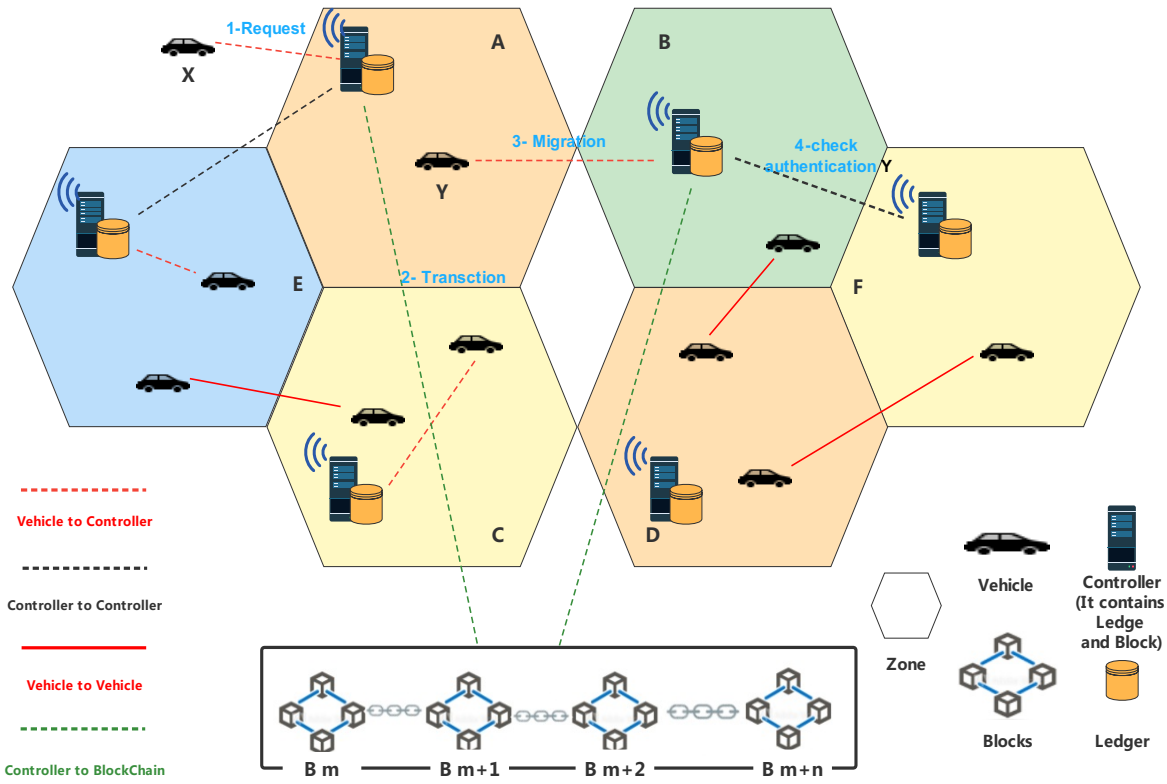

Fig. 1. Our proposed zone (Cluster)-based architecture for the Internet of vehicles (IoV) using blockchain.

a unique controller that manages and controls all the events taking place within the zone, such as the authentication of vehicles, migration, and communication among vehicles using a distributed ledger based on blockchain technology. The controllers, in this case, Roadside Units (RSUs), are assumed to have no limitations on energy consumption or processing power [22], while the vehicles have constraints on energy consumption and computational power [23]. Therefore, the zones are structured to enable communication between different controllers (RSUs) through R-to-R, RSU-to-vehicle communication through R-to-V, vehicle-to-vehicle communication through V-to-V, and RSU-to-blockchain communication through R-to-B. In addition, the zones can securely communicate with each other through a peer-to-peer (P2P) network enabled by the blockchain.

Scalability is an essential problem in the authentication process, especially given the high speeds at which vehicles are moving [24]. To address this, our proposed architecture uses a hierarchical structure, as illustrated in Fig. 1. Each zone has multiple layers of components, and a controller is responsible for managing a coverage zone. Controllers, R, communicate with each other in a network and interact with the public blockchain. Several possible events can occur between vehicles, controllers, and blockchains in the scenario. First, there are events between the vehicle and the controller, such as registration and join requests, migration requests, or essential vehicle services, as marked in Fig. 1 as $1, 2, 3$. Additionally, there are events between different controllers, such as checking authentication and events between the controller and blockchain. It is assumed that if a controller, R, goes down in any zone, an alternate controller in the network must manage the affected zone. It is also assumed that the controller, R, has all the information about the vehicles in its zone and the zone's strategy derived from the vehicles' information in the higher layer of the shared ledger. Therefore, the proposed architecture is adaptable and can accommodate changes in the number of zones, controllers, and vehicles.

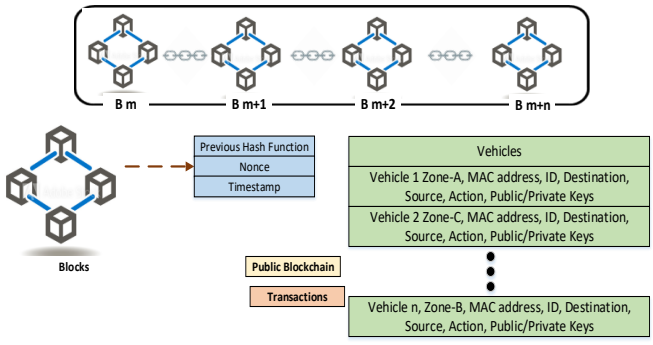

Fig. 2. Blockchain details and public blockchain in IoV.

