IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 6 February 2023, accepted 17 February 2023, date of publication 22 February 2023, date of current version 27 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3247222

RESEARCH ARTICLE

FC-PA: Fog Computing-Based Pseudonym Authentication Scheme in 5G-Enabled Vehicular Networks

BADIEA ABDULKAREM MOHAMMED[1], (Senior Member, IEEE), MAHMOOD A. AL-SHAREEDA[2], SELVAKUMAR MANICKAM[2], ZEYAD GHALEB AL-MEKHLAFI[1], ABDULRAHMAN ALRESHIDI[1], MESHARI ALAZMI[1], JALAWI SULAIMAN ALSHUDUKHI[1], AND MOHAMMAD ALSAFFAR[1]

[1]College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia
[2]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang 11800, Malaysia

Corresponding authors: Mahmood A. Al-Shareeda (alshareeda022@usm.my) and Selvakumar Manickam (selva@usm.my)

This work was supported by the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, under Project RG-21 082.

ABSTRACT The fifth-generation (5G) technology-enabled vehicular network has been widely used in intelligent transportation in recent years. Since messages shared among vehicles are always broadcasted by openness environment' nature, which is vulnerable to several privacy and security problems. To cope with this issue, several researchers have proposed pseudonym authentication schemes for the 5G-enabled vehicular network. Nevertheless, these schemes applied complected and time-consumed operations. Therefore, this paper proposes a fog computing-based pseudonym authentication (FC-PA) scheme to decrease the overhead of performance in 5G-enabled vehicular networks. The FC-PA scheme applies only one scalar multiplication operation of elliptic curve cryptography to prove information. A security analysis of our work explains that our scheme satisfies privacy-preserving and pseudonym authentication, which are resilient against common security attacks. With performance efficiency, our work can obtain better trade-offs between efficiency and security than the well-known recent works.

INDEX TERMS Fog computing, vehicular networks, 5G, privacy-preserving, authentication.

I. INTRODUCTION

With the essential increase in vehicle ownership, a lot of scholars have been done to assist passengers and drivers. As a result, the significance of promoting traffic efficiency and safety is more and more advertised [1], [2], [3]. Recently, the fifth-generation (5G) technology-enabled vehicular network has paid attention from industry and academic [4], [5], [6].

In general, an intelligent vehicle equipped with a wireless device called, an onboard unit (OBU) to share traffic messages among others [7], [8]. This message includes road conditions, traffic status, current time, speed, direction, and so on. Thus, the 5G-enabled vehicular network provides the best solution and obtains better awareness of traffic data for vehicles.

Direct connection between two mobile users in a cellular network, bypassing the base station (BS) and the core network, is referred to as device-to-device (D2D) communication [9], [10], [11]. Even if a device is within direct line of sight (D2D) range, communications in a traditional cellular network must first travel through the BS. Traditional low data rate mobile services can make use of BS communication because users are rarely in a position where they can directly address one other. Mobile customers in modern mobile networks, however, make use of high data rate services even though they may be out of direct communication range [12], [13], [14]. As a result, D2D communication in this scenario can significantly enhance the network's spectral efficiency. Beyond spectral efficiency, D2D communication benefits

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

may also include enhanced throughput, energy efficiency, latency, and fairness [15], [16], [17].

The limitations of current cloud computing methods become apparent in situations where there is a significant influx of data. The term ''fog computing'' was first used in the IoT context by Shi et al. [18], [19]. Industrial Internet of Things (IoT) is just one latency-sensitive application space where edge or fog computing is gaining traction and adoption [7], [20]. Some typical cloud services can be moved to the fog node of the network, which can have some beneficial consequences such as improved offloading, lower latency, and so on [21] and [22].

Messages are always broadcasted by openness environment' nature and are vulnerable to several privacy and security problems. Thus before to deployment of a promising 5G-enabled vehicular network, the privacy and security problems should be addressed [23], [24], [25].

Several research has proposed pseudonym authentication schemes to address privacy and security problems for vehicular networks. However, these schemes use the map-to-point function, bilinear pair operation, and elliptic curve operation (ECC), which these operations are considered complected and time-consumed operations. Therefore, this paper proposes a fog computing-based pseudonym authentication (FC-PA) scheme in 5G-enabled vehicular networks. The major contributions are as follows:

- In this paper, we propose an efficient FC-PA scheme by utilizing elliptic curve cryptography and general hash function to provide privacy-preserving and security.
- We present the security analysis of our work that the ECDL problem is hardness in the random oracle model to achieve security requirements in a 5G-enabled vehicular network.
- We evaluate in detail the performance of the FC-PA scheme concerning communication and computational costs. We show that our work is more efficient in the message signing and signature verification phases.

The remainder of this paper is arranged as follows. In Section II, we present the most recent pseudonym authentication schemes. The system model and design objectives are provided in Section III. We propose an FC-PA scheme for secure vehicular networks in Section IV. Section V provides security analysis while the performance efficiency is described in Section VI. Lastly, Section VII introduces the conclusions of this paper.

II. RELATED WORK

In vehicular networks, privacy and security issues have attracted vigorous research and insertion from academia and industry. In recent years, lots of pseudonym authentication schemes for vehicular networks have been put forward roughly to achieve privacy-preserving and security requirements as follows.

Pournaghi et al. [26] designed an authentication scheme by preserving the system's private key in each participated roadside unit (RSU). While Bayat et al. [27] designed a practical authentication scheme by preserving the system's private key into each participated vehicle provided by the RSU. Bayat et al. [28] constructed an authentication scheme without using the tamper-proof device (TPD), signers group, and online RSU. Ali and Li [29] designed a signature scheme to support the batch verification process for reducing the computational overhead on the RSU in high density with traffic areas. Al-Shareeda et al. [30] constructed a pseudonym authentication method to withstand impersonation attacks by frequently updating the vehicle's true identity. However, these schemes [26], [27], [28], [29], [30] employ the bilinear pair operations, which considers time-consuming and completed. Additionally, these schemes [26], [27], [28] use the map-to-point function to sign and verify messages. Thus, these schemes [29], [30] use a general hash function rather than a map-to-point function to reduce the overhead of the system with regard to communications and computational costs.

To avoid utilizing the complected operation in terms of map-to-point function and bilinear pair, several researchers have proposed an authentication scheme by using elliptic curve cryptography (ECC) and a general hash function to sign and verify messages shared among vehicles. Cui et al. [31] proposed a message authentication method according to the reputation system for joining in the communication by testing the reputation score of the vehicle. Cui et al. [12] designed a content-sharing scheme to pick proxy vehicles to get saving network traffic, valid hit ratio, and congestion of easing, and minimize time delay during peak hours for 5G-enabled vehicular networks. Zhang et al. [21] designed edge computing-based authentication by using a fuzzy logic mathematical method to authenticate between ordinary vehicles and edge computing for 5G-enabled vehicular networks. Alshudukhi et al. [32] designed a lightweight authentication scheme by preserving the system's master key in each TPD of RSU rather than in the TPD of OBU to achieve privacy-preserving and security properties. Al-Shareeda et al. [33] proposed an authentication scheme to address password-guessing attacks for 5G-enabled vehicular networks.

