IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 June 2024, accepted 12 July 2024, date of publication 15 July 2024, date of current version 26 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3428830

RESEARCH ARTICLE

D-BlockAuth: An Authentication Scheme-Based Dual Blockchain for 5G-Assisted Vehicular Fog Computing

HUSSAM DHEAA KAMEL AL-JANABI[1], SAIMA ANWAR LASHARI[2], AYMAN KHALIL[3], MAHMOOD A. AL-SHAREEDA[4], ABEER ABDULLAH ALSADHAN[5], MOHAMMED AMIN ALMAIAH[6], AND TAYSEER ALKHDOUR[7]

[1]Department of Computer Technical Engineering, Al-Mustafa University College, Baghdad 10068, Iraq
[2]College of Computing and Informatics, Saudi Electronic University, Riyadh 11588, Saudi Arabia
[3]Adnan Kassar School of Business, Lebanese American University, Beirut 1102 2801, Lebanon
[4]Department of Communication Engineering, Iraq University College (IUC), Basrah 61001, Iraq
[5]Department of Computer Science, Applied College, Imam Abdulrahman Bin Faisal University, Dammam 31451, Saudi Arabia
[6]King Abdullah II School of Information Technology, Department of Computer Science, The University of Jordan, Amman 11942, Jordan
[7]Department of Computer Networks, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

Corresponding author: Mahmood A. Al-Shareeda (m.alshareeda@iuc.edu.iq)

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Grant Kfu241047.

ABSTRACT Vehicular fog computing (VFC) is a developing concept that utilizes the ideas of fog computing to facilitate immediate communication and cooperative decision-making among vehicles. However, guaranteeing safe authentication in VFC presents notable difficulties as a result of characteristics such as dynamic network topology, extensive mobility, and limitations on resources. This paper introduces D-BlockAuth, an innovative authentication mechanism for 5G-assisted VFC that utilizes a dual blockchain approach. To reach the most vehicles, this link makes use of all the features of the fifth-generation base station (5G-BS). D-BlockAuth employs two blockchains: a permissioned blockchain to handle long-term identities and a consortium blockchain to enable streamlined and effective authentication at the fog layer. The D-BlockAuth concept incorporates advanced cryptographic techniques such as ring signatures and group signatures, which provide improved privacy and anonymity for vehicles within the network. The study provides a comprehensive description of the architecture of D-BlockAuth, examines its security characteristics, and assesses its performance using simulations. The results indicate that D-BlockAuth successfully performs both efficient and safe authentication in VFC, while also maintaining user privacy.

INDEX TERMS Vehicular fog computing, dual blockchain, authentication, security, privacy.

I. INTRODUCTION

Vehicular Fog Computing (VFC) has the potential to bring about a significant transformation in intelligent transportation systems [1], [2], [3]. VFC utilizes fog computing principles to expand cloud-based services to automobiles, facilitating the implementation of real-time applications such as traffic management, collision prevention, and cooperative driving [4], [5], [6], [7]. Nevertheless, this interlinked ecosystem presents novel security obstacles. An essential issue is to guarantee secure and dependable authentication between automobiles and fog nodes [8], [9].

Conventional authentication methods frequently encounter restrictions in VFC because of variables such as limited resources on vehicles and the dynamic topology of vehicular networks. Centralized designs that utilize Public Key Infrastructure (PKI) have the potential to cause bottlenecks and generate vulnerabilities due to the presence of single points of failure [10], [11]. Current blockchain technologies provide enhancements but may face challenges in terms of

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed M. A. Moustafa.

scalability and latency, which are critical factors for real-time applications in VFC [12], [13].

Industry and academia have been working on 5th Generation (5G) communication to solve the problems with previous communication technologies and satisfy the increasing needs for secure, low-latency, and high-bandwidth applications, among other game-changing technologies created in the last two decades [14]. Vehicular Ad Hoc Networks (VANETs) are a special type of mobile ad hoc network, in which vehicles communicate not only with each other but also with roadside infrastructure. Within this framework, VANET may make use of 5G's unique characteristics in conjunction with cloud computing to manage the massive amounts of data produced by vehicle nodes via vehicular clouds [15]. To further expand the application area of both VANET and IoT, the merging of the two has also been considered and studied. The performance and security needs of VANET applications and services are distinct from those of DSRC or cellular (3G and LTE/-A) on their own. To maintain a secure, flexible, and QoS-enabled communication architecture, VANET should use 5G communication technology.

Intelligent mobility provided by VFC presents promising opportunities, but it also brings about new security weaknesses due to its decentralized structure and dependence on wireless connection. Below is an analysis of several prevalent security exploits in VFC: Impersonation attacks involve the act of attackers assuming the identity of genuine vehicles or fog nodes to illicitly gain entry into the network. This can entail the participation of counterfeit fog nodes disseminating deceptive information or manipulated vehicles injecting malevolent data [16], [17]. Data Manipulation Attacks involve the deliberate tampering of data that is being shared between vehicles and fog nodes by malicious individuals. This may entail intercepting and altering traffic data, resulting in disturbances such as the transmission of incorrect instructions or the occurrence of accidents [18], [19]. These are a few of the security risks encountered by VFC. Ensuring the implementation of strong authentication, authorization, and encryption procedures, as well as intrusion detection and prevention systems, is essential for securing VFC settings.

This paper introduces D-BlockAuth, an innovative authentication technique that utilizes a dual blockchain architecture for VFC. D-BlockAuth overcomes the constraints of current methods by (i) Utilizing Dual Blockchain: The system employs two blockchains: a lightweight blockchain on fog nodes for efficient and rapid authentication, and a public blockchain for secure record-keeping and resolving disputes. (ii) D-BlockAuth uses cryptographic techniques to mitigate impersonation attacks, which involve malicious actors trying to impersonate genuine cars or fog nodes. (iii) The dual blockchain concept enhances scalability and performance by efficiently authenticating within the fog while preserving the immutability and security advantages of blockchain technology.

Thus, the main contribution of this paper is listed as follows.

- We proposed the D-BlockAuth scheme which is a dual blockchain-based authentication strategy designed for vehicular fog computing. It provides a reliable method for ensuring secure communication inside this network.
- We conduct integration with fog services which is a study on the smooth integration of D-BlockAuth with different fog services provided in vehicle fog computing. This may entail expanding the system to verify and grant access to fog-based resources such as real-time traffic data or collaborative mapping applications.
- We examine security analysis which the scalability of D-BlockAuth as the number of vehicles and fog nodes grows in the network. Suggest remedies to maintain the efficiency of the system while the network expands.
- We explore methods of performance evaluation to enhance the computational efficiency of D-BlockAuth. This is essential for fog nodes and vehicles that have limited resources. We will explore an efficient authentication scheme by utilizing lightweight cryptographic algorithms and effective blockchain implementation techniques and optimize the scalability and performance of the proposed authentication scheme. This paper examines the computational overhead, throughput, storage, transmission latency, and verification rate of the proposed D-BlockAuth scheme.

The rest of this paper is organized as follows. Section II presents a review of the literature on Vehicular Fog Computing (VFC). Section III provides the system model and security attacks. Section IV proposes phases of the D-BlockAuth scheme. Section V provides security analysis and comparison. Section VI evaluates the performance evaluation. The conclusion and future work of the D-BlockAuth scheme are described in Section VII.