The blockchain structure for the vehicular network is shown in Fig. 2. The system contains blockchain blocks of transactions, secret keys, and hash functions. Transactions encompass

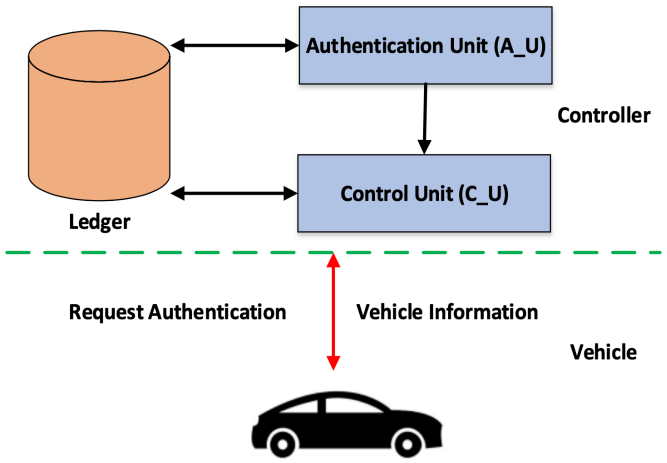

Fig. 3. Functional diagram between controller and vehicle in blockchain-enabled IoV.

all vehicle information, including vehicle ID, MAC address, zone number, and direction and route data. Each vehicle has public/private keys generated by R during registration. The vehicles can use the public key in their zones for data communication. The private key can be used during the migration from one zone to another and communications with other vehicles in different zones.

III. Blockchain-Based Controller

Specifically, the controller's internal structure and connection with the vehicles are shown in Fig. 3. The essential components for the controller, R, are the ledger, authentication unit, and control unit. The ledger, represented by $\mathcal{L}$, sustains and stores the vehicles' information. The controller's tasks can be adopted from the mechanism presented in [25]. We considered the public blockchain because the vehicles can register in any zone for secure communication and migration during movement. Consequently, it helps us to maintain the privacy of the vehicles [26]. The vehicles can enter the network and allocate public or private keys for the public blockchain. The blocks in the blockchain include secret keys, hash functions, and transactions in the public blockchain. The transactions contain vehicle data, such as the unique ID of vehicles with MAC addresses collected during driving. In contrast, the system creates a vector, represented by $\mathcal{V}_{info}$, which stores the information. The vehicles can obtain the public or private keys through $\mathcal{V}_{info}$ and a valid ID to enter their respective zones. They can also use the information for migration to other zones using $\mathcal{V}_{info}$.

It is noted that the controllers are handled by the consensus process proposed in [27], which is a secure and low latency proof of work protocol. Keeping the current consensus algorithm, we offered a vehicle-based secure blockchain consensus (VBSBC) algorithm due to limitations and drawbacks in the existing literature, i.e., centralized systems and flaws of real-life voting [28]. Our proposed VBSBC checks and endorses

Algorithm 1 Vehicle-based Secure Blockchain Consensus (VBSBC) Algorithm

```
Controller = Zone Information (Block Header, Block Version, Timestamp, Transactions)
Create Group (Group of agents for Mining Process) (Group of agent for Mining Process)
Controller ⟹ Data transferring among vehicles
Calculate transactions
Calculate functions
Calculate Hashed block header
    While Count_Zone do
     Mining the block
     Verify the Header
       Hash Function = endorse —— nonce; //endorse include header,pre-header,timestamp,transactions
     R = hash (H_m —— Nonce)
     Coordinate the Zones
     Extricate Nonce = getNonce (H_m)
     Transactions in Data
     nonce + +;
     end While
Blocks (Zone(j) = Data) //Mining Processing success
Share the Data of Zone
```

the transactions in their respective zones. To reduce overhead and the number of nodes, every authentication process between vehicles and controllers will only be allowed in the respective zones, which significantly optimizes processing time when vehicles join or exit. It also gets the approval of the vehicles in the zone during movement. In addition, VBSBC is needful for consensus algorithm in the vehicular network, illustrated in Algorithm 1 and Fig. 4. It is worth noting that our architecture also suffers from 51% computing power attack due to the common problem of the proof of work mechanism. Therefore, the proposed system needs to be applied in appropriate situations: sufficient zones and vehicle numbers. This limitation is one of the targets of our future work.

IV. Secure and Authentication Process

In the secure and authentication process, we consider distributed zones among vehicles in the network utilizing the blockchain technique. All the zones must handle the blockchain process and protect the data communication of vehicles while driving. However, we encounter a scenario where vehicles can migrate from one zone to another without re-authentication, which reduces time and computational costs. As observed from Fig. 1, the vehicles must register themselves with the controller in each zone to encrypt the data. In this way, each vehicle receives secret keys and encryption information. Afterwards, the controller transmits the encrypted information to the blockchain and the rest of the controllers simultaneously. The controller, R, accordingly delivers the public/private keys to each vehicle. The overall process is shown in Fig. 5, where the vehicle authentication with the controller occurs as one process. Nevertheless, the vehicle requests the controller to join its zone of interest. The authentication unit, represented as A_U, acquires the proposal and responds to the vehicle