However, the existing schemes [12], [21], [31], [32], [33] employ a large number of ECC operations (scalar operation) for signature verification operations, which causes high computational costs, especially in high density with traffic area. Since the computational process of OBU is low than other rest of the participants, lightweight cryptography operations should be used to sign and verify messages.

To address the above issues, we propose a fog computing-based pseudonym authentication (FC-PA) scheme in 5G-enabled vehicular networks. This work uses ECC instead of bilinear pair operation to address the communication and computational costs issue in [26], [27], [28], [29], and [30]. Besides, unlike the schemes in [12], [21], [31], [32], and [33], the proposed FC-PA scheme uses only one ECC-based operation to verify messages shared among vehicles.

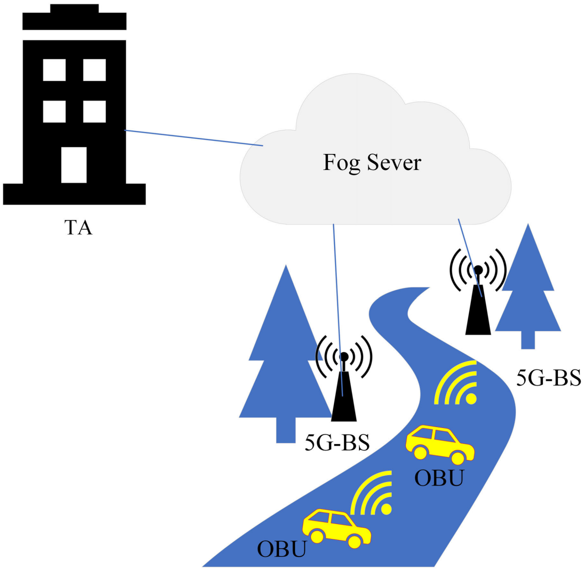

FIGURE 1. System Model of our Work for 5G-enabled Vehicular Fog Computing.

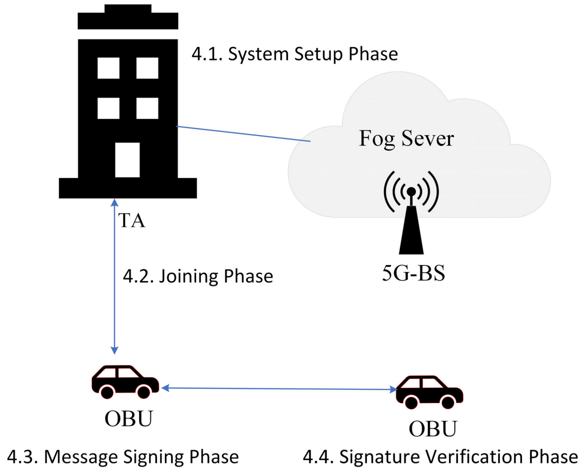

FIGURE 2. Phases of our Proposal.

III. BACKGROUND

In this section, the background of our FC-PA work is provided concerning the system model as well as design objectives as the following.

A. SYSTEM MODEL

There are four participants included in 5G-enabled vehicular fog computing. These participants are namely, 5G-base station (5G-BS), trusted authority (TA), fog server, and onboard unit (OBU). Figure 1 depicts the system model of our work.

- Trusted Authority (TA): The TA is trustworthy with capabilities of storage and major computation power than the rest of the participants. The TA enrolls the fog server and OBU joining the 5G-enabled vehicular network as well as preloads public parameters to the vehicle to secure communication.
- Fog Server: Based on our work, it supposes that the fog server has capabilities of storage and some computation of verification. The TA preserves its master key in the fog server to validate the vehicles during joining steps via 5G-BS.
- 5G-Base Station (5G-BS): The 5G-BS is a base station equipped along the roadside that helps as intermediate participants between the TA, fog server, and vehicles. The 5G-BS does not do any computational and storage operations.
- Onboard Unit (OBU): Each vehicle is installed in wireless devices, onboard Unit (OBU), to exchange information about road status among vehicles.

B. DESIGN OBJECTIVES

The main aim of design objectives is that our work will be archived the security requirements as the following steps.

- Authentication and Integrity: The receiver can verify that the transmission has not been manipulated and that the data was sent from a legitimate source.
- Conditionality: It is important to keep the vehicle's genuine identity hidden when transmitting to other vehicles on the road. Their privacy will be protected, and no outsider will be able to use their identities.
- Traceability: If a forged communication is created, the source and authority behind it must be determined using the TA.
- Resistance Against Security Attacks: Several distinct types of assaults exist, including replay, impersonation, modification, and man-in-the-middle.

IV. PROPOSED SCHEME

Our work comprises four phases namely, System Setup Phase, Joining Phase, Message Signing Phase, and Signature Verification Phase, as shown in Figure 2.

A. SYSTEM SETUP PHASE

The system's parameters are partially provided by this stage. TA must build the following procedures:

- TA constructs two large primes p and q. It defines a non-singular elliptic curve as the following equation.

$$y^2 = x^3 + ax + bmodp \tag{1}$$

  The above equation is over a prime field F_p, where a, b $\in F_p$.
- TA selects a point $P \in E(F_p)$ of order q which is the generator of the group based on additive cyclic which includes all points according to E with the point at infinity Ø.
- TA constructs three secure general hash functions $h_1(\cdot)$, $h_2(\cdot)$ and $h_3(\cdot)$ as $h_1 : G \to Z_q^*$ $h_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \to Z_q^*$ $h_3 : \{0, 1\}^* \to Z_q^*$.
- TA constructs its private key s selecting randomly from Z_q^* and the corresponding public key as $Pub_{TA} = s \cdot P$.

- TA protects its private key s into each fog server secretly.
- Finally, TA transmits the system parameters $\{p, q, P, G, Pub_{TA}, h_1, h_2, h_3\}$ to all fog servers and vehicles in 5G-enabled vehicular fog computing.