II. LITERATURE REVIEW

A. SECURITY AND PRIVACY FOR 5G-BASED VFC

Soleymani et al. [20] established a trust model, an authentication system for nodes and messages that preserves privacy. For vehicle nodes, the proposed node authentication checks their legitimacy, while for messages, the goal of message authentication is to guarantee their authenticity.

Xu et al. [21] presented LPPA-RCM, an authentication strategy for road condition monitoring that uses a lightweight equality test on ciphertexts to preserve privacy.

An authentication system that maintains user privacy by integrating 5G and edge computing is suggested by Zhang et al. [22], based on the existing framework's functional characteristics of inter-vehicle communication networks. Utilizing device-to-device technology, their suggested framework departs from the prior art of 802.11p-based inter-vehicle communication network design.

Edge nodes are responsible for message classification and verification in the suggested approach by Zhong et al. [23].

Additionally, to achieve local upload and download of video reports and to avoid storage of repetitive accident reports in the cloud, these nodes relay the first report message they receive about the same accident to the designated official cars.

As part of the handover process, Dewanta and Mambo [24] presented a secure and lightweight mutual authentication technique that takes into account limited-access FCS in vehicular network environments and service reservation scenarios during the login and service request phases.

Xu et al. [25] offered a lightweight privacy-preserving traffic condition monitoring (L-TCM) system, where the vehicle can broadcast safety-related messages and upload traffic condition messages with a single message thanks to the sanitizable signature.

For smart urban vehicle mobility, Farooqi et al. [26] created a fog computing model that prioritizes tasks to decrease fog computing latency and delay.

Using message authentication codes and Grain stream cipher, Cui et al. [27] suggested a lightweight authentication and encryption technique for the CAN bus of AVs. Efficient authentication between electronic control units is achieved by the system, and authentication failure due to counter inconsistency is addressed by using a re-synchronization protocol.

A safe and privacy-protecting authentication method is presented by Goudarzi et al. [28]. Elliptic Curve Cryptography (ECC) is used for message authentication in the proposed technique, whereas Quotient Filter (QF) is utilized for node authentication. Using techniques like as fuzzy verifiers and honeywords, Cui et al. [29] provided a UAV-assisted VANET two-factor AKA system that is practical, lightweight, and provably safe. The approach is built on chaotic maps.

B. AUTHENTICATION-BASED BLOCKCHAIN FOR VFC

Chen et al. [30] applied deep learning, blockchain, and fully homomorphic encryption (FHE) technologies, and they suggest a Decentralized Privacy-preserving Deep Learning (DPDL) model. Computing workloads are decentralized from centralized cloud services to edge computing (EC) nodes in their proposed Decentralized VANETs (DVANETs) architecture, which efficiently reduces network communication costs and congestion delay. To ensure safe and reliable data transfer between cars, roadside devices, and EC nodes, they employed blockchain technology.

Wang et al. [31] presented a deep learning-based verification model that can determine the reliability of uploaded messages, determine the credibility scores of vehicles based on these scores, and identify malicious vehicles based on them. The goal is to stop malicious vehicles from uploading false messages.

For trust management (FBTM) in the IoV, Haddaji et al. [32] suggested federated learning using a blockchain approach. Therefore, to enhance the data gathered for the learning process of the federated learning model, a vehicular trust evaluation is built. To further ensure the storage and sharing of global federated learning models, a unique reputation system based on blockchain is being built.

TABLE 1. Many threats addressed by current and D-BlockAuth schemes.

Threats	[30]	[31]	[32]	[33]	D-BlockAuth
Replay	✓	✓	✓	✓	✓
Non-repudiation	✗	✗	✓	✗	✓
Modification	✓	✗	✗	✓	✓
Impersonation	✓	✓	✗	✓	✓

Zhang et al. [33] provided an indirect reputation-based reciprocal incentive mechanism to encourage OBUs in the VANET to aid each other, which will decrease the number of attackers in the vehicle ad hoc network and limit the attack motivation of the OBUs.

C. CRITICAL ANALYSIS

We analyze to what extent existing security protocols for vehicular networks can handle the set of threats discussed in Table 1. These schemes include DVANET (decentralized deep learning model for vehicular ad hoc network) [30], BDLV (blockchain and deep learning based scheme for vehicular ad hoc network) [31], FBTM (Federated learning with blockchain for trust management) [32], DDQN (double deep Q-network) [33], and among others. Although those schemes have provided limited coverage over replay, non-repudiation, modification, and impersonation attacks. For example, although the Schemes Chen et al. [30] and Wang et al. [31] resolve the replay and impersonation attacks adequately, they do not support non-repudiation, which can lead to disputes over operations or transactions in the network. Another issue is, modification attack prevention capabilities were not taken into consideration in some of the works such as the absence in Wang et al. [31] and Zhang et al. [33]. D-BlockAuth promotes the field substantially as it bridges those gaps to include effective counter-measures against all diagnosed threats, every single one making sure a complete security framework D-BlockAuth comes with heightened cryptographic measures designed around dual blockchain technology that prevents unauthorized data tampering or fudging and takes a step further towards achieving non-repudiation by generating an evidential trail of all transactions. What is more, the novel design of SCRC can resist replay attacks and impersonation attacks well, which can offer safe and reliable communication for vehicular networks. Such critical evaluation emphasizes the inevitability of fully noted security solutions such as D-BlockAuth which can prevent all threat flaws, thus increasing trust practically and more realistically in vehicular communication systems.

III. PRELIMINARIES

A. DESIGN MODEL

This section describes the proposed D-BlockAuth system architecture. The document is additionally subdivided into two sub-sections, each addressing the registration and authentication procedure, and the message transmission and communication process, respectively. The primary physical components of the system architecture include vehicles, onboard units (OBUs), fog servers, and various sensors such as cameras, GPS modules, and infrared (IR) sensors. The following information is provided in summary:

- Vehicles: Vehicles are the fundamental and crucial entities of a VANET. Vehicles in VANETs are mobile devices. The On-board Unit (OBU) and numerous other sensors are installed on them. Vehicles are the primary source of data within the network.
- On-board Unit (OBU): This device is located within the car and serves the purpose of establishing communication with other vehicles and fog servers in the network. OBU utilizes communication protocols such as 3G, 4G, 5G, and 6G to establish connectivity with other sensors and vehicles. Additionally, OBUs consume less electricity to ensure the efficient operation of vehicles in the network.
- Fog servers: A fog server is a sensor mostly positioned adjacent to roadways to gather data. Every RSU has a well-defined operational territory.
- Other sensors: The sensors, such as GPS modules and IR sensors, are responsible for detecting and recording any action occurring within the VANET.