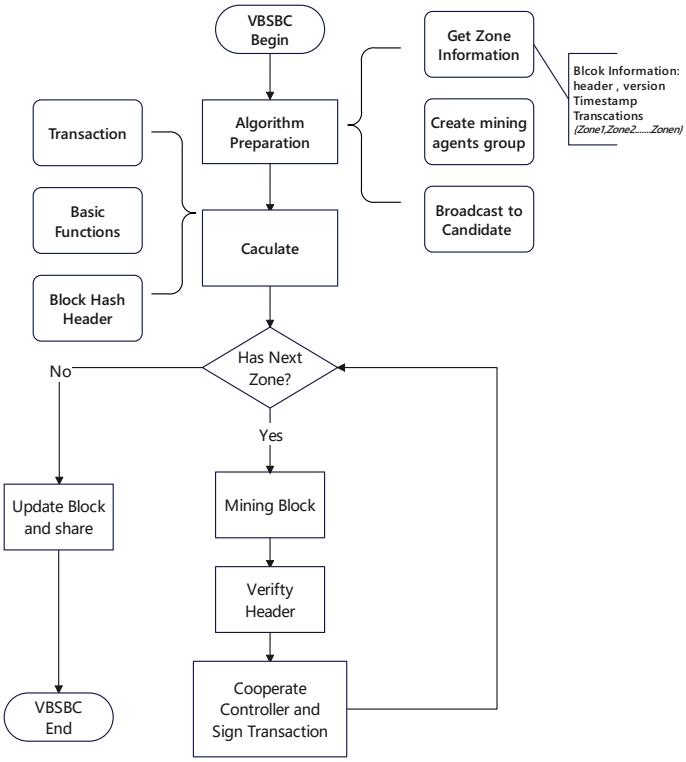

Fig. 4. Algorithm 1 flow chart.

after confirmation. The control unit, represented as C_U, sends the cryptographic information of the keys of the concerned vehicle. When a vehicle repeatedly transmits multiple joining requests to the controller, such flooding requests are considered a security attack. Therefore, the controller must take action as a defense mechanism. In our proposed process, A_U counts the number of requests sent by the vehicles. Hence, the controller considers that specific vehicle as malicious and blocks its ID and MAC address. Therefore, such a vehicle will not be able to enter the zone. The controller can also send information about the malicious vehicle. The blockchain shares this information through a shared ledger, allowing other controllers in different zones to reject such incoming requests by the malicious vehicles.

V. Key Distribution and Requesting Process

The A_U identifies the unique vehicle characteristics, such as location, identity, direction, and public and private keys. The C_U generate these characteristics. Through C_U, the data is explicit to the decentralized ledger security by the mechanism. All the information from the vehicles is registered and sent to the blockchain to save in the ledger. It must also be available for estimation by the other controllers. The public key, K_{pub}, is known only by the vehicles and the controllers, while the private key, K_{pri}, is used to sign transactions between the vehicles. K_{pri} and K_{pub} are mathematically related pairwise keys. The ciphertext encrypted with the K_{pub} can only be decrypted with the corresponding K_{pri}. Conversely, the ciphertext encrypted with the K_{pri} can only be decrypted with the corresponding K_{pub}. However, the controller sends the vehicle information to the blockchain directly.

Fig. 5 shows the whole work process of the proposed architecture. There are several steps involved. In the first step, the vehicle A requests to permit in the zone A that is managed by the controller A. In this way, the communication channel of A is established. Secondly, the vehicle A is authenticated, and controller A needs to transmit the vehicle data to the blockchain. Particularly, the controller shares secret keys protected for every vehicle since the keys are based on specific vehicle information. The vehicle utilized the generated keys with the help of the controller. The vehicle A communicates securely with any other vehicle or controller in any zone as they are authenticated. Moreover, it can securely connect with the blockchain. For instance, a vehicle in zone C can easily communicate with a vehicle in zone B.

Since the controller is responsible for organising and enforcing the zone's policy, in this case, the vehicle wants to travel from the existing zone to the adjacent zone and transmits the request to the destination zone, as shown in Fig. 1. In the destination zone, the authentication will be verified by the controller. The controller ascertains the requested vehicle information by enquiring about the blockchain to find non-authentic vehicles' legitimacy. This is because the blockchain holds the information of all authenticated vehicles. Thus, re-authentication is unnecessary when the vehicle passes through different zones. The controller recognizes the next zone for a vehicle moving and lets the other controller check the C_U and shared ledge. This way ensures that the vehicles are in the correct zone. As shown in Fig. 1, after the request and transaction, there are different processes, i.e., migration to other zones and authentication process.

VI. Migration and Authentication Process

As depicted in Algorithm 2, the migration process is among the zones for secure communication and requires less delayed for authentication process. The controller delivers the ability to manage the key process in zones that alleviate the transfer time for keys between the zones. The main point is to manage the controllers' keys in the zones to get the transfer mechanism. The main aim is to extract the third-party interaction within the transaction. It controls the time of key processing during vehicle authorization with the blockchain comprised of public/private keys. If the controller becomes dysfunctional, the adjacent zone's controller becomes aware of the event through the proposed architecture. In this way, the cellular structure has the least adjacent controller in the adjacent zones to that dysfunctional controller. Only that controller in the respective zone will be selected among these adjacent zones with fewer vehicles.

A transaction involves a series of handshake operations, with each operation in Fig. 5 considered indivisible atomic units. The transaction is only completed if all operations are successful. In the event of a failure in any part of the transaction, previously executed activities must be reversed. The controller must have the capability to undo all prior operations.