B. JOINING PHASE

This phase contributes to achieving a method of mutual authentication between the vehicles and the TA over fog servers. The 5G-BS is responsible to provide communication between the fog server and vehicles, as shown in Figure 3. This phase constructs the following steps:

- Vehicle: The vehicle v_i constructs the private value μ selecting randomly from Z_q^* and computes the public pseudonym-IDs $PPID_i$ as the following equation, where TID_i is the true identity of vehicle.

$$\begin{aligned} PPID_i &= \langle PPID_i^1, PPID_i^2 \rangle \\ PPID_i^1 &= \mu \cdot P \\ PPID_i^2 &= TID_i \oplus h_1(\mu \cdot Pub_{TA}) \end{aligned} \tag{2}$$

- Vehicle $\rightarrow$ fog server: The vehicle v_i sets and sends the messages session $\{PPID_i^1, PPID_i^2, T_1, \delta_{V2F}\}$ to fog server Fog_j, where $\delta_{V2F} = h_2(PPID_i^1||PPID_i^2||TID_1||T_i)$ and T_i is a freshness timestamp to avoid replay attacks.
- Fog server: Upon receiving the messages joining $\{PPID_i^1, PPID_i^2, T_1, \delta_{V2F}\}$, the fog server Fog_j initially tests the freshness of timestamp T_1 as Equation 3, where T_r is the receiving time and $\triangle$ is the predefined time. If Equation 3 holds, the fog server Fog_j continues the process; otherwise, the fog server Fog_j discards the message joining.

$$\triangle \geq T_r - T_1 \tag{3}$$

- Fog server: The fog server Fog_j uses TA's private key s to reveal the vehicle's true identity TID_i as the following equation.

$$TID_i = PPID_i^2 \oplus h_1(s \cdot PPID_i^1) \tag{4}$$

- Fog server: The fog server Fog_j checks the integrity of message joining $\{PPID_i^1, PPID_i^2, T_1, \delta_{V2F}\}$ by matching the signature as Equation 5. If Equation 5 holds, the fog server Fog_j continues the process; otherwise, the message joining will be discarded.

$$\delta_{V2F}^{-} \stackrel{?}{=} \delta_{V2F} \stackrel{?}{=} h_2(PPID_i^1||PPID_i^2||TID_1||T_i) \tag{5}$$

- Fog server: The fog server Fog_j tests the vehicle's true identity TID_i on the certificate revocation list (CRL) which is sent by TA to ensure that the vehicle is not blocked.
- Fog server: Upon TID_i is legal, the fog server Fog_j constructs $\alpha_i = h_2(PPID_i^1||PPID_i^2||Pub)$. Then the fog server Fog_j chooses randomly the value $\beta_i \in Z_q^*$ to compute and broadcast its public key as $Pub_{fog} = (\beta_i + \alpha_i)P$. Finally, the fog server Fog_j computes the signature key as $SK_i = \frac{\beta_i + \alpha_i}{s} mod q$
- Fog server $\rightarrow$ Vehicle: the fog server Fog_j sends $\{SK_{en}, T_2, \delta_{F2V}\}$ to the vehicle v_i, where $Sk_{en} = SK_i \oplus h_2(TID_1||T_2)$ and $\delta_{F2V} = h_2(SK_{en}||T_2||TID_1)$.
- Vehicle: The vehicle v_i initially tests the freshness of timestamp T_2. If it is valid, the vehicle v_i computes the signature key as $SK_i = Sk_{en} \oplus h_2(TID_1||T_2)$ and checks the integrity of message as $\delta_{F2V}^{-} = \delta_{F2V} = h_2(SK_{en}||T_2||TID_1)$.

C. MESSAGE SIGNING PHASE

This phase contributes to signing the message Msg_i exchanged among vehicles, as shown in Figure 4. This phase constructs the following steps:

- The vehicle v_i signs the message Msg_i by calculating $\sigma_i = h_3(PPID_i^1||PPID_i^2||Msg_i||Pub_{Fog}||Pub_{TA}||T_i)$, where T_i is the time validity.
- The vehicle v_i constructs randomly the value $z_i \in Z_q^*$ and computes $U_i = z_i \cdot \sigma_i \cdot Pub_{TA}$ and $R_i = (Sk_i + z_i \cdot \sigma_i)$ mod q. Then the vehicle v_i sets the signature as $\delta_i = (R_i, U_i)$.
- Finally, the vehicle v_i transmits the tuple $(PPID_i, T_i, Msg_i, \delta_i)$ to the nearby vehicles in 5G-enabled vehicular fog computing.

D. SIGNATURE VERIFICATION PHASE

This phase contributes to verifying the validity and authenticity of the tuple $(PPID_i, T_i, Msg_i, \delta_i)$ sent from vehicles in 5G-enabled vehicular fog computing. Two types of verification can occur during this stage: single-signature verification and batch-signature verification.

1) SINGLE-SIGNATURE VERIFICATION

It means that each vehicle in 5G-enabled vehicular fog computing checks one signature at a time, as shown in Figure 4. This method constructs the following steps:

- Upon receiving the tuple $(PPID_i, T_i, Msg_i, \delta_i)$ from the vehicle v_i, the verifier vehicle v_j initially tests the newness of the timestamp T_i as Equation 6, where T_r is the receiving time and $\triangle$ is the predefined time.

$$\triangle \geq T_r - T_i \tag{6}$$

- If T_i is valid, then the vehicle v_j can pass the authentication method further. The vehicle v_j accepts the message Msg_i, if Equation 7 holds. Otherwise, the data is discarded by the user v_j.

$$\begin{aligned} R_i \cdot Pub_{TA} &= (Sk_i + z_i \cdot \sigma_i) \cdot Pub_{TA} \\ &= Sk_i \cdot Pub_{TA} + z_i \cdot \sigma_i \cdot Pub_{TA} \\ &= \frac{\beta_i + \alpha_i}{s} \cdot Pub_{TA} + z_i \cdot \sigma_i \cdot Pub_{TA} \\ &= \frac{\beta_i + \alpha_i}{s} \cdot s \cdot P + z_i \cdot \sigma_i \cdot Pub_{TA} \\ &= (\beta_i + \alpha_i) \cdot P + z_i \cdot \sigma_i \cdot Pub_{TA} \\ &= Pub_{Fog} + z_i \cdot \sigma_i \cdot Pub_{TA} \\ &= Pub_{Fog} + U_i \end{aligned} \tag{7}$$

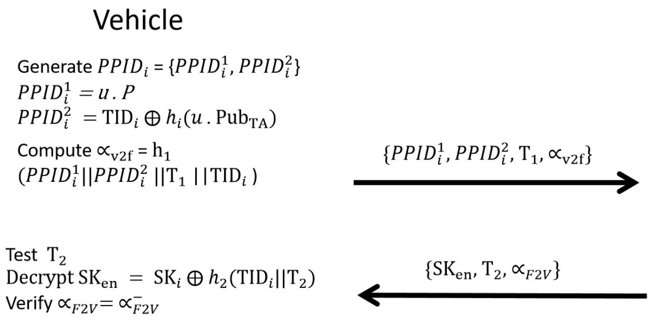

FIGURE 3. **Joining Process.**

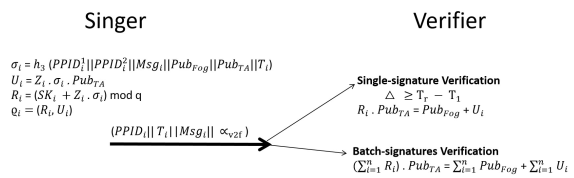

FIGURE 4. **Message Signing and Verification Process.**

2) BATCH-SIGNATURES VERIFICATION

It means that is each vehicle in 5G-enabled vehicular fog computing checks multiple signatures simultaneously, as shown in Figure 4. Upon receiving the tuples $(PPID_i{}^1, T_i{}^1, Msg_i{}^1, \delta_i{}^1)$, $(PPID_i{}^2, T_i{}^2, Msg_i{}^2, \delta_i{}^2)$, $(PPID_i{}^3, T_i{}^3, Msg_i{}^3, \delta_i{}^3)$,…,$(PPID_i{}^n, T_i{}^n, Msg_i{}^n, \delta_i{}^n)$ from the vehicles v_i, where i=1, 2, 3,…,n, this method constructs the following steps:

