IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 December 2023, accepted 4 January 2024, date of publication 8 January 2024,
date of current version 16 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3351278

RESEARCH ARTICLE

HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks

BADIEA ABDULKAREM MOHAMMED[1], (Senior Member, IEEE), MAHMOOD A. AL-SHAREEDA[2], ZEYAD GHALEB AL-MEKHLAFI[3], JALAWI SULAIMAN ALSHUDUKHI[3], AND KAWTHER A. AL-DHLAN[4]

[1]Department of Computer Engineering, College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia
[2]Department of Communication Engineering, Iraq University College, Basrah 11800, Iraq
[3]Department of Information and Computer Science, College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia
[4]Department of Artificial Intelligence and Data Science, College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia

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

This work was supported by the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, under Project RG-23116.

ABSTRACT The quick progress of 5G networks has allowed for intelligent driving. The primary environment for intelligent driving is provided by vehicular ad hoc networks (VANETs), which relay real-time data and communications between moving vehicles and fixed infrastructure. Since the communication is open-access, the message exchanged is vulnerable to privacy and security attacks. To address with this challenge, several authentication schemes have proposed. Nevertheless, the complexity of current these schemes means that re-authenticating vehicle identities every time they reach a new area of infrastructure coverage significantly hampers the overall network's efficiency. This paper has proposed a handover authentication, called HAFC scheme based on fog computing to achieve fastly re-authentication of vehicles via secure property transfer among infrastructures (fog servers) for 5G-assisted vehicular blockchain networks. The proposed HAFC scheme consists of both stages namely, initial-authentication stage and handover-authentication stage. In security analysis shows that the proposed HAFC scheme's vehicle to fog server-for both stages is Computational Diffie-Hellma (CDH)-secure. According to the simulation results, the novel handover authentication stage takes only a fraction of the time required for the first one.

INDEX TERMS Re-authentication scheme, handover authentication, 5G-assisted blockchain, fog computing, vehicular blockchain network.

I. INTRODUCTION

There will be about 50 billion Internet-connected devices, all working together to make life better for people everywhere. The Internet of Things (IoT) is the concept of connected, intelligent devices that increase the amount of communication and cooperation between them, thereby making the world a safer and more efficient place [1]. The Internet of Vehicles (IoV) is a new field that combines the Internet of Things (IoT) with Vehicular Ad hoc Network (VANET) infrastructures to improve the driving experience for passengers [2]. As the field of big data and the Internet of Things (IoT) continues to expand at a dizzying rate, IoV has emerged as a crucial enabling technology for the implementation of autonomous driving case and ad hoc networking in the near future. Conventional VANET is evolving into IoV in the current Intelligent Transportation Systems (ITS) research paradigm. The Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications provided by VANET, a form of MANET, are an integral part of Intelligent Transportation Systems (ITS) [3]. Using the dedicated short-range communication (DSRC) standard, critical data can be transmitted between vehicles while they are in motion [4]. Position, road, safety, traffic, and driver

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

support/luxury are just some of the many uses [5], [6] for this technology.

Networks of the fifth generation (5G) are optimised to enable URLLC application [7], such as the vehicle-to-everything (V2X) of Vehicular Ad Hoc Networks (VANET) in the Intelligence Transportation System [8]. Researchers and academics alike have become increasingly interested in 5G-assisted vehicular networks in recent years; for example, the 5G Automotive Association (5GAA) believes that Cellular V2X (C-V2X) developed by the Third Generation Partnership Project (3GPP) will be an appropriate technology to provide URLLC for 5G-assisted vehicular networks [9], and Qualcomm Technologies has announced that its 5G-assisted vehicular networks chipset, which supports C-V2X, will be available in 2018 [10]. As 5G-assisted vehicular networks advances rapidly, associated applications like autonomous vehicles can be brought to fruition very instantly.

Despite 5G-assisted vehicular networks' many benefits, some issues remain that must be addressed [11], [12]. Messages must be protected by a strong security method because they are sent over an open wireless network. In addition, confidentiality and speed of authentication must be guaranteed [13]. VANET also needs to prioritise and improve security. To achieve this, nodes must be able to transmit and receive data reliably and efficiently. However, it is vulnerable to malware attacks due to the unsecure environment in which it operates. In principle, VANETs should be able to protect users' personal information, keep their communications secure, and withstand security threats.

Every vehicular system terminal is potentially vulnerable to a wide variety of attacks, which poses serious challenges to putting smart vehicle system protocols into practice in the real world. The importance of vehicle-to-infrastructure communication in-vehicle systems cannot be overstated. When entering the range of a new fog server, vehicles must re-authenticate with each fog server, as is the case with most modern V2I communication methods. While these techniques can reliably verify the vehicle's identity, they also introduce issues including high communication costs and unnecessary duplication of effort. Most recent studies assume that vehicles will need to re-authenticate with a new fog server every time they enter a new fog server coverage region. This creates a lot of extra work and slows down the vehicle network. In a network where the topology is constantly shifting, any delay is unacceptable. In order to lessen the computing load on cars and the network delay, it is vital to lessen the redundancy created by refined authentication. Furthermore, in a decentralized nontrusted vehicular system, it is difficult to verify the trustworthiness and prohibit misbehaving cars. In addition, the computation of vehicle trustworthiness is not scalable, making it difficult to meet the evolving requirements of vehicle networks. The major contributions of this paper are listed as follows.

- This paper proposes a handover authentication scheme, called HAFC based on fog computing for 5G-assisted vehicular blockchain networks. The proposed HAFC scheme suggests incorporating blockchain technology for keeping track of car characteristics and credibility ratings. Because of the blockchain, the services can't be altered and their history can be tracked. Bitcoin transactions are treated as data updates whenever there is a change to a vehicle's properties. The dependability of the vehicle's attributes can be reliably computed because of the tamper-resistance, which prevents arbitrary falsification of those qualities. If a vehicle is traceable, its credibility can be questioned at any moment, and by looking at its past records, a more solid basis for its credibility estimation can be found.
- This paper introduces a scalable computing system that is blockchian-assisted in terms of trustworthiness. fog servers, acting as the system's miner, validate the reliability of the consensus method. In order to achieve near-instantaneous data logging of car characteristics, the system makes use of Merkle hash trees (MHT). The flexibility with which the archive may be updated to accommodate new vehicles, new vehicle models, and other network modifications is a major boon to the system's usability.
- This paper outlines the steps involved in the first level of authentication for vehicles joining the network. In this step, we combine the scalable computation of trustworthiness made possible by blockchain technology, and then we use the resulting value to verify the vehicle's dependability. In the first stage, users just need to do minimal processing to authenticate a new car. The legality of the vehicle can be verified entirely by fog server infrastructure via 5G-BS thanks to this authentication. When a vehicle has been authenticated as a valid member of the network, it will undergo a second handover phase during which it will undergo a third authentication. In order to streamline this handover authentication step and save time on computations for following vehicle authentication operations, some sort of handover message and a token are used. The flexibility of the network is enhanced by the handover phase's architecture, which makes it simple and safe for vehicle ownership to be transferred between fog servers.