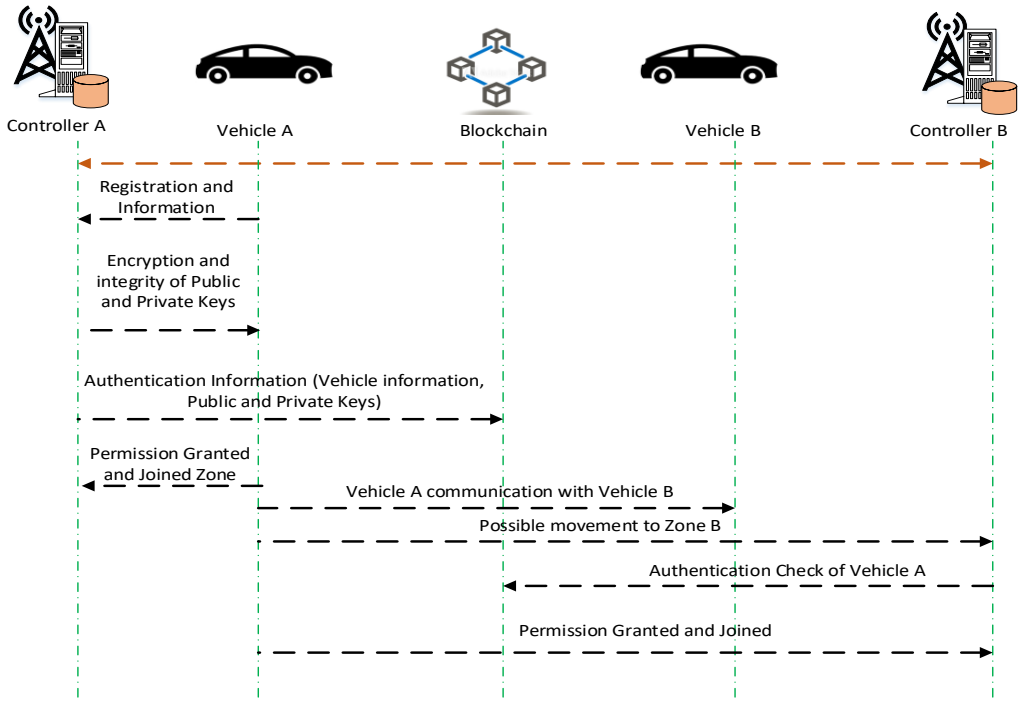

Fig. 5. Registration in a zone in the proposed architecture.

Algorithm 2 Vehicle Migration between Zones

```
Vehicles Registration to controllers in each zone
Required Authentication
Send Public/Private key
        Use Hash Function
        Vehicle_j = Receive (Hash 256)
        Join to Zone
            if Vehicles == registered controller then
            Authentication = True
            Compute the Mobility
            else
            Compute the Migration
            end if
            if moving == Requested then
            Join the Zone
            else
            Block
While Authentication == True do
    if (Mobility/Migration = = True) Then
    if Authenticate in Zone
    Controller_j: Data
    Update the zone information
    Migrate from current to requested zone
    else
    Controller_j: Blockchain updating
    end if
end While
While Authentication == False do
    Next zone controller = Received the data
    Next zone controller = decrypt the data
end While
```

TABLE I
SIMULATION PARAMETERS

Parameters	Values
Transmission Range	500m
Protocol	MAC/802.11
Mobility Model	Random
Number of Vehicles	200
Number of Zones	5
Packet Size	512 Byte
Area	10,000m × 10,000m
Number of Zones	5
Block Size	1 MB to 5 MB
Number of Miners	10 to 100

VII. PERFORMANCE EVALUATION

The proposed architecture's impact on the vehicles' authentication processes during data communication and the prevention of attacks is evaluated. The blockchain mechanism's influence on the proposed architecture is also analyzed. The proposed consensus algorithm is compared with existing techniques, and key generation and processing time are also evaluated. Table I displays the simulation parameters. The simulation is executed for 60 minutes, encompassing 5000 transactions between vehicles and the controller during zone migration. As a result, 1000 simulations are used to obtain the average results. Furthermore, our results are compared with two well-known methods, DPOS and DDPOS, as presented in [25] and [29].

To compare our proposed method's performance, we use the approach in DDPOS [29], which is a drone-based delegated proof of stake for the IoT. During the simulation, we also designed another scenario as a basic model, a traditional cen-

tralized IoV model. The basic model needs the integration of blockchain technology. Instead, it employs a common method utilizing a third-party authentication server for authentication and key exchange between participants. Unlike our model or DDPOS [29], it lacks P2P communication and depends on the authentication server during operation.

In our first experiment, we test the network performance of the proposed method from three dimensions: throughput, end-to-end latency, and packet loss rate. We mathematically evaluated the simulation duration to be 30 minutes. As shown in Fig. 6, the proposed method and the blockchain-based DDPOS algorithm significantly improve these three aspects compared to the basic model. Benefiting from the proposed method reducing the number of nodes during the authentication process, the proposed method outperforms DDPOS in these aspects.

- As shown in Fig. 6 (a), the throughput assents for the proposed method, the basic model, and DDPOS are 271, 185.3 and 257 b/s, respectively. This is because the proposed method and DDPOS did not need re-authentication and had fewer requests.
- In Fig. 6 (b), end-to-end delay is defined as the average time needed by the request and functions from vehicles to the controller or another vehicle. The end-to-end delays are 0.0210, 0.212, 0.0237 b/s for the proposed method, the basic model, and DDPOS. Due to the decentralized system design based on the zone, the transmission distance is shorter.
- In the IoV system, the packet loss rate is a critical parameter. To achieve the communication efficiency of the network, a low packet loss rate must be guaranteed. Fig. 6 (c) shows the packet loss rate between the proposed architecture and other existing models. The results show that the zone-based management model has a lower packet loss rate.