- The verifier vehicle v_j firstly checks the newness of timestamps as Equation 6 to avoid reply attacks.
- The vehicle v_j accepts the message Msg_i, if Equation 8 holds. Otherwise, the message is discarded by the vehicle v_j.

$$
\begin{aligned}
&(\sum_{i=1}^{n} R_i) \cdot Pub_{TA} \\
&\quad = (\sum_{i=1}^{n} (Sk_i + z_i \cdot \sigma_i)) \cdot Pub_{TA} \\
&\quad = (\sum_{i=1}^{n} Sk_i) \cdot Pub_{TA} + (\sum_{i=1}^{n} z_i \cdot \sigma_i) \cdot Pub_{TA} \\
&\quad = (\sum_{i=1}^{n} \frac{\beta_i + \alpha_i}{s}) \cdot Pub_{TA} + (\sum_{i=1}^{n} z_i \cdot \sigma_i) \cdot Pub_{TA} \\
&\quad = (\sum_{i=1}^{n} \frac{\beta_i + \alpha_i}{s} \cdot s \cdot P) + (\sum_{i=1}^{n} z_i \cdot \sigma_i) \cdot Pub_{TA} \\
&\quad = (\sum_{i=1}^{n} (\beta_i + \alpha_i)) \cdot P + (\sum_{i=1}^{n} z_i \cdot \sigma_i) \cdot Pub_{TA} \\
&\quad = \sum_{i=1}^{n} Pub_{Fog} + (\sum_{i=1}^{n} z_i \cdot \sigma_i) \cdot Pub_{TA} \\
&\quad = \sum_{i=1}^{n} Pub_{Fog} + \sum_{i=1}^{n} U_i \qquad (8)
\end{aligned}
$$

V. SECURITY ANALYSIS

This section analyzes the security of our work concerning the random oracle model (ROM) and security requirements as detailed in the following sections.

A. RANDOM ORACLE MODEL (ROM)

This section contributes to proving the security of our FC-PA work for 5G-enabled vehicular fog computing.

Theorem 1: The FC-PA system is protected from existential forgery under chosen message attack in the random oracle model. According to negligible probability ε, it there occur a third party TP posting has queries q_{h_2} and q_{h_3} to h_2 and h_3 oracle respectively, queries of key extraction q_{key} and queries of signature q_{sk} and resolve problem of ECDL in time t^- such that $t^- \leqslant \kappa t \frac{q_{h_2} q_{h_3}}{\varepsilon}$, where $\kappa = 12068$ for $\varepsilon 10(q_{sk}+1)(q_{h_2}+q_{h_3}, q_{key}+q_{sk})$.

Proof: This paper uses the forking lemma [34] to show the security inserting similar process utilized in the signature authentication method proposed in [34]. The third party TP tacks the problem of ECDL instances $(P, \eta P) \in G$ as a challenge, where $\eta \in Z_q^*$. Note that the third party TP utilizes challenger ϱ as a subroutine to resolve the problem of ECDL in the additive group G to calculate η with non-negligible probability. This process is played among the third party TP and the challenger ϱ. The third party TP executes the queries as follows.

- Setup: The challenger ϱ executes the Setup algorithm to issue the global system parameters for generating the private key s and the public key Pub_{TA}. These parameters are transmitted to the third party TP.
- Oracle (h_2): The challenger ϱ preserves a list L_{h_2} to save the tuple $\{PPID_i, R_i, \alpha_i, T_i\}$. The third party TP posts the queries on $(PPID_i, R_i, T_i)$ to h_2 oracle, the challenger ϱ finds the entry $(PPID_i, R_i, T_i)$ in the list L_{h_2}, if it is exist then ϱ transmits the tuple $\{PPID_i, R_i, \alpha_i, T_i\}$ to the third party TP, otherwise selects randomly a value $\alpha_i \in Z_q^*$, insert this number and include the new tuple $\{PPID_i, R_i, \alpha_i, T_i\}$ to L_{h_2}.
- Oracle (h_3): The challenger ϱ preserves an another list L_{h_3} to save the tuple $\{PPID_i^1, PPID_i^2, Msg_i, Pub_{Fog}, Pub_{TA}, T_i\}$. Firstly it is empty. The third party TP posts the queries on the tuple $\{PPID_i^1, PPID_i^2, Msg_i, Pub_{Fog},$

$Pub_{TA}, T_i\}$ to h_3 oracle. The challenger ϱ finds the entry in the list L_{h_3}, if it exists then ϱ transmits δ_i to TP, otherwise selects randomly a hash value $\delta_i \in Z_q^*$ and sends it to the third party TP. Then the challenger ϱ updates the list L_{h_3}.

- Key extraction Oracle: The third party TP posts the queries with public pseudonym-ID $PPID_i$ to the key generation oracle. The challenger ϱ selects randomly value $\omega_i \in Z_q^*$ and calculates $R_i = \omega_i \cdot P$ and finds the tuple $\{PPID_i, R_i, T_i\}$ in the list L_{h_2}. If it does not exist, then the challenger ϱ discards the queries and returns another message. Otherwise ϱ calculates the public key $\theta_i = R_i + \alpha_i \cdot Pub_{TA}$ and the private key as $\mu_i = \omega_i + \sigma_i smodq$. So the pair of keys issued as (θ_i, μ_i). Note that, the third party TP does not return the private key μ_i for the challenged public pseudonym-ID $PPID_i^-$ in the posted query $PPID_i^-$.
- Signing Oracle: The third party TP posts the queries with public pseudonym-ID $PPID_i$ to the signing oracle on the message Msg_i, the challenger ϱ finds the entry $\{PPID_i, R_i, \alpha_i, T_i\}$ in L_{h_2} and returns α_i and chooses randomly value z_i and sets $d_i = z_i P$. The challenger ϱ calculates $\theta_i = R_i + \alpha_i \cdot Pub_{TA}$, $W_i = z^{-1}(x_i - y_i)P$ and $R_i = y_i P$. Lastly, the result is the signature (R_i, W_i, δ_i). The verification can be executed by calculating the hashed value $h_3(PPID_i^1||PPID_i^2||Msg_i||Pub_{Fog}||Pub_{TA}||T_i)$ and matches with δ_i and the answer to the signing query is true. The challenger ϱ sends the signature $\delta_i = R_i, W_i, \delta_i$ to the third party TP. The challenger ϱ inserts the tuple $\{PPID_i^1, PPID_i^2, Msg_i, Pub_{Fog}, Pub_{TA}, T_i\}$.