B. SECURITY ATTACKS

- Replay Attacks: Replay attacks occur when an adversary intercepts valid data transmissions between cars or between cars and fog servers, stores it for later use, and then retransmits it. Vehicle security and safety on the road could be severely compromised as a result of this.
- Non-Repudiation: Non-repudiation is essential for VFC due to the constant flow of data between vehicles and fog nodes for reasons like traffic management, accident avoidance systems, and collaborative sensing. In the absence of it, malevolent individuals could falsify data or evade accountability for their activities, resulting in potential safety risks or impeding the proper functioning of the system.
- Modification Attacks: Modification attacks in vehicular fog computing seek to manipulate data that is communicated or stored within the system. This compromises the integrity of the data and has the potential to result in erroneous conclusions or potentially hazardous circumstances.
- Impersonation Attacks: In the realm of automotive fog computing, an impersonation attack is an act of malevolent intent in which an attacker assumes the identity of a genuine user or fog node within the network. The act of impersonating others can result in a range of security problems, underscoring the significance of having strong detection systems in place for vehicular fog computing.

TABLE 2. Notation used on their definition.

Notation	Definition
TA	Trusted Authority
E-Block and B-Block	Enrollment blockchain and broadcasting blockchain
MT	Message Transmission
Pub_x and Pri_x	Public key and a private key
VLD	Vehicle Location Database
V_{Req}	Vehicle enrollment request ID
V_{ID} and S_{Fog}	Vehicle ID and session ID
V_{age}	Age of the vehicle
P_{sen}	Pool of sensors
T	The current timestamp
F_{area}	Fog server territory
GM and EM	General messages and emergency messages
Pos	Position
$info$	The actual information
$Cert_{enr}$	Enrollment certificate

Algorithm 1 The Proposed D-BLockAuth Registration and Message Transmission

```
while $V_i$ wishes to exchange data do
    $V_i$ transmits a transaction request to the Fog server;
    $T_{info}(T, EM/GM, Pos, info) \rightarrow$ Fog server
    if $V_i$==Authenticated then
        Fog server discloses the position of $V_i$ from VLD as Proof of Presence (PoP);
    else if $V_i$ is within the $F_{area}$ then
        Fog server mines $T_{info}$
        Fog server inserts $T_{info}$ to the B-Block;
        Fog server sends the $T_{info}$ along with the $Pub_k$ of $V_i$ to other vehicles;
    else if Message==$EM$ then
        Remove $GM$ from $B-block$ after defined period;
    end if
    if Message==$GM$ then
        Remove $GM$ from $B-block$ after defined period;
    end if
    $V_i$ obtains enrolled with fog server;
    Fog server authenticates the $V_i$ and assigns $Pub_x$, $Pri_x$ key pair;
    Fog server utilises the $Pub_x$ of $V_i$ and adds it to the $E-Block$;
end while
```

IV. THE PROPOSED D-BLOCKAUTH SCHEME

This section proposes D-BlockAuth, an innovative authentication mechanism for VFC that utilizes a dual blockchain approach. The proposed D-BlockAuth employs two blockchains: a permissioned blockchain to handle long-term identities and a consortium blockchain to enable streamlined and effective authentication at the fog layer. The main phases of the proposed D-BlockAuth scheme are enrollment, authentication, and message broadcasting phases. Table 2 shows the notation used in their definition. Algorithm 1 shows steps of the proposed D-BLockAuth registration and message transmission in detail.

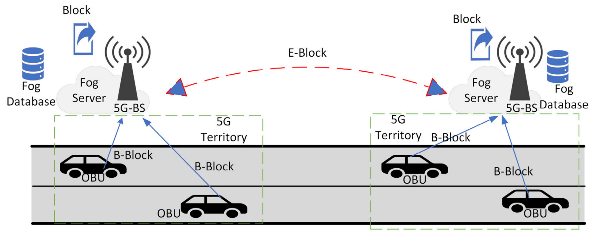


FIGURE 1. Proposed D-BlockAuth scheme for VFC.

A. ENROLLMENT PHASE

Two different blockchains are utilized by the proposed D-BlockAuth scheme that has been suggested. One blockchain, which is referred to as the enrollment blockchain (E-Block), is utilized to store information regarding the vehicles' registrations. This blockchain is administered by Trusted Authority (TA), and it is maintained by all of the fog servers that are part of the network. Both the storing of messages and the management of message transmission (MT) are the responsibilities of the second blockchain. This blockchain is referred to as the broadcasting blockchain (B-Block), and it is administered by a fog server across the communication range of the 5G-base station (BS), which is connected to the E-Block. Figure 1 is a representation of the entire proposed D-BlockAuth scheme for VFC that has been proposed. All of the cars that are interested in being a part of the network are required to register with the fog server by going through a covered area that is provided by 5G-BS. After that, the fog server will generate a public key (Pub_x) and a private key (Pri_x) pair for the car, and then it will assign those keys to the vehicle. For as long as it is a part of the network, the car will utilize its RSA public key as its identification. The public key serves as an anonymity-identity for the vehicle in question. When the vehicles are connected to the network, this ensures that their privacy is protected at all times. Additionally, the E-Block is where the XML files are stored, and they are shared among all of the fog servers and their B-Block. Additionally, each fog server is responsible for the upkeep of a vehicle location database (also known as VLD). This database is utilized to monitor and record the location of any vehicle that is within the communication range of 5G-BS. This is because fog servers have their own designated territories in which they function. To prevent an excessive amount of operational overhead, this database is updated on a relatively regular basis but is not included on the blockchain.

B. AUTHENTICATION PHASE

If a new vehicle wishes to join the network, the initial action that it takes is to generate a vehicle enrollment request ID (also known as a V_{Req}), as shown in Equation (1). This request ID includes the fundamental information that pertains to the vehicle, such as the vehicle ID (V_{ID}), the age of the vehicle (V_{age}), and the pool of sensors (P_{sen}) that are present in the car. The vehicle transmits this message to the closest fog server within its communication range, which is typically 300 meters, facilitated by the 5G-BS.

$$V_{Req} = (V_{ID}, V_{age}, P_{sen}) \tag{1}$$

Following the receipt of the request, the fog server conducts a verification of the legitimacy of the vehicle that is being requested. When it comes to being a part of the network, the car must not be more than ten years old and must be equipped with all of the necessary sensors. To enroll the vehicle onto the network, the fog server will generate a one-of-a-kind session ID (S_{Fog}) if there are prerequisites that are met, as shown in Equation (2). Every S_{Fog} that is enrolling the current vehicle includes the ID of the fog server (ID_{Fog}) that is enrolling the vehicle, the current timestamp (T), and the V_{Req}. The use of a hash function ensures the safety of the cipher.

$$S_{Fog} = h(V_{Req}, T, ID_{Fog}) \tag{2}$$

During the process of creating the session, the fog server is also responsible for doing the following activities simultaneously: It is necessary to assign a Pub_x and a Pri_x to the vehicle. It is necessary to encrypt the vehicle identification number (VIN) because it serves as the car's anonymity ID. Additionally, an enrollment certificate ($Cert_{enr}$) should be issued to the vehicle. The car is added to the VLD by the fog server, which also distributes the data associated with the vehicle with other reliable fog servers that are within its range. as shown in Equation (3).

$$\left\{ID_{Fog}, T, Pub_x, Cert_{enr}, S_{Fog}, ID_{Fog}\right\} \tag{3}$$

A proof-of-authority (PoA) consensus is utilized by the $E-Block$ blockchain, which is administered by the TA. Every fog server is connected to it as a member node to facilitate the exchange of information on vehicle enrollment. Because of this, every fog server has access to every piece of information on the vehicle. A request for temporary message services can be sent to the fog server by any vehicle that is traveling through the territory of another fog server. The fog server will conduct a search operation within the $E - Block$ to validate the information on the registration of the vehicle node that is stopping by. The fog server notifies the $B-Block$ to take into consideration that vehicle as a member and a potential sender and recipient of messages when the $E - Block$ approves the information. To guarantee that the vehicles are present in a specific fifth-generation base station (5G-BS) zone, a PoP consensus is implemented. It is the responsibility of the fog server to keep track of the present location of every vehicle. The cars continue to transmit their current location as a PoP and consistently update their current location. In this manner, the $B-Block$ is up to date consistently, and the messages are only transmitted to the cars that are currently taking part in the particular $B-Block$ and are located within the fog server territory (F_{area}).