Afterwards, we investigated the effect of the number of vehicles on the authentication delay as illustrated in Fig. 7. The authentication delay is the time the zone requires to authenticate the vehicles after sending the request to join the zone. For example, the DPOS [25] requires re-authenticating the vehicles before joining any zone. The joining process requires re-approving the vehicles among the zones when the vehicle moves from one zone to another. Hence, it requires the authentication process in every zone. On the other hand, DDPOS [29] does not need to re-authenticate the vehicles, and the same is the case with our proposed method. However, our proposed VBSBC algorithm required less authentication delay than DPOS and DDPOS due to its less time required. This shows that the vehicles can move faster and no re-authentication is necessary, proving our proposed work's efficacy.

We assess the effect of blockchain parameters, such as block size and miner count, on the proposed architecture's bandwidth and throughput. The number of transactions depends on the size of the block, which manages the throughput achieved by the proposed method. However, bigger blocks have slower propagation in different zones. As shown in Fig. 8 (a), the

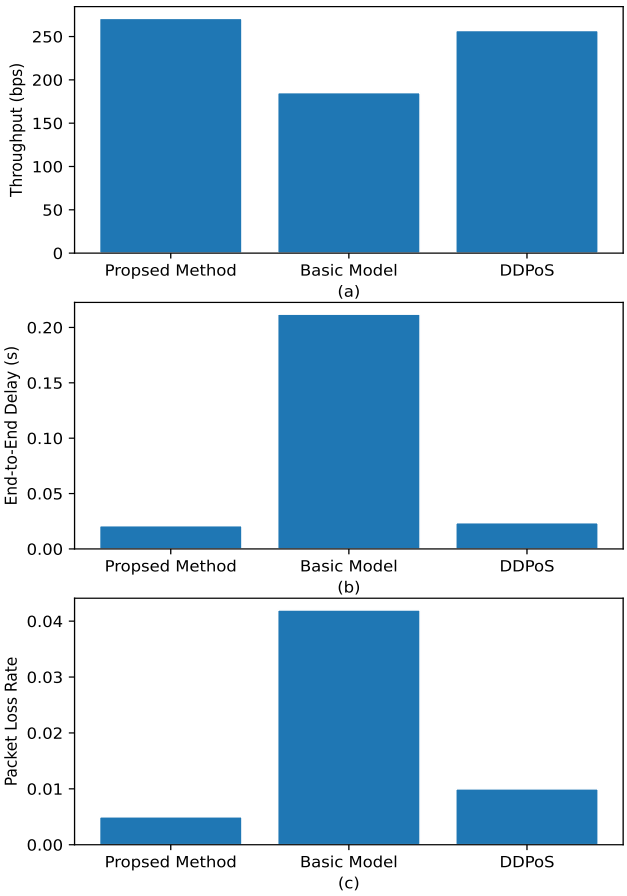

Fig. 6. Comparison of network performance. (a) Throughput. (b) End-to-end delay. (c) Packet loss rate.

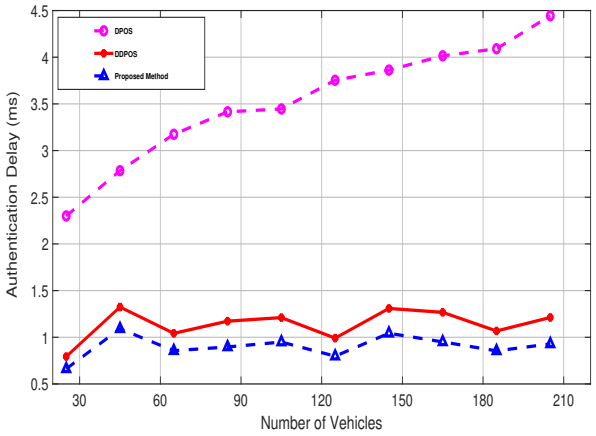

Fig. 7. The effect of the number of vehicles on authentication delay.

bandwidth consumption rises with the block size increase from 1 to 5 MB. This parameter directly impacts bandwidth in the proposed architecture. Additionally, Fig. 8 (b) shows that increasing the number of miners from 10 to 100 and the block size from 1 to 5 MB in all vehicle zones leads to an increase in throughput of the proposed method. More miners hasten the consensus among controllers. Also, a larger block size allows for processing more transactions per block, increasing the throughput rate.