The remainder of this work is structured as follows. In Section II, this paper provides literature review according to propose methods in vehicular system. In Section III, this paper introduces the background. In Section IV, this paper proposes HAFC scheme and describes its phases. Security analysis and performance evaluation are provided in Section V and Section VI, respectively. Lastly, this paper concludes the study in Section VII.

II. STATE OF THE ART

Some academics have proposed methods for protecting passengers' confidentiality in moving vehicles as follows. An effective and safe conditional privacy preservation strategy for vehicular system was proposed by Qi et al. [14].

Pseudonym-based technique and certificateless signature mechanism are combined to build the anonymous authentication scheme, which is used to ensure conditional privacy in VANETs. The technique also assures that the pseudonyms cannot be attached prior to being traced, which is a major benefit in the context of swiftly revoking vehicles. Analysis of the suggested scheme's security shows that it is up to the task of protecting users' personal information on VANETs. To ensure the safety of V2I connections, Zhong et al. [15] proposed a certificateless aggregate signature authentication technique with full aggregation in VANET. Aggregate signature is a method for authenticating messages while significantly reducing network and computational overhead. Further, we employ pseudonym to achieve conditional privacy preserving, with a trace authority (TRA) tasked with producing the pseudonym and, if necessary, monitoring the real identity throughout the communication. Goudarzi et al. [16] offered an authentication method that is both robust and private. Quotient Filter (QF) was utilised to handle node authentication in the proposed technique, whereas Elliptic Curve Cryptography (ECC) was employed to handle message authentication. In addition, in order to protect users' anonymity on VANET, each vehicle was assigned a unique pseudo-identity. Liu et al. [17] suggested PTAP, a revolutionary secure privacy-preserving traceable authentication technique in order to improve the situation in more ways than one and reduce computation costs by 32.75 percent on the vehicle side by employing semi-honest-RSU for enabling interaction between stakeholders without the need for a trusted third party.

Authentication by signature was done by a few researchers as follows. Based on lattice cryptography for quantum-resistance and Bonsai-tree signature architecture for forward security, Cao et al. [18] offered a novel group signature technique for authentication in VANETs. When tested against the Short Integer Solution (SIS) and the Learning With Errors (LWE) hardnesses, their technique was shown to be secure in all three of these areas. Jain et al. [19] suggested a method for verifying digital signatures that is both quick and easy to implement. The use of manual signatures for authentication purposes remains widespread. However, manual signatures are still not used in mobile and automobile networks for security purposes. Using an enhanced Elman backpropagation (I-EBP) model, they recreated the process of transforming handwritten signatures into bogus digital signatures. A digital signature was used to verify the identity of the sender and the integrity of the message during the network handshake. The data includes sensitive information about a vehicle's location on the road, so its security could be strengthened. Samra and Fouzi [20] explored ring signature and aggregate concepts in the certificate-less setting, where they can minimise costs while maximising advantages. In order to guarantee conditional privacy preservation authentication in VANET communication, they offered a new framework called Certificateless Aggregate based on Traceable Ring Signature (CLA-TRS), which drastically reduces the computational complexity associated with verifying signatures.

The topic of batch authentication is crucial for academic study as follows. In order to prevent unapproved vehicles from using a zone's services, Chen et al. [21] presented a batch authentication technique for VANETs called BASRAC, which includes rule-based access control during the authentication step. In addition to boosting authentication efficiency, batch verification is another feature that BASRAC offers. In addition, BASRAC protects privacy, so the partially trusted roadside unit (RSU) cannot access sensitive data about available services. Wang et al. [22] looked into the feasibility of a secure access control mechanism with batch verification for automotive ad hoc networks, with the goal of increasing network efficiency. The suggested method uses the same amount of operations for verifying requests as for a single verification, which is two bilinear pairing operations. Performance investigation showed that compared to other methods, the proposed one had the lowest computing cost and the lowest communication overhead. Maurya and Chaurasiya [23] proposed a secure and efficient anonymous batch authentication technique with conditional privacy (EABAS-CP) for the Internet of Things (IoT) setting, based on elliptic curve cryptography. The EABAS-CP method was able to provide conditional privacy by effectively identifying the offending vehicle. Distributed parameters in the RSU create a pseudo-identity for cars and generate unique signatures that can be communicated securely without the need for encryption or TAs.

The advent of 5G is a driving force behind the creation of vehicular systems as follows. Gupta et al. [24] proposed a unique approach towards an IoV architecture model and an authentication-based protocol (A-MAC) for smart vehicular communication. To ensure the necessary level of security, the technique calls for hash operations and use cryptographic ideas to transmit messages between cars. The effectiveness of a security system against different kinds of attacks can be gauged by measuring how well it performs. The goal of this study by Nyangaresi et al. [25] was to design a secure protocol that is both cost-effective and resistant to common security threats like spoofing, man-in-the-middle attacks, replays, and eavesdropping.

The advent of fog computing is a driving force behind the creation of vehicular systems as follows. In order to improve the efficiency of vehicle authentication, Han et al. [26] offered a fog-computing-based anonymous-authentication strategy for VANETs in order to allow vehicles and road-side units (RSUs) to authenticate themselves, which lessens the communication burden on the TA. To keep the anonymity up-to-date, they devised a fog-computing-based pseudonym-updating and -tracking technique that ensures continuous two-way communication and cuts down on the need for authorised vehicles to undergo additional authentication procedures. Fog computing was proposed by Al-Otaibi et al. [27] as a revolutionary method for detecting rogue nodes in vehicles while maintaining user privacy. The suggested approach prevented vehicles from exchanging traffic data with one another and instead permits communication only via roadside units (RSUs), which increases vehicle privacy, inter-vehicle communication, and computational efficiency. To further enhance the precision and effectiveness of VANETs, they system suggested an RSU authentication method and a mechanism that would enable RSUs to detect and delete vehicles producing bogus traffic data. In order to facilitate re-authentication, Han et al. [28] proposed integrating Mobile Edge Computing (MEC) server infrastructure into the current authentication architecture. On top of this authentication framework, they develop a new authentication mechanism by enhancing the preexisting Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) protocol. Pseudonyms are used in place of real names and authentication was performed with a one-way hash function to increase security.

Researchers have also proposed a few other ways that blockchain technology could be used in vehicular system as follows. Without relying on a central server in the cloud, Dwivedi et al. [29] suggested a new decentralised structure for VANETs. In addition, a system for using the blockchain to secure event data and vehicle authentication is presented here. Using this protocol, authorised users can safely retrieve event details from the IPFS. They used IPFS and blockchain to store data in a completely decentralised fashion. The suggested approach is evaluated in comparison to current best practises. Tan and Chung [30] proposed a secure authentication and key management strategy to solve the aforementioned problems. Because of the limitations of the standard VANET architecture, they have elected to use a novel VANET system model that incorporates edge computing infrastructure in our design. In order to prevent any unwanted interference, each vehicle's unique session key is used in our certificate-free authentication system. Maria et al. [31] tacked advantage of the distributed nature of blockchain technology to quickly reauthenticate vehicles by passing a secure authentication code between successive RSUs. The security study section demonstrates that the proposed blockchain-based anonymous authentication mechanism is secure and resistant to a variety of destructive security threats.