C. MESSAGE BROADCASTING PHASE

To converse and send messages within the network, only vehicles that have been registered and authenticated are permitted to do so. Not only should the communications that are being transmitted be protected and secured, but the network itself should also be protected and secured. On the other hand, only a fraction of the messages that are being passed around within the network are significant. Data such as information about accidents, thefts, extreme traffic overload, and other similar subjects may be included in these alerts. To prevent similar occurrences from occurring again in the future, this data can be employed. For this reason, the blockchain database only stores the most significant communications, while the remaining messages are deleted once a predetermined amount of time has passed. In addition to reducing the amount of storage space that is required, this serves to improve the overall efficiency of the blockchain. It is also important to note that the cars use their public key for communication, which ensures that their privacy is preserved within the network.

The vehicles parked in the $B - Block$ can generate two types of signals. Both "General messages" (GM) and "Emergency messages" (EM) fall under these categories. This includes all of the data housed inside the network as well as information about traffic, accidents, road closures, and similar events. A vehicle's sensor will add the information it has gathered about network activity into a blockchain transaction whenever it detects something. The fog server is responsible for verifying the identity of the vehicle as well as the current location of the vehicle, which is obtained from the VLD. If the car is discovered to be within the vicinity of the radius, which is often established to be 500 meters, it is permitted to generate the transaction. This transaction provides the timestamp (T) at which the information is captured, the message type (GM or EM), the position (Pos), and the actual information ($info$).

Within the F_{area}, the other vehicles receive transmissions from the fog server, which adds the transaction to a block in the blockchain and conducts mining. Figure 2 depicts the stream of data sensing and VFC transactions. The cars keep an eye on things going on around them, such as traffic conditions. When they're on the network, they document these things, turn them into message requests, and send them to the closest fog server as $T_{info}(T, GM/EM, Pos, Info)$. After the fog server certifies the vehicle's validity, it sends a message to the blockchain block as a transaction. When it comes to keeping the blockchain as efficient as possible, only the EM is saved in the database. Any other messages are erased after a certain amount of time.

V. SECURITY ANALYSIS

The suggested D-BlockAuth scheme is assessed in this part according to its security and resistance to different types of attacks.

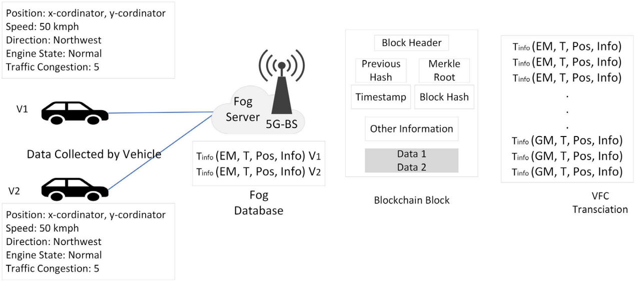


FIGURE 2. **Proposed Transaction of D-BlockAuth Scheme for VFC.**

To keep a blockchain network secure, all cars must agree on the same version of the ledger. The cars can agree on the sequence and inclusion of transactions in the blockchain thanks to consensus procedures. As a result, the consensus mechanism can screen out potentially harmful or fraudulent transactions before they are added to the blockchain.

Two consensus protocols, PoA and PoP, collaborate in the suggested dual blockchain design. The fog servers are a predetermined group of validators α in the PoA consensus. The network relies on these entities. It is the responsibility of these fog servers to validate the β transactions that are produced by a group of OBU in the network. The current state of the $E - Block$ is represented by OBU, and each block in the $E - Block$ has a hash value H_i and a set of validated transactions β_i. A validator α_{i+1} is selected at random from α every time initiates a new transaction. A new block is created with a nonce value $n(n + 1)$ added to its header when α_{i+1} is used. The remaining validators in α are then informed of this. The block β_{i+1} is appended to α once additional validators have confirmed it.

When a vehicle OBU_i wishes to exchange information with the network, it creates a transaction request T_{info} and sends it out into the network using the PoP consensus protocol. This includes the information that has to be communicated, the time stamp, and the location L of the file. The adjacent cars check the accuracy of the prior location data L', the current block hash V, and a random value D to calculate a challenge parameter Ch. As evidence of the challenge, this L_{Ch} is sent out to other OBU_i in the network, and a response T_{info} is received. The direction in which L is orientated about OBU_i is represented by L_{Ch}. Then, all the nodes in the network receive this Ch, and the $B - Block$ gets T_{info}. With each new block that is added to $B - Block$, the challenge parameters are updated.

A. SECURITY THEORETICAL EVIDENCE

D-BlockAuth is powerful against the highlighted risks according to theoretical studies. We completed extensive theory to prove the system can survive replay, non-repudiation, modification, or impersonation attacks, and common vehicular network threats. Each simulated scenario, which matches real-world vehicular network conditions, shows that D-BlockAuth decreases these risks. Theoretical assessments demonstrate the cryptographic resilience of the dual blockchain system, ensuring the protection of private data from unauthorized alterations.

Proposition We propose that the suggested D-BlockAuth scheme is resistant to replay, non-repudiation, modification, and impersonation attacks based on our theoretical analysis and empirical evidence.

B. THE NONCE SAFEGUARDS THE BLOCKCHAIN FROM REPLAY ASSAULTS.

The nonce is stored on the blockchain along with the transaction details. Every transaction is double-checked to make sure the nonce is distinct to deter replay attacks. The transaction is refused because it is not legitimate if the nonce is not unique. Consider two transactions, T^{x1}_{info} and T^{x2}_{info}, that share the same transaction hash. Here, T^{x1}_{info} is the original transaction, and T^{x2}_{info} is a replay of T^{x1}_{info}. In the absence of nonce:

T^{x1}_{info} = valid transaction

T^{x2}_{info} = valid transaction

Nevertheless, the blockchain verifies the uniqueness of the nonce for every transaction through the use of nonce:

$T^{x1}_{info} + n1$ = valid transaction

$T^{x2}_{info} + n1$ = invalid transaction (replay attack)

C. NON-REPUDIATION

Because the technique requires vehicles to connect their T_{info} anytime they generate a Pri_x, it can prevent non-repudiation assaults. The equation $x = \mathrm{H}(T_{info}, Pri_x)$ generates a digital signature. This can be confirmed by other users through the Pub_x as well.

$\mathrm{H}(T_{info}, Pri_x)$ = x (the validation of digital signatures)

$\mathrm{H}(T_{info}, Pub_x)$ = x (Verifying the legitimacy of messages)

The blockchain records both the transaction and the digital signature. The message's legitimacy and the sender's identity can be proven with this immutable record.