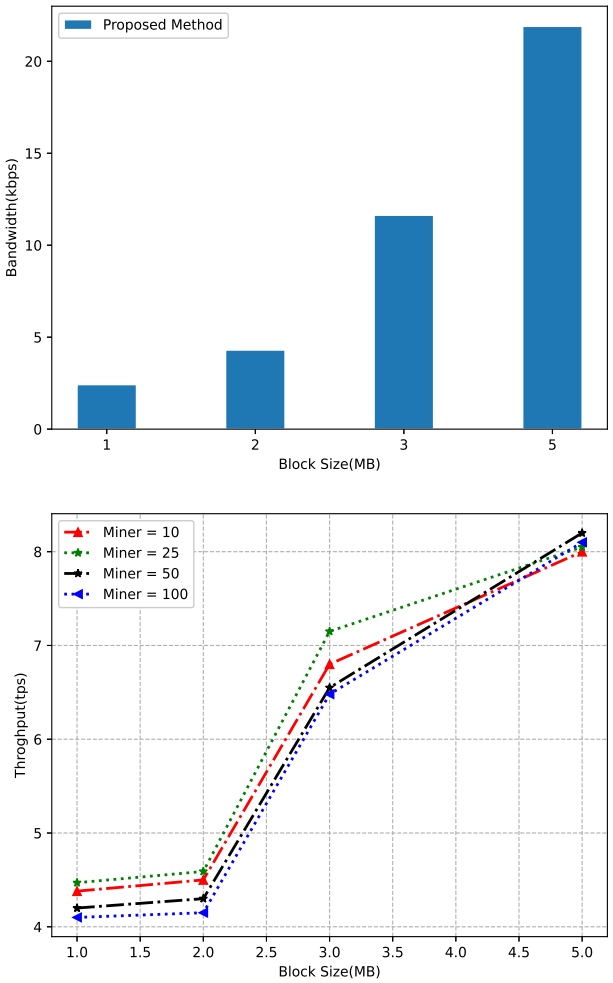

Fig. 8. Impact of blockchain on the proposed method.

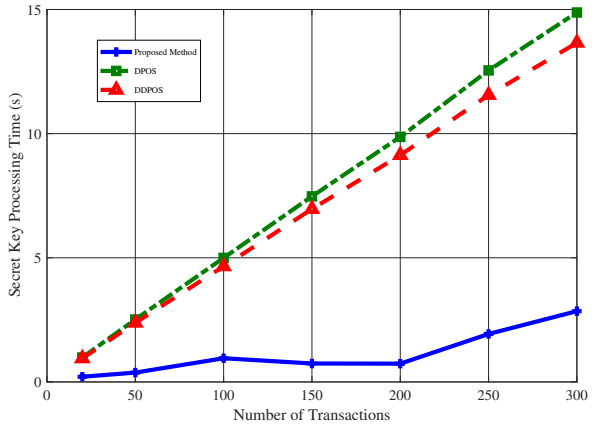

Fig. 9. Key processing time vs the number of transactions.

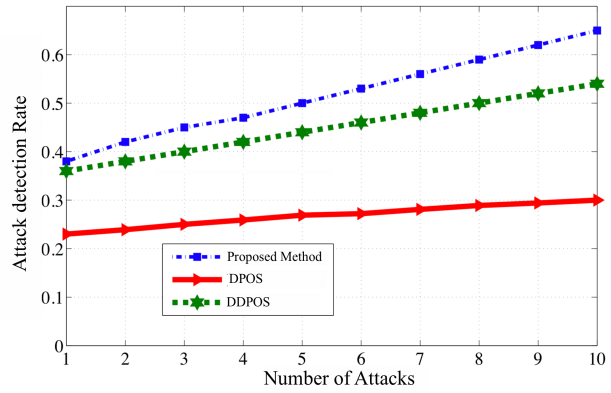

Fig. 10. Attack detection rate vs the number of attacks.

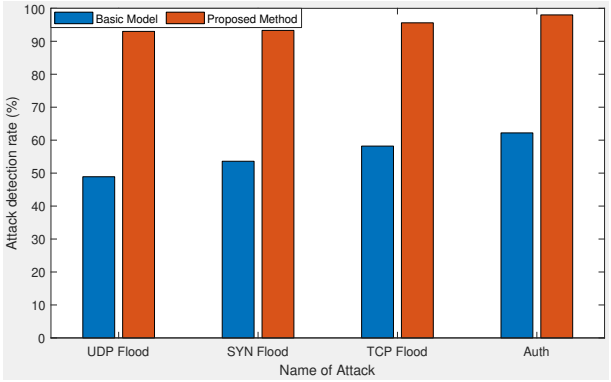

Fig. 11. Attack detection probability.

In our next experiment, we show the key processing time versus the number of transactions as depicted in Fig. 9. Furthermore, the key processing time is compared among our proposed method, DPOS [25], and DDPOS [29]. As observed from Fig. 9, as the number of transactions increases, our proposed algorithm outperforms the existing methods in the key processing time during the movement of vehicles from one zone to another. This is a significant result, as the public and private key transfer time in the key processing time in each zone should be considered during the movement of vehicles from one zone to another. This is because the controller in our proposed method can handle the keys and use a lightweight consensus mechanism for transferring the keys. Additionally, the controller can directly control each zone's public and private keys.

In the final experiment, we evaluated the number of attacks and the effectiveness of our proposed algorithm in detecting them, as shown in Fig. 10. This work focused on denial-of-service (DoS) attacks, but future research can explore other types of attacks. We simulated five zones with 150 authentic vehicles and 50 non-authentic vehicles that could enter the zones with fake IDs and launch DoS attacks. Fig. 10 shows that the DPOS algorithm had a lower attack detection rate due to the need for re-authentication of vehicles. In contrast, our proposed DDPOS algorithm had a better detection rate

as the number of attacks increased, as it does not require re-authentication when vehicles move between zones. The simulation results verify that that our proposed method outperforms both DPOS and DDPOS. In addition, as shown in Fig. 11, our proposed method also performed better than the basic model in detecting different types of DoS attacks, such as SYN/UDP/TCP Flood and the authentication attack (AUTH) that can occur when a vehicle attempts to join a zone [30]. This attack is characterized by a large number of transactions being sent to block actual transactions from being processed. It is important to note that as the number of attacks increases, the attack detection rate must also increase.