However, while moving from one RSU coverage area to another, authentication has not received a lot of focus in the aforementioned studies. At the same time, the vehicle attribute parameters are underutilised in order to compute a vehicle's trustworthiness, which would greatly enhance the dependability and scalability of vehicular system. Therefore, this paper proposes HAFC scheme that support handover authentication using fog server instead of RSU for 5G-assisted vehicular blockchain networks.

III. BACKGROUND

A. ARCHITECTURE OF SYSTEM

As shown in Figure 1, the architecture of the system model of the proposed HAFC scheme includes one Trusted Authority (TA), some Fifth Generation-Base Station (5G-BS), some fog servers, and several Onboard Units (OBUs) installed in vehicles as the major components that interact together in the 5G-assisted vehicular blockchain network. The description of these components is provided as follows.

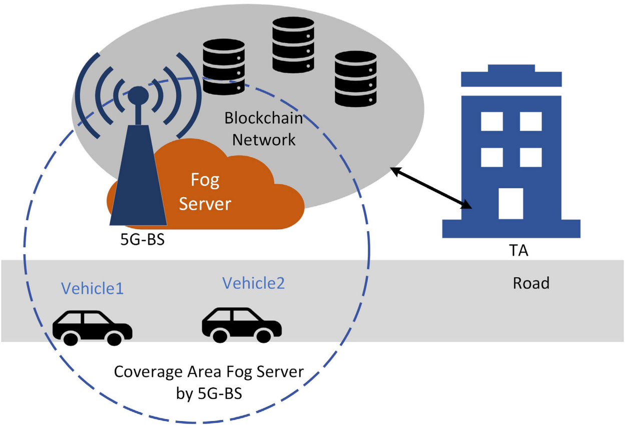

FIGURE 1. Architecture of system model for HAFC scheme.

- Trusted Authority (TA): A reliable administration that can set system parameters and add vehicles and fog servers to the database. The TA is also accountable for carrying out the procedure of traceability.
- Fifth Generation-Base Station (5G-BS): Is wireless infrastructure deployed by the roadside. Under the assumption, any storage purpose or computing process doesn't happen in this component. Therefore, the main purpose of this component is to increase the serve large number of vehicles within its coverage.
- Fog Server: Fog servers are in charge of gathering data on vehicles' attributes, performing scalable computations on vehicle trustworthiness, and updating the trustworthiness blockchain. A fog server must also verify the legitimacy of a vehicle's registration. The fog server must perform the initial authentication of a vehicle if it has not yet been authenticated in the system. If a vehicle enters this fog server's coverage area via 5G-BS after leaving the coverage area of another fog server via 5G-BS, this fog server will authenticate the vehicle's handover using that other fog server's data.
- Onboard Unit (OBU): On-board units (OBUs) refer to the many sensor nodes installed in a vehicle. OBUs gather the vehicle's true attributes and relay that data to fog servers via 5G-BS in the area. When the vehicle comes under a 5G-BS coverage, it must perform initial authentication or handover authentication with the fog server applying a set of parameters provided by TA and authentication parameters or tokens transmitted by the fog server.
- Blockchain Network: The blockchain is used to keep track of the reliability and characteristics of automobiles in this system. For the sake of authenticating a car, these details are crucial.

B. DESIGN GOAL

The design target of the proposed HAFC scheme is to resist forged vehicles with both aspects and security attacks. The forged vehicles discussed in this article fall into two categories: forged newcomers and forged handover vehicles.

- First Aspect: Someone has created a fake car to join the network and needs it verified as a legitimate car by the fog server via 5G-BS. Under the assumption that the attacker can access the forged vehicle's storage, he can retrieve the attacker's session key PK_1, which was produced by the vehicle using the fog server's public key and the attacker's secret key. It is possible for the attacker to receive the fog server's sent parameters and timestamps.
- Second Aspect: Someone has forged a vehicle intended for use in the area of the next fog server via 5G-BS coverage and wishes to have it verified by that fog server. Our working hypothesis is that the attacker can retrieve the previous session key created by the car using the parameters transmitted by the previous fog server. The attacker can also receive the token sent by the subsequent fog server as well as the parameters and timestamps sent by the previous fog server.

C. SECURITY ATTACKS MODEL

The proposed HAFC scheme should be resisted security attack models as follows.

- Man-in-the-Middle (MITM) Attack: A Man-in-the-Middle (MITM) attack is one in which the attacker positions themselves between the sender and the recipient of a message and attempts to alter its contents. The original data will be modified by such an attack. We presume that a man-in-the-middle (MITM) attacker can intercept the communication and perform the required calculations.
- Reply Attack: With a replay attack, the adversary collects authentication messages already delivered from the vehicle to the fog server and tries to pass the authentication using the fog server. This type of attack makes use of a legitimate message. It's possible for malevolent individuals to leverage a defunct authentication message to their advantage.

D. BLOCKCHAIN CONCEPT

Blockchain is a distributed ledger that does not rely on a single administrator. Blockchain's main benefit is its low cost and efficiency in solving problems like personal trustworthiness records in networks. Instead than relying on a centralised system, P2P interaction is used. For records to be instantly verifiable, transparent and traceable, indisputable and difficult to tamper with, blockchain employs cryptographic technology, timestamp and consensus algorithm to assure the consistency of information in each node database.

Data integrity preservation, data encryption, consensus calculation for workload proof, block linkage, etc. are some of the most common uses for hash functions. Common hash functions in blockchain applications include SHA256 and RIPEMD160. Transactions and blocks are encrypted using SHA256, while bitcoin addresses are generated using RIPEMD160. The use of hash pointers as part of a block-linking function is depicted in Figure 2. Blockchain employs Merkle hash trees extensively. Binary tree blockchains are normal. Nodes store data hashes. The MHT leaf nodes will have txn rcd hashes. The hash value identifies the Merkle root after adding leaf node pairs to the block. The value of the node hashAB is the hash of the two leaf nodes hashA and hashB, as shown in Figure 2. Assuming there are two identical leaf nodes, the system will utilise the above approach to compute hashEE when there is only one leaf node, as in the case with hashE.