D. MODIFICATION

Cryptographic hashes and distributed consensus are used to thwart modification attacks (PoP and PoA). A hash pointer connects each block in the RBC and MBC to the one before it, forming a chain of blocks. If a block were to be modified, its hash would change, which would influence the hash of all blocks that followed it in the chain. The hash of block *Block* will change if an attacker attempts to modify it in the following way:

$$H'(Block + 1) = H(Block(T_{info}))$$

There will be an expiration date on the hash pointer that connects *Block* to the subsequent block ($Block + 1$). To keep the blockchain secure, it is necessary to update the hash of ($Block + 1$) to reflect the change in *Block*'s hash as:

$$H'(Block + 1) = H(H'(Block) + (Block + 1)(T_{info}))$$

In addition, a consensus procedure (PoA for $E - Block$ and PoS for $E - Block$) that necessitates agreement from the majority of network nodes is used to attain a distributed consensus. The consensus mechanism will reject any attempt to alter a block if the hash value does not match the one that the majority of participants have agreed upon.

E. IMPERSONATION

With the addition of a timestamp and other information, each vehicle registered to the $E - Block$ receives a unique pair of Pub_x and Pri_x keys. The authenticity of the signature is confirmed by the Pub_x by utilizing the $E - Block$ of the vehicles.

if Verify-Vehicle(OBU_i, Pub_x) = True: OBU_i = verified.

An identification proof is stored in the $B-Block$ whenever this vehicle conducts a transaction in the network, together with its Pub_x.

$$B - Block.insert(transaction(T_{info}, Pub_x))$$

Therefore, if a malicious actor attempts to impersonate a trusted vehicle, it may be identified by comparing its details with those in the $E - Block$, and if it is not detected, it can be removed from the network.

VI. PERFORMANCE EVALUATION

This subsection examines the computational overhead, throughput, storage, transmission latency, and verification rate of the proposed D-BlockAuth scheme. This paper evaluates and compares the proposed D-BlockAuth scheme and other recent schemes of Chen et al. [30], Wang et al. [31], Haddaji et al. [32] and Zhang et al. [33].

A. SIMULATION SETUP

For implementing and validating our proposed D-BlockAuth model, the OMNeT++ network simulator was employed to simulate extensive experiments. Minimal values that configured the simulation environment to design a realistic vehicular fog computing (VFC) scenario, were:

- Network Topology: There are some works where they model the dynamic network topology similar to the real-world vehicular networks. To account for a range of traffic patterns, the simulation incorporated different types of road layouts, intersections, and highway segments.
- Mobility Model: Simulation-based V2V communication study We used the Simulation of Urban MObility (SUMO) tool to create realistic vehicle mobility patterns. To represent the wide range of realistic mobility, vehicles were endowed with different speeds, routes, and traffic densities.
- Communication Range: Vehicles and fog nodes could communicate at the range of 300 meters to simulate the common VFC communication cases.
- Fog Nodes: Fog nodes were sparsely deployed on the road network to perform efficient data processing and background authentication.

- Traffic Density: The scalability analysis of the D-BlockAuth scheme was performed by the simulation of 300 to 1100 vehicles.
- Resource Limitations: These simulations included computational limitations for system onboard and fog nodes, storage capacity, and bandwidth of the vehicles and the fog nodes.
- Latency Requirement: We targeted an end-to-end latency of under 50ms (necessary for real-time V2V applications in a VFC environment) for networks with up to 1100 vehicles in our simulations.

1) PARAMETERS

- Simulation Duration: All simulations lasted for 3600 seconds to collect enough data to be analyzed.
- Message Frequency: General message (GM) and emergency message (EM) messages were produced by vehicles every second.
- Blockchain Configuration: The main blockchain architecture includes the Enroll Blockchain and the Broadcast Blockchain, which are dual blockchains. The E-Block uses a Proof of Authority (PoA) consensus, while the B-Block uses a lightweight consensus mechanism to improve performance.

2) PERFORMANCE METRICS

The performance of the D-BlockAuth scheme was evaluated based on the following metrics:

- Throughput: Measurable as the throughput, the number of transactions executed per second.
- Transmission Latency: Average duration for messages to be broadcast and validated.
- Storage Requirements: Storage used by the blockchain increased with the number of vehicles - approx.
- Verification Rate: Transactions verified per hour.

B. COMPUTATIONAL OVERHEAD

The time it takes for the vehicle to register and authenticate itself when it initially enters the network is represented by the computational overhead. Included in this is the time required to generate the Pub_x and Pri_x key pair and post the vehicle details to the blockchain.

C. THROUGHPUT

The throughput, which is associated with the $B-Block$, is the maximum number of transactions that can be efficiently communicated per second (T_{info}/sec) with varying numbers of vehicles in the network. We can figure out the throughput by plugging the numbers into this formula.

$$Throughput(T_{info}/sec) = \frac{Size\ of\ Block}{Size\ of\ T_{info}\ Average} \times \frac{1}{Time\ of\ Block} \quad (4)$$

Figure 3 demonstrates the throughput of different authentication schemes (related schemes and proposed D-BlockAuth) as the number of vehicles increases from 100 to 1100. The throughput performance of the D-BlockAuth compared to the existing scheme is significantly higher. With a higher network load, although the throughput of all schemes decreases with the number of vehicles increases, D-BlockAuth keeps a comparatively higher throughput. This is the result of its dual Blockchain processing which separates the authentication processes and doesn't put that weight on a single blockchain, improving the overall efficiency of the network. Increased vehicle density results in a significant drop in D-BlockAuth throughput, where D-BlockAuth maintained a higher throughput under increased vehicle density, illustrating D-BlockAuth scalability and performance in demanding vehicular fog computing environments.

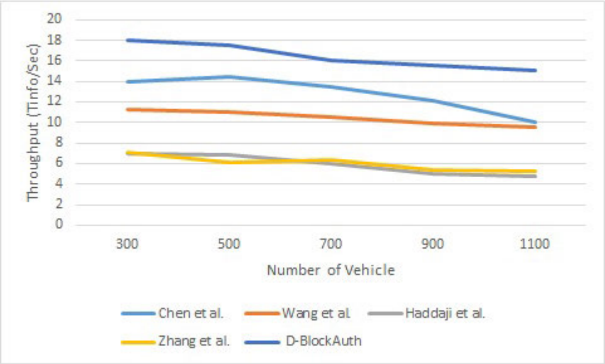


FIGURE 3. Evaluation of various schemes' throughputs with varied vehicle counts.

D. STORAGE

Each blockchain's storage use as a percentage of the total number of vehicles is displayed in Figure 4. When the number of vehicles equals 300, 500, 700, 900, and 1100, storage of $E - Block$, equals 0.8 GB, 1.2 GB, 2.1 GB, 2.4 GB, and 3.9 GB, respectively. When the number of vehicles equals 300, 500, 700, 900, and 1100, storage of $B - Block(EM)$ equals 1.6 GB, 1.8 GB, 2.9 GB, 4.3 GB, and 6.4 GB, respectively. When the number of vehicles equals 300, 500, 700, 900, and 1100, storage of $E-Block+B-Block$ equals 2.4 GB, 3.9 GB, 6.2 GB, 7.3 GB, and 8.7 GB, respectively. The reason behind the inconsistency in the $E - Block$ line graph is that, although both GM and EM are originally stored on the blockchain,GM is eventually erased to improve the $E-Block$'s efficiency.