Therefore, the third party TP can build a legal signature δ_i on a chosen message Msg_i^- anytime. Adopting the forking lemma, when the challenger ϱ replies to the signing queries with the same random value with distinct $z_i \neq z_i$, the third party TP issues two distinct signature $\delta_i^- = R_i^-, W_i^-, \delta_i^-$ and $\delta_i^* = R_i^*, W_i^*, \delta_i^*$. So

$$R_i^- = \mu_i z_i^- + \sigma_i modq \tag{9}$$
$$R_i^* = \mu_i z_i^* + \sigma_i modq \tag{10}$$

The challenger ϱ resolves the problem of ECDL and returns the private key μ_i from the given signatures R_i^- and R_i^*. Utilizing Equation 9 and 10, it can be concluded.

$R_i^- - R_i^* = (\mu_i z_i^- - \mu_i z_i^*)modq$. This implies $mu_i = \frac{R_i^- - R_i^*}{z_i^- - z_i^*} modq$

Thus the challenger ϱ can resolves the problem of ECDL with the time $t^- \leqslant \kappa t \frac{q_{h_2} q_{h_3}}{\varepsilon}$, where $\kappa = 12068$ for $\varepsilon 10(q_{sk}+1)(q_{h_2}+q_{h_3}, q_{key}+q_{sk})$. This game proves that the problem of ECDL is infeasible to resolve. For this reason, our solution satisfies the requirement of existential unforgeability against the agreement assault.

B. SECURITY REQUIREMENTS

The FC-PA work should be achieved the essential security requirements as follows.

- Authentication and Integrity: To make sure that the singer and validity of a message before accepting it, the proposed FC-PA work checks the signature attached to the tuple sent and only accepts the messages that achieve $\sigma_i^- = \sigma_i$, where σ_i^- is calculated by analyzing the hashed value $h_3(PPID_i^1||PPID_i^2||Msg_i||Pub_{Fog}||Pub_{TA}||T_i)$. Therefore, our work archives the authentication and integrity requirements for 5G-enabled vehicular fog computing.
- Confidentiality: To achieve confidentiality, our work generates two random values s and μ as $Pub_{TA} = s \cdot P$ and $PPID_i^1 = \mu \cdot P$, respectively. Once a third party attempts to obtain the vehicle's true identity TID_i from aid, he/she cannot do without these two random values as $TID_i = PPID_i^2 \oplus h_1(s \cdot PPID_i^1)$. Thus, it becomes a hardness problem. Therefore, our work archives the confidentiality requirement for 5G-enabled vehicular fog computing.
- Traceability: The TA will be able to identify and then shut down any maliciously registered vehicle that is trying to send out forged messages or otherwise interfere with the system's normal operation. In response to the forging message, the car communicates with the TA through 5G-BS. The TA verifies its aid and if valid in the list registration as $TID_i = PPID_i^2 \oplus h_1(s \cdot PPID_i^1)$ utilizing the private key s of the system. The TA can then revoke access by incorporating the new list into all active fog servers. Our research also documents the need for auditability in vehicle fog computing provided by 5G.
- Resistance Against Replay Attack: Our work can avert replay attack by adopting timestamp T_i in the tuple $(PPID_i, T_i, Msg_i, \delta_i)$. This indicates the departure time of the message tuple. Let T_r and $\triangle$ are the receiving time and the predefined time delay, respectively. The verifier requires to test the $\triangle \geq T_r - T_i$. If this is the case, then there is no opportunity for a repeat assault. Because of this, the vehicular fog computing we've developed using 5G is secure against replay attacks.
- Resistance Against Impersonation Attack: Since it is impossible for a third party to fake the signature tuple, no one can pretend to be the legitimate vehicle broadcasting the communication. The verifier checks the signature tuple by using the equation $R_i \cdot Pub_{TA} = Pub_{Fog} + U_i$. In the absence of this, an impersonation assault cannot occur. So, for vehicle fog computing provided by 5G, our approach is secure against impersonation attacks.
- Resistance Against Modification Attack: Similar to the forgery attack, it needs a third party to modify/impersonate a signature tuple that is checked by calculating $\sigma_i^- = h_3(PPID_i^1||PPID_i^2||Msg_i|| Pub_{Fog}||Pub_{TA}||T_i)$. Then the verifier checks whether $\sigma_i^- = \sigma_i$. Hence, our work is safe from modification attacks for 5G-enabled vehicular fog computing.
- Resistance Against Man-In-The-Middle Attack: Since the vehicles are talking directly with one another, there

TABLE 1. The Required Processing Time for Several Types of Cryptographic Operations.

Abbr.	Running Time
RT_{bp}	5.811 ms
RT_{pm-bp}	1.5654 ms
RT_{pa-bp}	0.0106 ms
RT_{mtp}	4.1724 ms
RT_{sm-ecc}	0.6718 ms
RT_{pa-ecc}	0.0031 ms

is no way for an outsider to launch a security attack of that nature. Our solutions for 5G-enabled vehicle fog computing are, thus, secure against MITM attacks.

VI. PERFORMANCE EFFICIENT

This section describes and compares the performance efficiency of our work and the recent existing schemes concerning computational and communication overheads as follows.

A. COMPUTATIONAL OVERHEAD

To convey how long it takes to execute various kinds of cryptographic operations, this paper makes use of the following notations.

- RT_{bp}: Running time of a bilinear pairing.
- RT_{pm-bp}: Running time of a multiplicative group G_1 based point multiplication.
- RT_{pa-bp}: Running time of an adaptive group G based point addition.
- RT_{mtp}: Running time of a group G_1 based map-to-point function.
- RT_{sm-ecc}: Running time of a group G based scalar point multiplication.
- RT_{pa-ecc}: Running time of a group G based point addition.

In this paper, the running time of the general cryptographic hash function has not been included due to its time-consuming very negligible value of processing cost. For satisfying the 80-bit security level, this work selects the bilinear pairings $e^- : G_1 \times G_1 \rightarrow G_2$ for pseudonym authentication schemes [28], [29]. Where G_2 and G_1 indicates multiplicative group and cyclic additive group with the same size prime order 160 bits with generator P. Where P is a point based on the supersingular curve $y^2 \equiv (x^3 + x) mod p$ with embedded degree 2, where the prime size P is 512 bits. Since our work and existing pseudonym authentication schemes [21], [32], [33] are lies on ECC. This work selects an adaptive cyclic group G of order q with generator P. Where P is a point based on an elliptic curve of non-super singular $y^2 \equiv x^3 + x mod p$, where both p and q are of equal size 160 bits and, a, b Z_q^*. According to this setting, the running time of cryptographic operations used is depicted in Table 3.