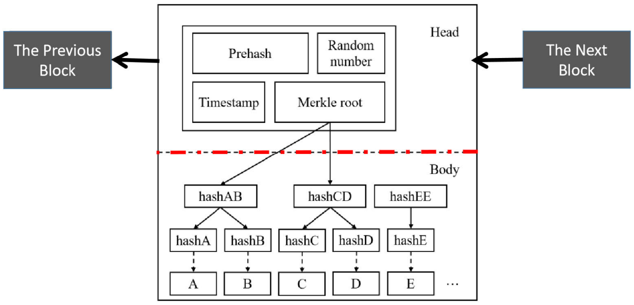

FIGURE 2. The blocks structure.

A blockchain-assisted trustworthiness scalable compute system is developed with blockchain's tamper-resistance and traceability as key features. The fog server is the central node in this system, and it is responsible for mining vehicle attribute data in order to implement the scalable computation of vehicle trustworthiness in real time. The consensus method ensures that all vehicles in the network have the same level of dependability at all times. Each fog server can look up a vehicle's trustworthiness value in the blockchain to see if it satisfies the region's requirements for access to information. Authentication of identity is made easier because to the reliability. The blockchain will make the computation of a vehicle's trustworthiness more efficient, leading to greater use.

E. PROPOSED 5G-ASSISTED VEHICULAR BLOCKCHAIN NETWORKS FRAMEWORK

Each vehicle node is temporarily associated with a single fog server, and each fog server is accountable for the scalable computation of a number of vehicle nodes' trustworthiness values. Each fog server is tasked with mining the attribute data of vehicles operating in its region, doing an evaluation, and adding the trustworthiness value of those vehicles to the distributed ledger. TAI, or trustworthiness attribute information, and TL, or trustworthiness level, are two terms that have been clearly defined.

Description 1 (Trustworthiness Attribute Information, TAI): TAI is a set of parameters indicating numerous vehicle properties. Set $A = a_1, a_2, a_3, \ldots a_m$, where A is the set of

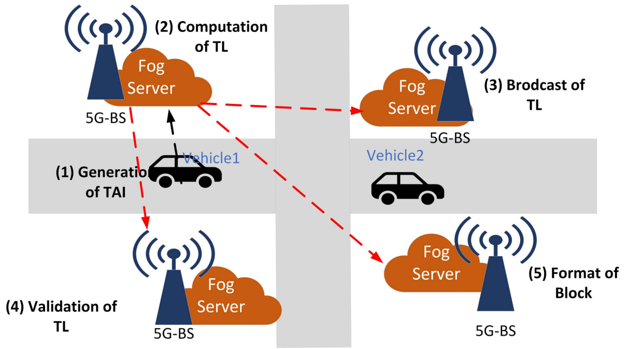

FIGURE 3. Proposed framework of 5G-assisted Vehicular Blockchain networks.

TAI and a_1, a_2, a_3,...a_m are parameters a_m has gathered by OBUs. OBUs gather up these transmissions and relay them to the fog server via 5G-BS. TAI improves the scalability of the data source used in the computation of trustworthiness. The fog server will use TAI to determine the TL of each vehicle.

Description 2 (Trustworthiness Level, TL): The TL of a vehicle is a standardised, sharable computing benchmark that is derived from the TAI data acquired from that vehicle and used by all fog servers.

Example of the suggested vehicular blockchain networks is presented in Figure 3. The fog servers awarded as part of the plan contribute to the blockchain's ability to keep track of a vehicle's reliability history. A new notation, TL_n, has been introduced to indicate the reliability at time n. The fog server provides input for a trustworthiness calculation of the car at present and is recorded in a distributed ledger. The data in each block is then determined based on its provenance and the reliability of previous blocks. Finally, these amounts are recorded in the blockchain so that all fog servers may be searched for and retrieved at any time. Following are the five main stages of the calculation:

- Generation of TAI: TAI is produced by the vehicle's OBUs. When these values are altered, the Bitcoin wallet automatically updates the relevant roadside devices.
- Computation of TL: When a vehicle sends its TAI to the nearest fog server via 5G-BS, the fog server receives information about the vehicle, the node, and any changes made to the vehicle. After receiving the TAI, the fog server determines the car's TL.
- Broadcast of TL: Other fog servers in the network receive not just the TL but also the TAI.
- Validation of TL: After receiving the transmission, all fog servers will make every effort to find the answer. After a miner has successfully solved the problem, a new block in the blockchain is created by appending a validated TL to the end of the chain.
- Formation of Block: Once the verified TL has been appended to the blockchain, a copy of the modified blockchain is saved on every node.

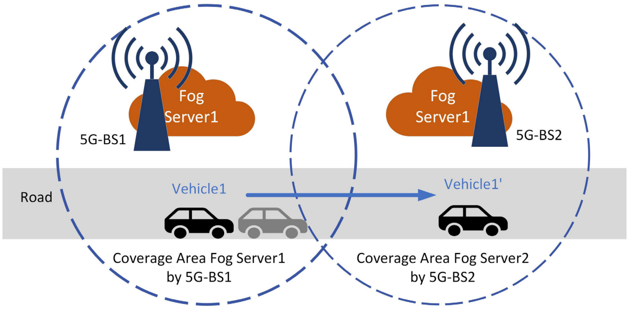
5G-BS1
Fog Server1
Fog Server1
5G-BS2
Road
Vehicle1
Vehicle1'
Coverage Area Fog Server1 by 5G-BS1
Coverage Area Fog Server2 by 5G-BS2

FIGURE 4. Explanation of the proposed HAFC scheme.

IV. PROPOSED HAFC SCHEME

With the aim of solving the issue of secure vehicle handover between two neighboring fog servers, this paper proposes a handover authentication scheme based on fog computing called HAFC for 5G-assisted vehicular blockchain networks. The proposed HAFC scheme's hypothetical implementation is shown in Figure 4. The basic steps of the plan are as follows. To begin, the fog server and the car finish the authentication process and generate an initial session key depending on the vehicle's current trustworthiness level. Then, when the vehicle's fog server coverage area via 5G-BS changes, the outgoing fog server transmits a handover certificate to the incoming fog server and the vehicle, and the incoming fog server sends a token to the vehicle. After the vehicle and the latter fog server concurrently calculate the corresponding session key, the car can once again communicate with the roadside infrastructure. Keep in mind that this only applies while the car is within the next fog server's coverage area. The fog server must merely verify if the vehicle's reliability has been altered. The proposed HAFC scheme consists of both stages namely, initial-authentication stage and handover-authentication stage, which each stage has server phases. In initial-authentication stage, the generation of key (GenKey), generation of private key (GenVehPK) for vehicle, and generation of private key (GenFogPK) for fog server. While handover-authentication stage consists of four main phases, namely, generation of handover certificate (GenHC), generation of token (GenToken), generation of private key2 (GenVehPK2) for vehicle, generation of private key2 (GenFogPK2) for fog server.

A. INITIALIZATION STAGE

This stage executes the following process.

- The TA issues a bilinear paring $e' : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, witch $\mathbb{G}$ and $\mathbb{G}_T$ are two groups of cyclic with order p achieving the mapping connection.
- The TA selects three general-one way hash functions H_0, H_1, H_2 as $H_0 : \mathbb{G} \rightarrow \{0, 1\}^*$, $H_1, H_2 : \{0, 1\}^* \rightarrow Z_q^*$.
- The TA picks two different generators h and g in the group $\mathbb{G}$.