It is worth mentioning that there are still many limitations to be discussed.

1) *51% Attacks*: 51% of the attacks pose a significant threat to the blockchain network, and 51% of attackers will have enough computational power to exclude or tamper with transactions deliberately. For shared blockchain networks based on the proof-of-work mechanism, it is challenging to prevent 51% attacks. Therefore, our proposed architecture must ensure sufficient zones. Otherwise, the cost of attacks will be significantly reduced.
2) *Vehicle Speed*: In real-world applications, vehicles' speed must be considered. High-speed movement of vehicles can negatively impact the IoV architecture, affecting wireless communication efficiency and mobility. In our simulation experiments for the proposed architecture, we assumed a transmission distance of 500 m and a vehicle speed of 10 m/s. For faster mobility, issues related to the stability of wireless links and the verification and migration process may arise.
3) *Security Issues*: As the IoV technology progresses, the forms and methods of attacking it also become more varied. Therefore, attack detection and defense methods must be specifically targeted to keep pace with these developments. Our simulation experiment only studied popular DoS attacks, such as SYN/UDP/TCP and authentication attacks. In real-world applications, more defense methods against various attacks must be considered.

VIII. Conclusion

In this work, we proposed an efficient vehicle-based secure blockchain consensus (VBSBC) algorithm to overcome the security and effectiveness of the gigantic data on the Internet of vehicles (IoV). Our proposed system operates in a decentralized manner, enhancing security and avoiding the drawbacks of centralization, such as high costs and delays. Security is a critical aspect of the IoV, and the VBSBC algorithm leverages blockchain technology to ensure secure communication among vehicles. The simulation results showed that our proposed VBSBC algorithm outperformed existing state-of-the-art algorithms regarding authentication delay, key processing time, and attack detection rate. However, the uncontrolled distribution of vehicles could impact the accuracy of the consensus mechanism if there are too few vehicles in a given area. This limitation of our proposed system will be considered in future studies.

Acknowledgement

This work is supported by the Beijing Natural Science Foundation (No. 4212015).

References

[1] L. D. Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet of Things J.*, vol. 8, no. 13, pp. 10452-10473, Jul. 2021.
[2] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Trans. Industr. Inform.*, vol. 17, no. 11, pp. 7669-7678, Nov. 2021.
[3] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, and M. Shinoy, "Blockchain for the Internet of vehicles: How to use blockchain to secure vehicle-to-everything (V2X) communication and payment ?," *IEEE Sens. J.,* vol. 21, no. 14, pp. 15807-15823, Jul. 2021.
[4] B. Ji *et al.,* "Survey on the Internet of vehicles: Network architectures and applications," *IEEE Commun. Mag.*, vol. 4, no. 1, pp. 34-41, Mar. 2020.
[5] M. Waqas *et al.*, "A comprehensive survey on mobility-aware D2D communications: Principles, practice and challenges," *IEEE Commun. Surv. Tuts.*, vol. 22, no. 3, pp. 1863-1886, 3rd Quart. 2020.
[6] T. Limbasiya, D. Das, and S. K. Das, "MComIoV: Secure and energy-efficient message communication protocols for the Internet of vehicles," *IEEE/ACM Trans. Netw.*, vol. 29, no. 3, pp. 1349-1361, Jun. 2021.
[7] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 2, pp. 1054-1079, 2nd Quart. 2017.
[8] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Privacy-preserving smart parking system using blockchain and private information retrieval," in *Proc. Int. Conf. Smart Appl. Commun. Netw.,* (Sharm El Sheikh, Egypt), Dec. 2019, pp. 1–6.
[9] T. Xiao *et al.*, "Smart-contract-based economical platooning in blockchain-enabled urban Internet of vehicles," *IEEE Trans. Industr. Inform.*, vol. 16, no. 6, pp. 4122–4133, Jun. 2020.
[10] Y. Chen, X. Hao, W. Ren, and Y. Ren, "Traceable and authenticated key negotiations via blockchain for vehicular communications," *Mobile Inf. Syst.*, vol. 2019, Art. no. 5627497, pp. 1–10, Dec. 2019.
[11] S. Tu *et al.*, "Security in fog computing: A novel technique to tackle an impersonation attack," *IEEE Access*, vol. 6, pp. 74993-75001, Dec. 2018.
[12] M. Waqas, Y. Niu, M. Ahmed, Y. Li, D. Jin, and Z. Han, "Mobility-aware fog computing in dynamic environments: Understandings and implementation," *IEEE Access*, vol. 7, pp. 38867-38879, Nov. 2018.
[13] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the Internet of vehicles," *IEEE Trans. Intell. Transp. Syst.,* vol. 22, no. 7, pp. 3997-4004, Jul. 2021.
[14] M. Kamal, M. Tariq, G. Srivastava, and L. Malina, "Optimized security algorithms for intelligent and autonomous vehicular transportation systems," *IEEE Trans. Intell. Transp. Syst.,* early access, Nov. 2021.
[15] H. Chai, S. Leng, K. Zhang, and S. Mao, "Proof-of-reputation based-consortium blockchain for trust resource sharing in Internet of vehicles," *IEEE Access*, vol. 7, pp. 175744–175757, Dec. 2019.
[16] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *Proc. 21st Conf. of Open Innovations Assoc. (FRUCT),* (Helsinki, Finland), Nov. 2017, pp. 321–329.
[17] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Industr. Inform.*, vol. 15, no. 6, pp. 3680-3689, Jun. 2019.
[18] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11169-11185, Nov. 2019.
[19] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in Internet of vehicles with blockchain," *IEEE Internet of Things J.*, vol. 7, no. 12, pp. 11815-11829, Dec. 2020.
[20] A. E. Gencer, S. Basu, I. Eyal, R. Van Renesse, and E. G. Sirer, "Decentralization in Bitcoin and Ethereum networks," in *Proc. Financial Cryptography Data Security Conf.,* (Berlin, Heidelberg), Dec. 2018, pp. 439-457.
[21] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, "Bloxroute: A scalable trustless blockchain distribution network whitepaper v1.0," Bloxroute Labs, Evanston, IL, USA, Whitepaper, Mar. 2018.
[22] X. Wang *et al.*, "Power maximization technique for generating secret keys by exploiting physical layer security in wireless communication", *IET Commun.*, vol. 14, no. 5, pp. 872-879, Mar. 2020.