Figure 4 presents the performance of different authentication schemes (D-BlockAuth and other schemes) based on storage requirements. by 1100 vehicles to 300 vehicles. The performance results of the D-BlockAuth scheme in terms of storage usage are illustrated to be efficient at all simulated leads and display a steady and slower growth of the storage overhead compared to the other schemes. The efficiency comes from how D-BlockAuth stores EMs long-term and removes GMs after time based on its strategy. As the number of D-BlockAuthed vehicles decreases, the storage requirements for all schemes decrease, but D-BlockAuth

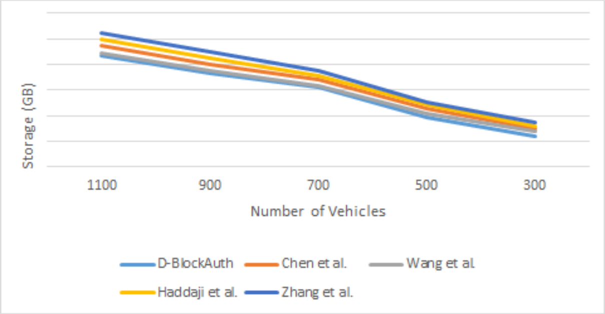


FIGURE 4. Data storage for proposed D-BlockAuth scheme and other schemes.

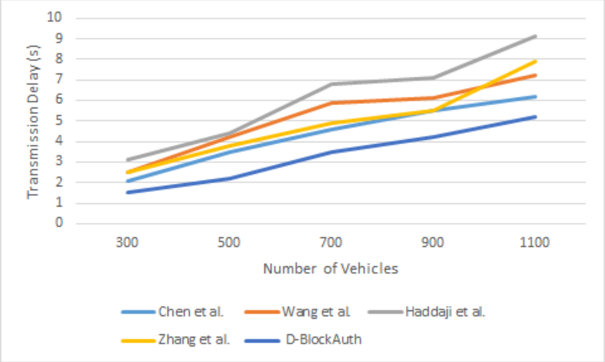


FIGURE 5. Analysis of transmission delays in various schemes with varied numbers of vehicles.

maintains a much larger advantage in reducing storage use. This work, which demonstrates the large scale and mobility robustness operation of FogHorn with vehicles in vehicular fog computing environments (under high-density scenarios) provides substantial evidence of the effectiveness as well as scalability of the compute approach.

E. TRANSMISSION LATENCY

The average amount of time that passes between sending and receiving transactions is called transmission delay. Although several factors influence this, the most important of these is the total number of vehicles on the network at any given moment. When there are more vehicles on the road, the gearbox delay increases accordingly. A vehicle's verification rate is the number of times per second that an RSU confirms the vehicle's identity. The quantity of automobiles being validated at any given moment has an inverse relationship with this.

Figure 5 compares the proposed D-BlockAuth scheme to current systems and finds that it has a smaller transmission latency. In the event of an emergency, a shorter transmission delay would be advantageous since it would indicate a faster flow of messages.

The throughput performance and corresponding transmission latency of the proposed D-BlockAuth scheme were simulated under various authentication scenarios for each vehicle, as shown in Figure 5. In summary, the results show that the D-BlockAuth scheme generally results in a lower transmission latency relative to other schemes, especially when the number of vehicles in the network increases. This reduced latency is the result of the dual blockchain architecture that optimizes the distribution of authentication tasks and thus reduces processing delays. Fast and timely communication is paramount for real-time applications in vehicular fog computing, so the swift processing of authentication requests in D-BlockAuth is also important. On the other hand, the rest of the schemes experience more delays which point out that there are possible bottlenecks and inefficiencies in their designs. This is even more highlighted by the improved performance of D-BlockAuth when it comes to keeping the latency low in terms of the response time it takes to reduce drastically the transmission latency and loss in the VFC systems.

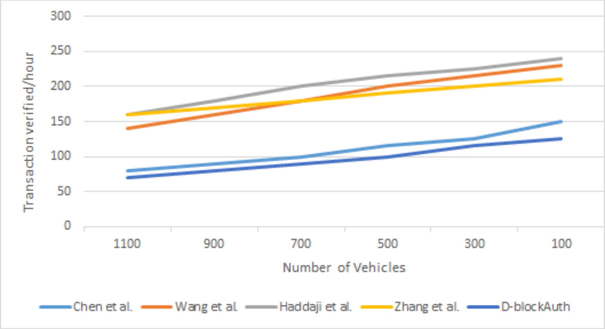


FIGURE 6. Transaction verification rate for different numbers of vehicles.

F. VERIFICATION RATE

The network's transactional load grows in direct proportion to the number of vehicles connected to it, since more vehicles mean more transactions. So, as the number of vehicles in the network increases, performance gradually drops. The $B - Block$ block size is 1 megabyte, which is equal to 1024 kilobytes. Block time is 28 seconds, and the average size of T_{info}/sec is 200 bytes. A block's validation and mining times, as measured by the fog server using Proof of Presence (PoP), make up the block time. The suggested schemes have a minimal block time since they use VLD, which the vehicles update regularly with their current position as PoP. The blockchain bypasses the VLD and gets the necessary data immediately whenever it's needed, drastically cutting down on block time. Each blockchain, $E - Block$, and $B - Block$, uses its database. Two databases exist one for car registration information and another for network messaging (GM and EM). At first, both GM and EM are stored in the storage. However, after a certain amount of time—which can be adjusted based on the needs of the network—the GM is deleted from the storage to make room for more critical emergency messages.

Figure 6 illustrates the transaction verification rate of various authentication schemes (related schemes and the proposed D-BlockAuth) concerning the number of vehicles injected from 100 to 1100. The verification performance of the proposed D-BlockAuth scheme was dramatically improved concerning the existing schemes. The dual blockchain architecture streamlines authentication tasks, which improves scalability and eliminates bottlenecks. With the growth of the number of cars, the verification rate in D-BlockAuth is also growing, proving the high stability of the solution under high loads in the network. The slower increase in the remaining three schemes, on the other hand, suggests the better performance of D-BlockAuth under the dynamic and resource-constraint vehicular fog computing scenarios.

G. DISCUSSION

Advancements of the D-BlockAuth Diluted Block Scheme: In this part, we detail the enhanced safety scalability and performance, so that it is possible to see exactly how our approach stands out using their company-offered blockchain approaches for VFC.