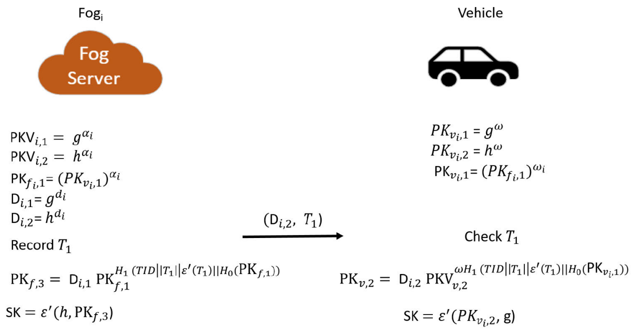
Fog$_i$
Fog Server
Vehicle
$PKV_{i,1} = g^{\alpha_i}$
$PKV_{i,2} = h^{\alpha_i}$
$PK_{f_{i,1}} = (PK_{v_{i,1}})^{\alpha_i}$
$D_{i,1} = g^{d_i}$
$D_{i,2} = h^{d_i}$
Record T_1
$PK_{f,3} = D_{i,1}\, PK_{f,1}^{H_1(TID||T_1||\varepsilon'(T_1)||H_0(PK_{f,1}))}$
$SK = \varepsilon'(h, PK_{f,3})$
$(D_{i,2}, T_1)$
$PK_{v_{i,1}} = g^{\omega}$
$PK_{v_{i,2}} = h^{\omega}$
$PK_{v_{i,1}} = (PK_{f_{i,1}})^{\omega_i}$
Check T_1
$PK_{v,2} = D_{i,2}\, PKV_{v,2}^{\omega H_1(TID||T_1||\varepsilon'(T_1)||H_0(PK_{v_{i,1}}))}$
$SK = \varepsilon'(PK_{v_{i,2}}, g)$

FIGURE 5. **Description of vehicle to Fog server-initial authentication stage.**

- Finally, the TA selects randomly non-zero item $\alpha_i, \alpha_i + 1, \cdots \in Z_q^*$ with prime order p for fog server Fog_i, $Fog_i + 1, \cdots$.

B. INITIAL AUTHENTICATION STAGE

In this step, the TL value produced by the trustworthy scalable computation system is used. During this step, a fog server will help a vehicle authenticate its identity so that the fog server can generate a session key for use with the vehicle while the vehicle is within the fog server's signal range. The description of the vehicle to fog server-initial authentication stage is shown in Figure 5. This stage includes three phases: GenKey, GenVehPK, and GenFogPK as follows.

1) GENKEY PHASE

A Diffie-Hellman secret key is created by using the respective public keys of the fog server and the vehicle in the following steps.

- Fog server Fog_i computes $PK_{f_1} = (PK_{veh_1})^{\alpha_i}$ and the vehicle computes $PK_{v_1} = (PKV_{i,1})^{\omega}$, where α_i and ω are the private keys of fog server and the vehicle, receptively.
- Fog server Fog_i selects $d_i \in Z_q^*$ and computes $D_{i,1} = g^{d_i}$.
- After $D_{i,2} = h^{d_i}$ is computed, Fog server Fog_i is transmitted to the vehicle alongside a recorded timestamp T_1.

2) GENVEHPK PHASE

This phase executes the following steps.

- The vehicle verifies the timestamp T_1 from the fog server Fog_i.
- The vehicle computes PK_{v_2} as the following Equation 15.

$$PK_{v_2} = D_{i,2} \cdot PKV_{i,1}^{\omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))} \tag{1}$$

  where $D_{i,2}$ is fog server Fog_i's transmitted message; TID_v is the car's individual identification number; $\epsilon'(T_1)$ is the car's reliability rating at timestamp T_1.
- Lastly, the vehicle calculates session key SK as the following Equation 2.

$$SK = \epsilon'(PK_{v_2}, g) \tag{2}$$

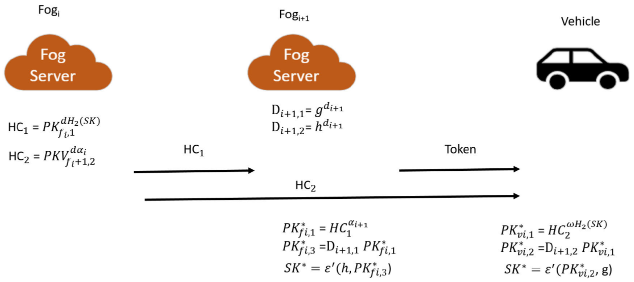
Fog$_i$
Fog Server
Fog$_{i+1}$
Fog Server
Vehicle
$HC_1 = PK_{f_{i,1}}^{dH_2(SK)}$
$HC_2 = PKV_{f_{i+1,2}}^{d\alpha_i}$
$D_{i+1,1} = g^{d_{i+1}}$
$D_{i+1,2} = h^{d_{i+1}}$
HC$_1$
Token
HC$_2$
$PK^*_{fi,1} = HC_1^{\alpha_{i+1}}$
$PK^*_{fi,3} = D_{i+1,1}\, PK^*_{fi,1}$
$SK^* = \varepsilon'(h, PK^*_{fi,3})$
$PK^*_{vi,1} = HC_2^{\omega H_2(SK)}$
$PK^*_{vi,2} = D_{i+1,2}\, PK^*_{vi,1}$
$SK^* = \varepsilon'(PK^*_{vi,2}, g)$

FIGURE 6. **Description of Vehicle to Fog server-handover authentication stage.**

3) GENFOGPK PHASE

This phase executes the following steps.

- The fog server Fog_i computes PK_{f_3} as the following Equation 3.

$$PK_{f_3} = D_{i,1} \cdot PK_{f,1}^{\omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{f_1}))} \tag{3}$$

  where $D_{i,1}$ is his own calculated secret message, TID_V is the vehicle's true identity, and $\epsilon'(T_1)$ is the vehicle's trustworthiness at timestamp T_1. The TL value is calculated via a scalable and trustworthy computing system. When a vehicle's immediate trustworthiness reaches zero, the fog server treats it as a revoked vehicle and stops providing its services. A revoked car cannot pretend to be a regular vehicle and communicate with the fog server since blockchain is tamer-resistant.
- Lastly, the fog server Fog_i calculates the session key SK as the following Equation 4.

$$SK = \epsilon'(h, PK_{f_3}) \tag{4}$$

C. HANDOVER AUTHENTICATION STAGE

This phase occurs when a vehicle leaves the signal coverage of one fog server and enters that of another, and it is performed by the system to provide a smooth transition of vehicle-to-infrastructure communication. The fog server initially verifies the vehicle's legitimacy via the blockchain. If the vehicle's reliability has not changed since it first accepted the previous fog server authentication until now, then the current fog server does not need to re-authenticate the reliability of the vehicle. The description of the vehicle to fog server-handover authentication stage is shown in Figure 6. Then, the procedures below will be put into effect.