[23] M. Waqas *et al.*, "Authentication of vehicles and road side units in intelligent transportation system," *Comput. Mater. Contin.*, vol. 64, no. 1, pp. 359-371, May 2020.

[24] S. Tu *et al.*, "Reinforcement learning assisted impersonation attack detection in device-to-device communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1474-1479, Feb. 2021.

[25] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1120-1132, Apr.-Jun. 2021.

[26] S. Tu, M. Waqas, F. Huang, G. Abbas, and Z. H. Abbas, "A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing," *Comput. Netw.*, vol. 195, Art. no. 108196, Aug. 2021.

[27] A. Yazdinejad *et al.*, "SLPOW: Secure and low latency proof of work protocol for blockchain in green IoT networks," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC2020-Spring)*, (Antwerp, Belgium), May 2020, pp. 1–5.

[28] S. Tu *et al.*, "Security in fog computing: A novel technique to tackle an impersonation attack," *IEEE Access*, vol. 6, pp. 74993-75001, Dec. 2018.

[29] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of things with decentralized blockchain-based security," *IEEE Internet of Things J.*, vol. 8, no. 8, pp. 6406-6415, Apr. 2021.

[30] C. Lyu, X. Zhang, Z. Liu, and C. -H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of things against DoS attacks," *IEEE Access*, vol. 7, pp. 31068-31082, Mar. 2019.

SHANSHAN TU received his PhD degree from the Computer Science Department at Beijing University of Posts and Telecommunications in 2014. From 2013 to 2014, he visited the University of Essex for National Joint Doctoral Training. He worked in the Department of Electronic Engineering at Tsinghua University as a postdoctoral from 2014 to 2016. He is currently an Associate Professor in the Faculty of Information Technology at Beijing University of Technology, China. His research interests are in cloud computing and information security techniques.

Haoyu Yu received the B.E degree in Internet of Things from Shandong University of Science and Technology, Tsingtao, China, in 2020. He is currently pursuing the M.E degree in Computer Science from Beijing University of Technology, Beijing, China. His research interests include Internet of vehicles security and Blockchain.

Akhtar Badshah received PhD degree with the Faculty of Computer Science and Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Pakistan. Currently, he is a Lecturer with the Department of Software Engineering, University of Science and Technology, Bannu, Pakistan. Since 2014, he has been with the Department of Software Engineering, University of Malakand, Pakistan, as a Lecturer. His research interests include cryptography, blockchain, and IoT security.

MUHAMMAD WAQAS (Senior Member, IEEE) received his PhD degree with the Department of Electronic Engineering, Tsinghua University, Beijing, China in 2019. From Oct. 2019 to Sept. 2021, he was a Research Associate at the Faculty of Information Technology, Beijing University of Technology, Beijing, China. Currently, he is an Assistant Professor at the Computer Engineering Department, College of Information Technology, University of Bahrain, Bahrain. He is also an Adjunct Senior Lecturer at the School of Engineering, Edith Cowan University, Australia. He has more than 100 research publications in reputed Journals and Conferences. He is an Associate Editor of the International Journal of Computing and Digital Systems. His current research interests are in the areas of Wireless Communication, vehicular networks, Fog/Mobile Edge Computing, Internet of Things and Machine Learning. He is recognised as a Global Talent in the area of Wireless Communications by UK Research and Innovation and Professional Member of Engineer Australia.

Zahid Halim (Senior Member, IEEE) received the B.S. degree (Hons.) in computer science from the University of Peshawar, Peshawar, Pakistan, in 2004, and the M.S. and PhD degrees in computer science from the National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2007 and 2010, respectively. From 2007 to 2010, he was a Faculty Member (Lecturer and then Assistant Professor) at the National University of Computer and Emerging Sciences.

He is currently a Professor at the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Pakistan. His current research interests include machine learning and data mining, probabilistic/uncertain data mining, and human factors in computing. Dr. Halim is a member of the IEEE Computational Intelligence Society. He is a recipient of the prestigious Research Productively Award-2017 from the Pakistan Council of Science and Technology. He has also received the 6th HEC Outstanding Research Award 2015-2016 in the best research paper category. For his academic performance in 2016, he received the HEC Best University Teacher Award (BUTA)-2016.

Iftekhar Ahmad (Senior Member, IEEE) received the Ph.D. degree in communication networks from Monash University, Australia, in 2007. He is currently an Associate Professor with the School of Engineering, Edith Cowan University, Australia. His research interests include 5G technologies, green communications, QoS in communication networks, software-defined radio, wireless sensor networks, and computational intelligence.