- Security Advancements: D-BlockAuth works on a dual blockchain architecture solution which is two times more secure compared to the traditional single blockchain method. D-BlockAuth keeps the keys to manage long-term identities on a separate blockchain versus with real-time authentication transactions, preventing a single point of failure. This architecture resolves the exposure to exploitation and breaches in the countless existing systems through which a common blockchain solution will reveal personal data during high-frequency operations. Adopting group and ring signatures additionally protects the network from impersonation and replay attacks, which is critical to preserving data integrity and privacy.
- Scalability Improvements: Conventional consensus mechanisms, until now, have failed to handle high transaction volumes of VFC efficiently and thus constrained the scalability of blockchain solutions. The way D-BlockAuth overcomes this challenge is by implementing a consortium blockchain that utilizes an optimized consensus designed for high throughput, latency. By setting up D-BlockAuth this way, we allow the service to autoscale with no limitation of cars or authentication requests in a way that will not impact the speed and reliability of the network. This is a significant advancement, as that eliminates the typical bottlenecks of early blockchain implementations that the system can grow in VFC environments.
- Performance Enhancements: For blockchain-based VFC systems, the performance becomes significant and related to how fast transactions are processed and how responsive the system is. D-BlockAuth works like no one else and offers multi-layered architecture using dual blockchain design that brings exceptional performance. These features help in processing authentication transactions at a quicker rate with the security not compromised, Designed from the ground up to enhance and optimize the experience of VFC applications, the performance of D-BlockAuth matches the instantaneous demands posed by these defects; outperforming existing blockchain solutions that try to prioritize both speed and security over one another.

In this work, the D-BlockAuth scheme is a long stride over the application of blockchain technology over vehicular fog computing. D-BlockAuth thereby not only advances the state-of-the-art by tackling very important challenges such as security, scalability, and performance but also represents a practically significant and sound approach that can be well-implemented in VFC environments with dynamic workloads. These advances are critical for blockchain to be adopted in intelligent transportation systems, a key application area where fast communication and timing accuracy are crucial.

VII. CONCLUSION AND FUTURE WORK

In this paper, a vehicular fog computing authentication method called D-BlockAuth uses dual blockchain technology to address security challenges in this 5G-BS-based area. Dual blockchains combine consortium and public blockchains to improve security, scalability, and privacy over single-chain techniques. A consortium blockchain secures fog network communication in D-BlockAuth. The public blockchain creates tamper-proof audit records and improves system accountability. The two blockchains' sharing of tasks reduces consortium blockchain scalability issues in fog computing. To protect user identities and ensure legal fog network participation, D-BlockAuth uses pseudonymization.

In the security evidence section, the proposed scheme resists replay attacks non-repudiation, modification, and impersonation, which leads to secure communication among vehicles in 5G-assisted VFC. The significance of doing both theoretical and empirical validation will be further explored in future work by expanding this study to include simulations using the AVISPA simulator. Meanwhile, the D-BlockAuth scheme provided the following list of possible future research directions:

- Enhanced Productivity: Streamlining the authentication scheme's cryptographic processes to lessen the computing burden on vehicles and fog nodes with limited resources. Investigating low-overhead blockchain protocols developed for use in car fog computing.
- Protected Data and Identity: To better safeguard user privacy while ensuring accountability, procedures for dynamic pseudonym changing should be implemented. For compromised vehicles or fog nodes, it is important to design a more robust revocation mechanism within the dual blockchain architecture. Using methods like homomorphic encryption to make sure sensitive data may be processed securely on fog nodes without anyone finding out.
- Efficiency and scalability: Testing how well the dual blockchain method scales in a congested urban setting with many autos and fog nodes. Improving the speed of transaction processing and reducing latency requires

creating methods for efficient blockchain consensus procedures.

- Combined Use of Different Technologies: Investigating how the suggested system can work in tandem with other cutting-edge technologies for sophisticated vehicle uses, such as 5G communication and machine learning. Looking into fog computing as a means for vehicles to work together in making decisions while protecting users' privacy.
- Application in the Real World: Building a working model of the system and putting it through its paces in a computer simulation of vehicular fog. To verify the scheme's viability and efficacy, we'll use a real-world testbed that includes automobiles and fog nodes.

This is by no means an exhaustive list of possible avenues for further study. The ever-changing demands and difficulties of privacy and security in vehicle fog computing will determine the precise foci.

REFERENCES

[1] N. Keshari, D. Singh, and A. K. Maurya, "A survey on vehicular fog computing: Current state-of-the-art and future directions," *Veh. Commun.*, vol. 38, Dec. 2022, Art. no. 100512.

[2] O. Nazih, N. Benamar, H. Lamaazi, and H. Chaoui, "Toward secure and trustworthy vehicular fog computing: A survey," *IEEE Access*, vol. 12, pp. 35154–35171, 2024.

[3] I. Javed, X. Tang, K. Shaukat, M. U. Sarwar, T. M. Alam, I. A. Hameed, and M. A. Saleem, "V2X-based mobile localization in 3D wireless sensor network," *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Feb. 2021.

[4] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 87–93, Feb. 2019.

[5] M. A. Saleem, S. Zhou, A. Sharif, T. Saba, M. A. Zia, A. Javed, S. Roy, and M. Mittal, "Expansion of cluster head stability using fuzzy in cognitive radio CR-VANET," *IEEE Access*, vol. 7, pp. 173185–173195, 2019.

[6] T. Klein, T. Fenn, A. Katzenbach, H. Teigeler, S. Lins, and A. Sunyaev, "A threat model for vehicular fog computing," *IEEE Access*, vol. 10, pp. 133256–133278, 2022.

[7] I. Javed, X. Tang, M. A. Saleem, A. Javed, M. A. Zia, and I. A. Shoukat, "Localization for V2X communication with noisy distance measurement," *Int. J. Intell. Netw.*, vol. 4, pp. 355–360, Jan. 2023.

[8] M. A. Saleem, Z. Shijie, and A. Sharif, "Data transmission using IoT in vehicular ad-hoc networks in smart city congestion," *Mobile Netw. Appl.*, vol. 24, no. 1, pp. 248–258, Feb. 2019.

[9] M. A. Saleem, Z. Shijie, M. U. Sarwar, T. Ahmad, A. Maqbool, C. S. Shivachi, and M. Tariq, "Deep learning-based dynamic stable cluster head selection in VANET," *J. Adv. Transp.*, vol. 2021, pp. 1–21, Jul. 2021.

[10] J. Huang, Y. Qian, and R. Q. Hu, "Security provision for vehicular fog computing," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[11] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, and T. H. Rassem, "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, Mar. 2023.

[12] C. Zhu, G. Pastor, Y. Xiao, and A. Ylajaaski, "Vehicular fog computing for video crowdsourcing: Applications, feasibility, and challenges," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 58–63, Oct. 2018.

[13] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, and A. Alsewari, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, p. 872, Feb. 2023.

[14] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[15] T. Mekki, I. Jabri, A. Rachedi, and M. B. Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," *Veh. Commun.*, vol. 9, pp. 268–280, Jul. 2017.

[16] C.-Y. Weng, C.-T. Li, C.-L. Chen, C.-C. Lee, and Y.-Y. Deng, "A lightweight anonymous authentication and secure communication scheme for fog computing services," *IEEE Access*, vol. 9, pp. 145522–145537, 2021.

[17] B. A. Mohammed, M. A. Al-Shareeda, A. A. Alsadhan, Z. G. Al-Mekhlafi, A. A. Sallam, B. A. Al-Qatab, M. T. Alshammari, and A. M. Alayba, "Service based VEINS framework for vehicular ad-hoc network (VANET): A systematic review of state-of-the-art," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 4, pp. 2259–2281, Jul. 2024.

[18] Y. Erb, Ö. N. Subas, A. Zhyliak, and O. Zimmermann, "Societal perception of security threats in vehicular fog computing," CII Student Papers, Karlsruhe, Germany, White Paper 1000150170, Aug. 2022, p. 76.