1) GENHC PHASE

This phase executes the following steps.

- The fog server Fog_i runs this procedure to create a handover certificate (HC) for fog server Fog_{i+1} and the vehicle. Using the range $d \in Z_q^*$, fog server Fog_1 picks a random number. The formula for HC_1 is:

$$HC_1 = PK_{f_1}^{dH_2(SK)} \tag{5}$$

  where PK_{f_1} is determined by the GenKey phase (see Subsection IV-B1) and SK is the session key generated by GenFogPK phase (see Subsection IV-B3. A copy of HC_1 is transmitted to the Fog_{i+1} in the next tier of the system. So, here's how to figure out HC_2:

$$HC_2 = PKI_{i+1,2}^{\alpha_i d} \tag{6}$$

where $PKI_{i+1,2}$ is the portion of the Fog_{i+1} public key that was produced during the configuration process.

- Lastly, the fog server Fog_i sends HC_2 to vehicle via 5G-BS.

2) GENTOKEN PHASE

This phase executes the following steps.

- A value $d_i + 1$ is selected at random from the range Z_p^* when HC_2 is received from Fog_i.
- The fog server Fog_i computes the token $D_{i+1,2} = h^{d_i+1}$
- The fog server Fog_i sends the token to the vehicle via 5G-BS.

3) GENVEHPK2 PHASE

This phase executes the following steps.

- Once the vehicle obtains the token from Fog_{i+1} and HC_2 form the fog server Fog_i, the vehicle calculates $PK_{v_1}^*$ and $PK_{v_2}^*$ as the following Equation 7 and Equation16, respectively.

$$PK_{v_1}^* = HC_2^{\omega H_2(SK)} \tag{7}$$

$$PK_{v_2}^* = D_{i+1,2} \cdot PK_{v_1}^* \tag{8}$$

where $D_{i+1,2}$ is the token.

- Lastly, the vehicle computes SK^* as the following Equation 9.

$$SK^* = \epsilon'(PK_{v_2}^*, g) \tag{9}$$

4) GENFOGPK2 PHASE

This phase executes the following steps.

- The fog server Fog_{i+1} calculates $PK_{f_1}^*$ and $PK_{f_3}^*$ as the following Equation 10 and Equation11, respectively.

$$PK_{f_1}^* = HC_1^{\alpha_{i+1}} \tag{10}$$

$$PK_{f_3}^* = D_{i+1,1} \cdot PK_{f_1}^* \tag{11}$$

- Lastly, The fog server Fog_{i+1} computes SK^* as the following Equation 12.

$$SK^* = \epsilon'(h, PK_{f_3}^*) \tag{12}$$

V. SECURITY ANALYSIS

A. THE CORRECTION OF EQUATIONS

1) CORRECTNESS OF EQUATION 2

At this point, it's crucial that the fog server's and car's session keys match up, despite being generated independently. $SK = \epsilon'(PK_{v_2}, g)$, while $SK = \epsilon'(h, PK_{f_3})$ are the session keys generated by the vehicle and fog server, respectively. The evidence of correction Equation 2 is as follows:

$$\begin{aligned}
SK &= \epsilon'(PK_{v_2}, g) \\
&= \epsilon'(D_{i,2} \cdot PKV_{i,1}^{\omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))}, g) \\
&= \epsilon'(h^{d_i} \cdot h^{\alpha_i \omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))}, g) \\
&= \epsilon'(h, g^{d_i} \cdot g^{\alpha_i \omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))}) \\
&= \epsilon'(h, D_{i,1} \cdot PK_{v_1}^{\alpha_i \omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))}) \\
&= \epsilon'(h, D_{i,1} \cdot PK_{v_1}^{\alpha_i \omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))}) \\
&= \epsilon'(h, PK_{f_3})
\end{aligned} \tag{13}$$

The validity of this Equation 2 is demonstrated.

2) CORRECTNESS OF EQUATION 12

The next fog server and the vehicle must both arrive to the same session key at this point, but they must arrive at it independently. $SK^* = \epsilon'(PK_{v_2}^*, g)$ is the session key generated by the vehicle, while $SK^* = \epsilon'(h, PK_{f_3}^*)$ is the session key generated by the fog server. Here is how the evidence stacks up:

$$\begin{aligned}
SK^* &= \epsilon'(PK_{v_2}^*, g) \\
&= \epsilon'(D_{i+1,2} \cdot PK_{v_1}^*, g) \\
&= \epsilon'(h^{d_{i+1}} \cdot HC_2^{\omega H_2(SK)}, g) \\
&= \epsilon'(h^{d_{i+1}} \cdot PKV_{i+1,2}^{\alpha_i d \omega H_2(SK)}, g) \\
&= \epsilon'(h^{d_{i+1}} \cdot h^{\alpha_i+1\alpha_i d \omega H_2(SK)}, g) \\
&= \epsilon'(h, g^{d_{i+1}} \cdot g^{\alpha_i+1\alpha_i d \omega H_2(SK)}) \\
&= \epsilon'(h, D_{i+1,1} \cdot PK_{f_1}^*) \\
&= \epsilon'(h, PK_{f_3}^*)
\end{aligned} \tag{14}$$

This Equation 12 is also demonstrated to be correct.

B. SECURITY OF HAFC STAGES

This section evaluates the proposed HAFC scheme has been proven to be CDH-secure in G as the following substations.

1) SECURITY OF INITIAL AUTHENTICATION STAGE

Theorem 1: It proves CDH-security in G for the planned vehicle to fog server-initial authentication.

Proof. Based on our security model, attacker Att can access the car's storage and retrieve the GenKey-issued $PK_{v,1}$. Using the vehicle TID_v, the timestamp T_1 sent by the Fog_i, and the vehicular trustworthiness $\epsilon'(T_1)$ determined by the trustworthiness scalable computation, attacker Att can derive $H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v,1}))$, which can be verified in the blockchain. Both the value $D_{i,2}$ delivered by Fog_i and its public parameter $PKV_{v_i,2}$ are accessible to attacker Att.

If the attacker is able to determine the session key for this stage, he/she can then determine the value of $PK_{v,2}$. The following can be observed in the GenVehPK algorithm:

$$PK_{v_2} = D_{i,2} \cdot PKV_{i,1}^{\omega H_1(TID_v||T_1||(T_1)\epsilon'(T_1)||H_0(PK_{v_1}))} \tag{15}$$

where ω is some unknown parameter of the car that attacker Att does not know. That is, both the CDH issue and the DDH issue in G can be solved by c. Nonetheless, our security model makes it challenging to resolve the CDH problem and the DDH problem in G. Therefore, issue has a marginal edge in G_1 when calculating $g_1^{l_{i+1}-l_{i-1}^{l_i}}$.