For simplicity, let MSP, SSV, and BSV indicate the message signing phase, single signature verification, and batch signature verification, respectively. The computation cost of existing schemes [28], [29] are based on bilinear pair as follows. In Bayat et al.'scheme [28], it required 2 bilinear pair operations, 4 scalar multiplication operations, 1 addition point operation, and 1 MapToPoint hash function; thus, the entire cost of computation for MSP is $2RT_{bp} + 4RT_{pm-bp} + 1RT_{pa-bp} + 1RT_{mtp} \approx 22.067$ ms. While the process of SSV in the Bayat et al.'s scheme [28], it needed 1 bilinear pair operation, 4 scalar multiplication operations, 1 addition point operation, and 1 MapToPoint hash function; thus, the entire cost of computation for SSV process is $1RT_{bp} + 4RT_{pm-bp} + 1RT_{pa-bp} + 1RT_{mtp} \approx 16.256$ ms. While the process of BSV in Bayat et al.'s scheme [28], it needed (4+n) scalar multiplication operations, n addition point operations, and n MapToPoint hash functions; hence, the entire cost of computation for BSV process is $(4 + n)RT_{pm-bp} + nRT_{pa-bp} + nRT_{mtp} \approx 6.2616 + 5.7484\,n$ ms. In Ali and Li' scheme [29], it needed 3 scalar multiplication operations and 1 addition point operation; thus, the entire cost of computation for MSP is $3RT_{pm-bp} + 1RT_{pa-bp} \approx 4.7068$ ms. While the process of SSV in the Ali and Li' scheme [29], it required 1 bilinear pair operation, 1 scalar multiplication operation; thus, the entire cost of computation for SSV process is $1RT_{bp} + 1RT_{pm-bp} \approx 7.3764$ ms. While the process of BSV in Ali and Li' scheme [29], it needed 1 bilinear pair operation, n scalar multiplication operations; thus, the entire cost of computation for BSV process is $1RT_{bp} + nRT_{pm-bp} \approx 5.811 + 1.5654n$ ms

The computation cost of existing schemes [21], [32], [33] are based on ECC as follows. In Zhang et al.' scheme [21], it required 3 scalar point multiplication operations; thus, the entire cost of computation for MSP process is $3RT_{sm-ecc} \approx 2.015$ ms. While the process of SSV in Zhang et al.' scheme [21], it needed 2 scalar point multiplication operations; thus, the entire cost of computation for SSV process is $2RT_{sm-ecc} \approx 1.3436$ ms. While, the process of BSV in Zhang et al.' scheme [21], (n+1) scalar point multiplication operations; thus, the entire cost of computation for BSV process is $n + 1RT_{sm-ecc} \approx 0.6718 + 0.6718n$ ms. In Alshudukhi et al.' scheme [32], it required 2 scalar multiplication operations; thus, the entire cost of computation for MSP process is $2RT_{sm-ecc} \approx 1.3436$ ms. While the process of SSV in Alshudukhi et al.' scheme [32], it needed 3 scalar point multiplication operations and 1 addition point operation; thus, the entire cost of computation for SSV process is $3RT_{sm-ecc} + 1RT_{pa-ecc} \approx 2.026$ ms. While the process of BSV in Alshudukhi et al.' scheme [32], (2+n) scalar point multiplication operations and n point additions; thus, the entire cost of computation for BSV process is $(2 + n)RT_{sm-ecc} + nRT_{pa-ecc} \approx 1.3436 + 0.6749\,n$ ms. In Al-Shareeda et al.' scheme [33], it required 2 scalar multiplication operations; thus, the entire cost of computation for MSP process is $2RT_{sm-ecc} \approx 1.3436$ ms. While the process of SSV in Al-Shareeda et al.' scheme [33], it needed 2 scalar point multiplication operations and 1 addition point operation; thus, the entire cost of computation for SSV process is $2RT_{sm-ecc} + 1RT_{pa-ecc} \approx 1.3467$ ms. While the process

TABLE 2. Overhead of Computational Comparison.

Schemes	MSP Process (ms)	SSV Process (ms)	BSV Process (ms)
Bayat et al. [28]	$2RT_{bp} + 4RT_{pm-bp} + 1RT_{pa-bp} + 1RT_{mtp} \approx 22.067$	$1RT_{bp}+4RT_{pm-bp}+1RT_{pa-bp}+1RT_{mtp} \approx 16.256$	$(4+n)RT_{pm-bp} + nRT_{pa-bp} + nRT_{mtp} \approx 6.2616 + 5.7484n$
Ali and Li [29]	$3RT_{pm-bp} + 1RT_{pa-bp} \approx 4.7068$	$1RT_{bp} + 1RT_{pm-bp} \approx 7.3764$	$1RT_{bp} + nRT_{pm-bp} \approx 5.811 + 1.5654n$
Zhang et al. [21]	$3RT_{sm-ecc} \approx 2.015$	$2RT_{sm-ecc} \approx 1.3436$	$n + 1RT_{sm-ecc} \approx 0.6718 + 0.6718n$
Alshudukhi et al. [32]	$2RT_{sm-ecc} \approx 1.3436$	$3RT_{sm-ecc}+1RT_{pa-ecc} \approx 2.026$	$(2+n)RT_{sm-ecc}+nRT_{pa-ecc} \approx 1.3436 + 0.6749n$
Al-Shareeda et al. [33]	$2RT_{sm-ecc} \approx 1.3436$	$2RT_{sm-ecc} + 1RT_{pa-ecc} \approx 1.3467$	$(2+n)RT_{sm-ecc}+nRT_{pa-ecc} \approx 1.3436 + 0.6749n$
Our FC-PA	$1RT_{sm-ecc}+1RT_{pa-ecc} \approx 0.6749$	$1RT_{sm-ecc} + 1RT_{pa-ecc} \approx 0.6749$	$RT_{sm-ecc} + nRT_{pa-ecc} \approx 0.6718 + 0.0031n$

TABLE 3. The Execution Time Required for Different Cryptographic Operations.