[19] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, A. Khalil, M. A. Al-Shareeda, B. A. Mohammed, A. A. Alsadhan, A. M. Alayba, A. M. S. Saleh, H. A. Al-Reshidi, and K. Almekhlafi, "Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5G-assisted vehicular communications," *IEEE Access*, vol. 12, pp. 71232–71247, 2024.

[20] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," *Veh. Commun.*, vol. 29, Jun. 2021, Art. no. 100335.

[21] Y. Xu, C. Yao, J. Cui, and H. Zhong, "LPPA-RCM: A lightweight privacy-preserving authentication scheme for road condition monitoring in fog-based VANETs," *J. Syst. Archit.*, vol. 143, Oct. 2023, Art. no. 102967.

[22] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7940–7954, Jul. 2020.

[23] H. Zhong, L. Wang, J. Cui, J. Zhang, and I. Bolodurina, "Secure edge computing-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3774–3786, 2023.

[24] F. Dewanta and M. Mambo, "A mutual authentication scheme for secure fog computing service handover in vehicular network environment," *IEEE Access*, vol. 7, pp. 103095–103114, 2019.

[25] Y. Xu, X. Liu, J. Cui, H. Zhong, and J. Zhang, "L-TCM: A lightweight privacy-preserving traffic condition monitoring scheme with source authentication in cloud-assisted VANETs," *IEEE Syst. J.*, vol. 21, no. 11, pp. 4654–4665, Nov. 2020.

[26] A. M. Farooqi, M. A. Alam, S. I. Hassan, and S. M. Idrees, "A fog computing model for VANET to reduce latency and delay using 5G network in smart city transportation," *Appl. Sci.*, vol. 12, no. 4, p. 2083, Feb. 2022.

[27] J. Cui, Y. Chen, H. Zhong, D. He, L. Wei, I. Bolodurina, and L. Liu, "Lightweight encryption and authentication for controller area network of autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14756–14770, Nov. 2023.

[28] S. Goudarzi, S. A. Soleymani, M. H. Anisi, M. A. Azgomi, Z. Movahedi, N. Kama, H. M. Rusli, and M. K. Khan, "A privacy-preserving authentication scheme based on elliptic curve cryptography and using quotient filter in fog-enabled VANET," *Ad Hoc Netw.*, vol. 128, Apr. 2022, Art. no. 102782.

[29] J. Cui, X. Liu, H. Zhong, J. Zhang, L. Wei, I. Bolodurina, and D. He, "A practical and provably secure authentication and key agreement scheme for UAV-assisted VANETs for emergency rescue," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 2, pp. 1454–1468, Mar. 2024.

[30] J. Chen, K. Li, and P. S. Yu, "Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 11633–11642, Aug. 2022.

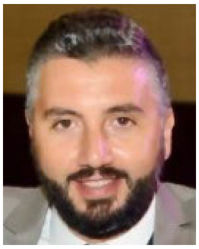
[31] S. Wang, Y. Hu, and G. Qi, "Blockchain and deep learning based trust management for Internet of Vehicles," *Simul. Model. Pract. Theory*, vol. 120, Nov. 2022, Art. no. 102627.

[32] A. Haddaji, S. Ayed, and L. Chaari, "Federated learning with blockchain approach for trust management in iov," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.* Springer, 2022, pp. 411–423.

[33] B. Zhang, X. Wang, R. Xie, C. Li, H. Zhang, and F. Jiang, "A reputation mechanism based deep reinforcement learning and blockchain to suppress selfish node attack motivation in vehicular ad-hoc network," *Future Gener. Comput. Syst.*, vol. 139, pp. 17–28, Feb. 2023.

HUSSAM DHEAA KAMEL AL-JANABI was born in Baghdad, Iraq, in 1986. He received the B.S. degree in computer communications engineering from Al-Rafidain University College, in 2008, and the M.Sc. and Ph.D. degrees in telecommunication and network engineering from the Kharkiv National University of Radio Electronics (KNURE), in 2010 and 2013, respectively. He is currently an Assistant Professor of computer technical engineering with Al-Mustafa University College. His research interests include wireless communications, MIMO, WiMAX, LTE, visible light communication, control systems, wireless sensor networks, 5G, the Internet of Things (IoT), and LiFi technology.

SAIMA ANWAR LASHARI received the B.Sc. degree (Hons.) in computer science from the University of Engineering and Technology (UET), Lahore, Pakistan, in 2004, and the M.Sc. and Ph.D. degrees in information technology from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia, in 2012. Her research interests include data mining, classification, and soft sets.



AYMAN KHALIL received the M.Sc. degree in networking and telecommunications from Lebanese University/Saint Joseph's University, Beirut, Lebanon, in 2007, and the Ph.D. degree in telecommunications from the National Institute of Applied Sciences (INSA), Rennes, France, in 2010. During the Ph.D. degree, he was with the Institute of Electronics and Telecommunications of Rennes (IETR), where he worked on the optimization of high data rate WPAN systems. He has been involved in supervising Ph.D. students in Lebanon and France. He has been involved in several European projects, including OMEGA, where he worked for three years in developing solutions and protocols for next-generation home networks. His main research interests include next-generation computer systems, security, network coding, AI-based optimization solutions, and data analytics.

MAHMOOD A. AL-SHAREEDA received the B.S. degree in communication engineering from Iraq University College, the M.Sc. degree in information technology from Islamic University of Lebanon (IUL) in 2018, and the Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He was worked as a Postdoctoral Fellowship at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He is currently an Assistance Professor at Communication Engineering, Iraq University College (IUC). His current research interests include network monitoring, the Internet of Things (IoT), vehicular ad hoc network (VANET) security and IPv6 security.

ABEER ABDULLAH ALSADHAN is currently an Assistant Professor of information security and artificial intelligence with Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. She has published a number of publications in reputed journals. Her research interests include machine learning, deep learning, cyber security, and the Internet of Things.

MOHAMMED AMIN ALMAIAH is currently an Associate Professor in cybersecurity with The University of Jordan. He has published over 120 research articles in highly reputed journals, such as the *Engineering and Science Technology, an International Journal*, *Education and Information Technologies*, and IEEE Access. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include cybersecurity, cyber risk assessment, and cyber risk management.

TAYSEER ALKHDOUR received the Ph.D. degree in computer science and engineering from the King Fahd University of Petroleum and Minerals (KFUMP), Dhahran, Saudi Arabia. He is currently an Assistant Professor with the Department of Computer Networks and Communication, College of Computer Science and Information Technology, King Faisal University (KFU). He is also a Consultant for quality and academic accreditation in the deanship of development and quality accreditation at KFU. He is providing quality and academic accreditation consultations to different colleges and programs. He was the leader of different teams that were working on applying for NCAAA and ABET accreditation. At KFU, he is an internal reviewer for the programs applying for NCAAA accreditation. He has a certificate as IDEAL Scholar "Program Assessment Leader." In addition to NCAAA, he has experience in different accreditation commission standards, such as ABET and AACSB. He has delivered tens of workshops in different areas of quality and academic accreditation. He was a Reviewer of the National Center for Academic Accreditation and Evaluation (NCAAA) and the National Center for Training Assessment and Accreditation (MASAR), Saudi Arabia.