Second, Fog_i conceals the value of $D_{i,1}$, which is required for Att to use algorithm GenFogPK to compute PK. In conclusion, the proposed HAFC scheme is CDH-secure in G_1 during the vehicle to fog server-initial authentication stage.

2) SECURITY OF HANDOVER AUTHENTICATION STAGE

Theorem 1: It proves CDH-security in G for the planned vehicle to fog server-handover authentication.

Proof. In our security paradigm, the Att is able to access the vehicle's storage and get the SK that was generated during the first phase during the handover procedure. With SK, A may determine $H_1(SK)$. The value $D_{i+1,2}$ that Fog_{i+1} transmitted can also be obtained via Att.

The opponent has to know the value of $PK_{v_i,2}$ in order to determine the session key for this phase. The GenVehPK2 algorithm shows that

$$PK_{v_2}^{*} = D_{i+1,2} \cdot PK_{v_1}^{*} \tag{16}$$

where $PK_{v_1}^{*} = HC_2^{\omega H_2(SK)}$. Att does not know the value of ω, which is a secret in the proposed HAFC scheme.

That is, both the CDH issue and the DDH issue in G can be solved by Att. Nonetheless, our security model makes it challenging to resolve the CDH issue and the DDH issue in G. Therefore, Att has a marginal edge in G_1 when calculating $g_1^{l_{i+1}-l_{i-1}^{l_i}}$.

Second, Fog_i conceals the value of $D_{i+1,1}$, which is required for Att to use algorithm GenFogPK2 to compute SK^*. In conclusion, the proposed HAFC scheme's vehicle to fog server-handover authentication stage is CDH-secure in G.

C. SECURITY ATTACK RESISTANCE

The proposed HAFC scheme is resist against the following security attacks.

- Reply Attack Resistance: Messages encrypted using SK by the car are vulnerable to reply attacks. The encrypted timestamp would be rendered useless and the data unauthenticable if the attacker delayed sending the encrypted data to the fog server through 5G-BS. The attacker's material will also fail authentication at the subsequent fog server if it is sent along with the authentication from the prior fog server. Because the session key generated by the vehicle and the subsequent fog server does not encrypt this information.
- Man-In-The-Middle (MITM) Attack Resistance: The Fog_i or Fog_{i+1}'s transmission could be intercepted by an MITM attacker. He/she might resend the message to the car if he decides to alter it. A session key will be produced by the car based on the tampered message if the vehicle receives a compromised $D_{I,2}$ and T_1. But, fog server will not verify the integrity of the session key produced with the altered setting.

TABLE 1. Comparison of computation overhead.

Items	Description
language	C
Operation system	Linux
Ubuntu Version	16.04 TLS
CPU	2.60 GHz Intel(R) Xeon(R) CPU E5-2650 v2
RAM	8 GB

VI. PERFORMANCE EVALUATION

In order to demonstrate the efficacy of the proposed HAFC scheme, simulations are run using the GNU Multiple Precision Arithmetic (GMP) library and the Pairing-Based Cryptography (PBC) library. Table 1 shows the specification hardware and software used in this experiment [32].

Time requirements of various algorithms when executed on various parts of the system are first simulated. Figure 7 depicts the results of a comparison simulation of seven phases: GenKey, GenVehPK, GenFogPK, GenHC, GenToken, GenVehPK2, and GenFogPK2. Among them, GenKey, GenVehPK, and GenFogPK are phases of the vehicle to fog server-initial authentication stage. The entire computation overhead of GenKey phase is 2.5 ms. The whole computation overhead of GenVehPK phase is 12.2 ms. The whole computation overhead of GenFogPK phase is 13.3 ms. While, the rests are phases of the handover authentication stage. The whole computation overhead of GenHC phase is 11.2 ms. The whole computation overhead of GenToken phase is 6.1 ms. The whole computation overhead of GenVehPK2 phase is 8 ms. The whole computation overhead of GenFogPK2 phase is 5.7 ms. Fog_i executes GenKey of fog server, GenFogPK, and GenHC. Fog_{i+1} executes GenToken and GenFogPK2. The vehicle executes the phases of GenKey, GenVehPK, and GenVehPK2. It's easy to understand how the handover phase costs far less than the launch phase for a vehicle. Vehicle-based operations also require less time investment than fog server-based ones.

Both the initial authentication phase and the handover authentication phase of vehicle to fog server are simulated in the proposed HAFC scheme to determine their respective time costs. The outcomes are depicted in Figure 8. The time investment in the planned overhand authentication step is cut in half as compared to the time needed for the primary authentication procedure. This is due to the fact that during the changeover phase of the HAFC scheme, the vehicle only needs to implement a few procedures based on the previous session key generated by the previous fog server. The handover between the retiring and serving fog servers performs some of the computational tasks.

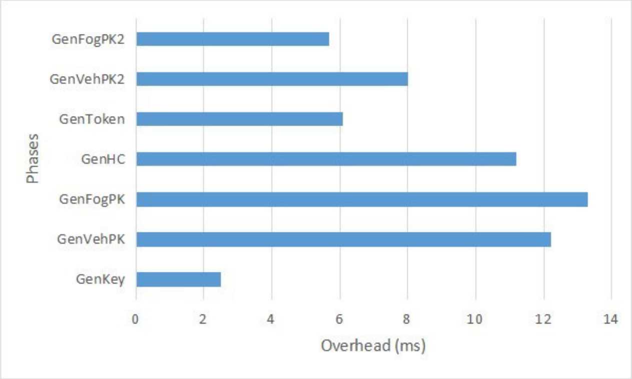

FIGURE 7. The proposed HAFC scheme phases' overhead comparison.

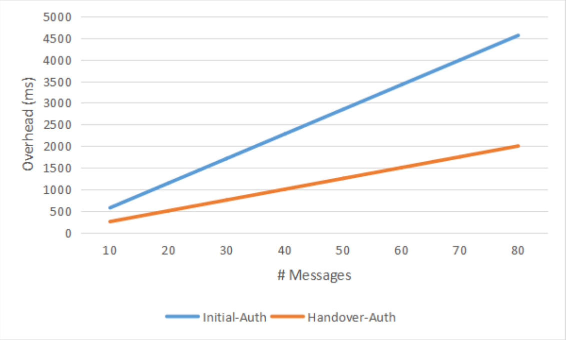

FIGURE 8. Overhead comparison of a vehicle among both stages.