Schemes	Tuple Format	Items	Single Size	Batch Size
Bayat et al.' scheme [28]	$\{V, m, r, T_{i1}, T_{i2}, T_{i3}, PID_i, ts_i\}$	$(v, T_{i1}, T_{i2}, T_{i3}, PID_i \in G_2), (r \in Z_q^*)$	$5 \cdot 128 + 20 + 4 = 664$ bytes	664n bytes
Ali and Li' scheme [29]	$\{m_i, PID_i, \sigma_i, t_i\}$	$(PID_{i,v}, \theta_i, D_i \in G_2), (PID_{i,T} \in Z_q^*)$	$3 \cdot 128 + 20 + 2 \cdot 4 = 284$ bytes	284n bytes
Zhang et al.' scheme [21]	$\{PID_j, M_j, Y_j, S_j, T_j\}$	$(PID_j = \{PID_{j,1}, PID_{j,2}, Y_j \in G\}), (S_j \in Z_q^*)$	$3 \cdot 64 + 20 + 4 = 216$ bytes	216n bytes
Alshudukhi et al.' scheme [32]	$\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$	$(PsID_i^1 \in G), (PsID_i^2, \sigma_{m_i} \in Z_q^*)$	$64 + 2 \cdot 20 + 4 = 108$ bytes	108n bytes
Al-Shareeda et al.' scheme [33]	$\{AID_i, R_i, M_i, T_i, \sigma_i\}$	$(R_i, \sigma_i \in G), (AID_i \in Z_q^*)$	$2 \cdot 64 + 20 + 4 = 152$ bytes	152n bytes
FA-PA	$\{PPID_i, T_i, Msg_i, \delta_i\}$	$(PID_i^1 \in G), (PID_i^2, U_i, R_i \in Z_q^*)$	$64 + 3 \cdot 20 + 4 = 128$ bytes	128n bytes

of BSV in Al-Shareeda et al.' scheme [33], 2 scalar point multiplication operations and (n+1) addition point operation; thus, the entire cost of computation for BSV process is $(2+n)RT_{sm-ecc} + nRT_{pa-ecc} \approx 1.3436 + 0.6749\,n$ ms. While, in our FC-PA scheme, it required 1 scalar multiplication operation and 1 point addition; thus, the entire cost of computation for MSP process is $1RT_{sm-ecc} + 1RT_{pa-ecc} \approx 0.6749$ ms. While, the process of SSV in our FC-PA scheme, it needed 1 scalar point multiplication operation and 1 addition point operation; thus, the entire cost of computation for SSV process is $1RT_{sm-ecc} + 1RT_{pa-ecc} \approx 0.6749$ ms. While, the process of BSV in our FC-PA scheme, 1 scalar point multiplication operations, and n addition point operation; thus, the entire cost of computation for BSV process is $RT_{sm-ecc} + nRT_{pa-ecc} \approx 0.6718 + 0.0031n$ ms.

To conclude the above process, Table 2 summarizes the overhead of computational comparison for existing works and our proposal. Figure 5 shows the computational comparison for MSP and SSV processes, while Figure 6 summarizes the overhead of computational comparison to verify multiple messages.

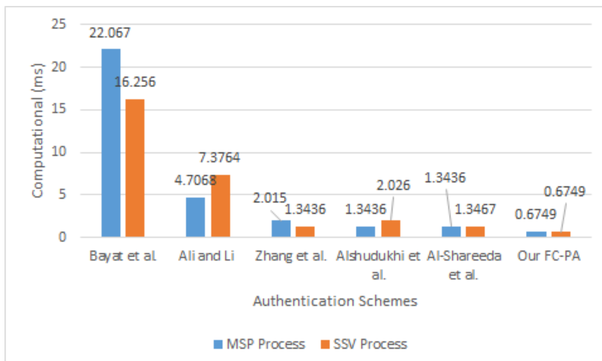

FIGURE 5. Overhead of Computational Comparison for MSP and SSV Processes.

B. COMMUNICATION OVERHEAD

This subsection reviews and compares the overhead of communication of our work with the existing schemes [28], [29] based on bilinear pair and that of [21], [32], and [33] based on ECC. To achieve an 80-bit security level, the size of p is equal to 64 bytes and 20 bytes for the bilinear pair and ECC, respectively. A point on E includes x, y coordinates, in which the size of each item in G_1 and G are 128 bytes and 40 bytes, respectively. Additionally, the size of the timestamp and hash function is 4 bytes and 20 bytes, respectively. This work supposes that the size of the message is the same for all the existing schemes. Consequently, this work takes into consideration the size of the signature on the message with the relevant public pseudonym-IDs.

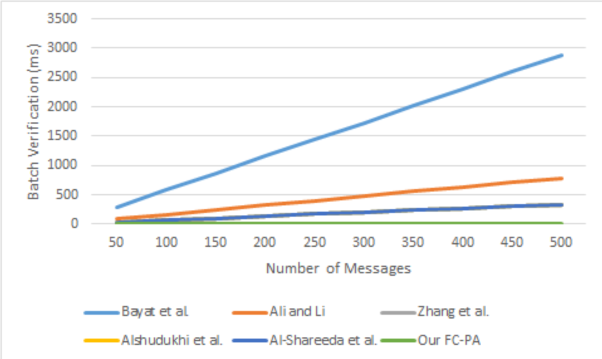

FIGURE 6. Overhead of Computational Comparison for BSV Process.

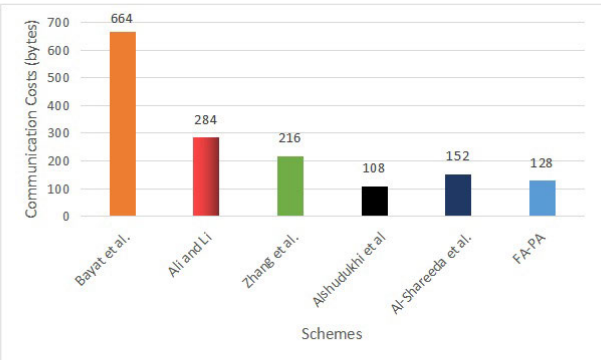

FIGURE 7. Overhead of Communication Comparison.

The communication cost of existing schemes [28], [29] are based on bilinear pair as follows. In Bayat et al.' scheme [28], the vehicle broadcasts $\{V, m, r, T_{i1}, T_{i2}, T_{i3}, PID_i, ts_i\}$ to other, $(v, T_{i1}, T_{i2}, T_{i3}, PID_i \in G_2)$, $(r \in Z_q^*)$ and ts_i is a timestamp; thus, the entire cost of communication is $5 \cdot 128 + 20 + 4 = 664$ bytes. In Ali and Li' scheme [29], the vehicle broadcasts $\{m_i, PID_i, \sigma_i, t_i\}$ to other, where $(PID_i = PID_{i,v}, PID_{i,T}, T_i and \sigma_i = \theta_i, D_i)$, $(PID_{i,v}, \theta_i, D_i \in G_2)$, $(PID_{i,T} \in Z_q^*)$ and 2 timestamps (T_i, t_i); thus, the entire cost of communication is $3 \cdot 128 + 20 + 2 \cdot 4 = 284$ bytes.