VII. CONCLUSION AND FUTURE WORK

This paper has proposed a handover authentication, called HAFC scheme based on fog computing for 5G-assisted vehicular blockchain networks. The proposed HAFC scheme consists of both stages namely, initial-authentication stage (the generation of key (GenKey), generation of private key (GenVehPK) for vehicle, and generation of private key (GenFogPK) for fog server) and handover-authentication stage (generation of handover certificate (GenHC), generation of token (GenToken), generation of private key2 (GenVehPK2) for vehicle, generation of private key2 (GenFogPK2) for fog server). Fog_i executes GenKey of fog server, GenFogPK, and GenHC. Fog_{i+1} executes GenToken and GenFogPK2. The vehicle executes the phases of GenKey, GenVehPK, and GenVehPK2. In the subsection of security analysis, the validity of these equations used are demonstrated. In conclusion, the proposed HAFC scheme is CDH-secure in G_1 during the vehicle to fog server-initial authentication stage. Meanwhile, the proposed HAFC scheme's vehicle to fog server-handover authentication stage is CDH-secure in G. The proposed HAFC scheme is resist against the reply and MITM attacks. Finally, the performance evaluation of the proposed HAFC scheme, the time required for the handover authentication stage was found to be half that of the first authentication.

In future work, the proposed solution will expanded to evaluate the performance of proposed algorithm and compare it with comparative schemes in terms of communication costs, computation costs, power consumption costs. Meanwhile, the lattice algorithm should be implement to address quantum attacks.

ACKNOWLEDGMENT

The authors would like to acknowledge the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, for funding this research through project number ((RG-23 116)).

REFERENCES

[1] L.-M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, "Deployment of IoV for smart cities: Applications, architecture, and challenges," *IEEE Access*, vol. 7, pp. 6473–6492, 2019.

[2] T. Limbasiya and D. Das, "IoVCom: Reliable comprehensive communication system for Internet of Vehicles," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 6, pp. 2752–2766, Nov. 2021.

[3] N. Gupta, A. Prakash, and R. Tripathi, "Medium access control protocols for safety applications in vehicular ad-hoc network: A classification and comprehensive survey," *Veh. Commun.*, vol. 2, no. 4, pp. 223–237, Oct. 2015.

[4] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[5] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[6] S.-B. Lee, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2715–2728, Jul. 2012.

[7] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[8] 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.

[9] A. Bazzi, A. O. Berthet, C. Campolo, B. M. Masini, A. Molinaro, and A. Zanella, "On the design of sidelink for cellular V2X: A literature review and outlook for future," *IEEE Access*, vol. 9, pp. 97953–97980, 2021.

[10] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.

[11] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of Vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[12] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2015.

[13] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun.*, Apr. 2008, pp. 246–250.

[14] J. Qi, T. Gao, X. Deng, and C. Zhao, "A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs," *Veh. Commun.*, vol. 38, Dec. 2022, Art. no. 100535.

[15] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, Feb. 2019.

[16] 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.

[17] X. Liu, Y. Wang, Y. Li, and H. Cao, "PTAP: A novel secure privacy-preserving & traceable authentication protocol in VANETs," *Comput. Netw.*, vol. 226, May 2023, Art. no. 109643.

[18] Y. Cao, S. Xu, X. Chen, Y. He, and S. Jiang, "A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios," *Comput. Netw.*, vol. 214, Sep. 2022, Art. no. 109149.

[19] A. Jain, J. Singh, S. Kumar, Ţ. Florin-Emilian, M. T. Candin, and P. Chithaluru, "Improved recurrent neural network schema for validating digital signatures in VANET," *Mathematics*, vol. 10, no. 20, p. 3895, Oct. 2022.

[20] B. Samra and S. Fouzi, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET," *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100414.

[21] S. Chen, Y. Liu, J. Ning, and X. Zhu, "BASRAC: An efficient batch authentication scheme with rule-based access control for VANETs," *Veh. Commun.*, vol. 40, Apr. 2023, Art. no. 100575.

[22] T. Wang, L. Kang, and J. Duan, "A secure access control scheme with batch verification for VANETs," *Comput. Commun.*, vol. 205, pp. 79–86, May 2023.

[23] C. Maurya and V. K. Chaurasiya, "Efficient anonymous batch authentication scheme with conditional privacy in the Internet of Vehicles (IoV) applications," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–14, 2023.

[24] N. Gupta, R. Manaswini, B. Saikrishna, F. Silva, and A. Teles, "Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET," *Future Internet*, vol. 12, no. 4, p. 63, Apr. 2020.

[25] V. O. Nyangaresi, A. J. Rodrigues, and S. O. Abeka, "Efficient group authentication protocol for secure 5G enabled vehicular communications," in *Proc. 16th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2020, pp. 25–30.

[26] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PLoS ONE*, vol. 15, no. 2, Feb. 2020, Art. no. e0228319.

[27] B. Al-Otaibi, N. Al-Nabhan, and Y. Tian, "Privacy-preserving vehicular rogue node detection scheme for fog computing," *Sensors*, vol. 19, no. 4, p. 965, Feb. 2019.

[28] K. Han, M. Ma, X. Li, Z. Feng, and J. Hao, "An efficient handover authentication mechanism for 5G wireless network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.

[29] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 12, pp. 1913–1922, Dec. 2021.

[30] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2020.

[31] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Feb. 2021.

[32] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Jul. 2021.

BADIEA ABDULKAREM MOHAMMED (Senior Member, IEEE) received the B.Sc. degree in computer science from Babylon University, Iraq, in 2002, the M.Tech. degree in computer science from the University of Hyderabad, India, in 2007, and the Ph.D. degree from Universiti Sains Malaysia, Malaysia, in 2018. He is currently an Assistant Professor with the College of Computer Science and Engineering, University of Ha'il, Saudi Arabia. He is permanently an Assistant Professor with Hodeidah University, Yemen. His research interests include wireless networks, mobile networks, vehicle networks, WSN, cybersecurity, and image processing. In his research area, he has published many papers in reputed journals and conferences. He is an IAENG Member and an ASR Member.

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

ZEYAD GHALEB AL-MEKHLAFI received the B.Sc. degree in computer science from the University of Science and Technology, Yemen, in 2002, the M.Sc. degree in computer science from the Department of Communication Technology and Network, Universiti National Malaysia (UKM), in 2011, and the Ph.D. degree from the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in 2018. He is currently a Lecturer with the University of Ha'il, where he is also an Assistant Professor with the Faculty of Computer Science and Engineering. His current research interests include wireless sensor networks, energy management and control for wireless networks, time synchronization, bio-inspired mechanisms, and emerging wireless technologies standards.

JALAWI SULAIMAN ALSHUDUKHI received the B.Sc. degree in computer science from the University of Ha'il, Saudi Arabia, in 2002, the M.Sc. degree in computer networks from La Trobe University, Australia, in 2010, and the Ph.D. degree from Oxford Brookes University, U.K., in 2016. He is currently an Assistant Professor with the College of Computer Science and Engineering, University of Ha'il. His current research interests include wireless sensor networks, energy management and propagation models, WSNs MAC protocol, and intelligent transportation systems.

KAWTHER A. AL-DHLAN is currently a Professor of computer science. She has 13 years of experience in data science and more than 27 years in academic fields. She also teaches with the University of Ha'il, Saudi Arabia. Moreover, she is interested in many branches of CS, such as security, cloud computing, and deep learning.