The communication cost of existing schemes [21], [32], [33] are based on ECC as follows. In Zhang et al.' scheme [21], the vehicle broadcasts $\{PID_j, M_j, Y_j, S_j, T_j\}$ to other, where $(PID_j = \{PID_{j,1}, PID_{j,2}, Y_j \in G\})$, $(S_j \in Z_q^*)$ and T_j is timestamp; thus, the entire cost of communication is $3 \cdot 64 + 20 + 4 = 216$ bytes. In Alshudukhi et al.' scheme [32], the vehicle broadcasts $\{PsID_i^1, PsID_i^2, m_i, TS_i, \sigma_{m_i}\}$ to other, where $(PsID_i^1 \in G)$, $(PsID_i^2, \sigma_{m_i} \in Z_q^*)$ and TS_i is timestamp; thus, the entire cost of communication is $64 + 2 \cdot 20 + 4 = 108$ bytes. In Al-Shareeda et al.' scheme [33], the vehicle broadcasts $\{AID_i, R_i, M_i, T_i, \sigma_i\}$ to other, $(R_i, \sigma_i \in G)$, $(AID_i \in Z_q^*)$; thus, the entire cost of communication is $2 \cdot 64 + 20 + 4 = 152$ bytes. While, our FA-PA scheme, the vehicle broadcasts $\{PPID_i, T_i, Msg_i, \delta_i\}$ to other, $(PID_i^1 \in G)$, $(PID_i^2, U_i, R_i \in Z_q^*)$ and T_i is timestamp; thus, the entire cost of communication is $64 + 3 \cdot 20 + 4 = 128$ bytes. Figure 7 shows overhead of communication comparison.

VII. CONCLUSION

In this work, we have proposed a fog computing-based pseudonym authentication (FC-PA) scheme that supports batch signature verification, privacy-preserving, and pseudonym authentication for the 5G-enabled vehicular network. In order to verify data, the FC-PA system uses a single scalar multiplication operation of elliptic curve cryptography. The security analysis describes that our work is secure under the random oracle model. Additionally, the FC-PA scheme can withstand common security attacks like replay, impersonation, modification, and man-in-the-middle attacks. Finally, the FC-PA scheme can obtain better trade-offs between efficiency and security than other recent works.

In future studies, we will focus on designing a scheme with better scalability and compatibility that will be more appropriate for the 5G-enabled vehicular network.

ACKNOWLEDGMENT

The authors would like to acknowledge the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, for funding this research.

REFERENCES

[1] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.

[2] M. A. Al-Shareeda and S. Manickam, "COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *Int. J. Environ. Res. Public Health*, vol. 19, no. 23, p. 15618, Nov. 2022.

[3] Y. Yang and K. Hua, "Emerging technologies for 5G-enabled vehicular networks," *IEEE Access*, vol. 7, pp. 181117–181141, 2019.

[4] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, "Security challenges of location privacy in VANETs and state-of-the-art solutions: A survey," *Future Internet*, vol. 13, no. 4, p. 96, Apr. 2021.

[5] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications," *Sustainability*, vol. 14, no. 23, p. 15900, Nov. 2022.

[6] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. Rodrigues, "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1630–1638, Feb. 2021.

[7] M. N. S. Almalki, A. L. Challoob, and M. A. Al-Shareeda, "ID-PPA: Robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network," in *Advances in Cyber Security*, vol. 1347. Penang, Malaysia: Springer Nature, Dec. 2020, pp. 80–94.

[8] M. M. Hamdi, L. Audah, S. A. Rashid, and M. Al Shareeda, "Techniques of early incident detection and traffic monitoring centre in VANETs: A review," *J. Commun.*, vol. 15, no. 12, pp. 896–904, 2020.

[9] M. A. Hamdan, A. M. Maklouf, and H. Mnif, "Review of authentication with privacy-preserving schemes for 5G-enabled vehicular networks," in *Proc. 15th Int. Conf. Secur. Inf. Netw. (SIN)*, Nov. 2022, pp. 1–6.

[10] J. Cui, J. Yu, H. Zhong, L. Wei, and L. Liu, "Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 20, 2022, doi: 10.1109/TITS.2022.3227949.

[11] M. A. Al-Shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, A. Khalil, M. A. Alazzawi, and A. S. Al-Hiti, ''Proposed efficient conditional privacy-preserving authentication scheme for V2V and V2I communications based on elliptic curve cryptography in vehicular ad hoc networks,'' in *Advances in Cyber Security*. Penang, Malaysia: Springer, Dec. 2021, pp. 588–603.

[12] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, ''Reliable and efficient content sharing for 5G-enabled vehicular networks,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1247–1259, Feb. 2020.

[13] A. A. Ahmed, S. J. Malebary, W. Ali, and O. M. Barukab, ''Smart traffic shaping based on distributed reinforcement learning for multimedia streaming over 5G-VANET communication technology,'' *Mathematics*, vol. 11, no. 3, p. 700, Jan. 2023.

[14] M. A. Al-Shareeda and S. Manickam, ''Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation,'' *Symmetry*, vol. 14, no. 8, p. 1543, Jul. 2022.

[15] M. M. A. Al-shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and I. H. Hasbullah, ''Security schemes based conditional privacy-preserving in vehicular ad hoc networks,'' *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, 2020.

[16] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong, ''DBCPA: Dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks,'' *IEEE Trans. Mobile Comput.*, pp. 1–15, 2022.

[17] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, ''Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU),'' *Sustainability*, vol. 14, no. 16, p. 9961, Aug. 2022.

[18] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, ''Edge computing: Vision and challenges,'' *IEEE Internet Things J.*, vol. 3, pp. 637–646, May 2016.

[19] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, ''Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey,'' *IEEE Access*, vol. 9, pp. 121522–121531, 2021.

[20] D. Miao, L. Liu, R. Xu, J. Panneerselvam, Y. Wu, and W. Xu, ''An efficient indexing model for the fog layer of industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4487–4496, Oct. 2018.

[21] 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.

[22] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, ''Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs,'' *IEEE Syst. J.*, vol. 14, no. 4, pp. 5373–5383, Dec. 2020.

[23] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ''VANet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[24] M. Soni, B. S. Rajput, T. Patel, and N. Parmar, ''Lightweight vehicle-to-infrastructure message verification method for VANET,'' in *Data Science and Intelligent Applications*. Cham, Switzerland: Springer, 2021, pp. 451–456.

[25] P. Shah and T. Kasbe, ''A review on specification evaluation of broadcasting routing protocols in VANET,'' *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100418.

[26] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, ''NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET,'' *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018.

[27] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, ''NERA: A new and efficient RSU based authentication scheme for VANETs,'' *Wireless Netw.*, vol. 26, pp. 3083–3098, Jun. 2019.

[28] M. Bayat, M. Barmshoory, S. M. Pournaghi, M. Rahimi, Y. Farjami, and M. R. Aref, ''A new and efficient authentication scheme for vehicular ad hoc networks,'' *J. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 171–183, 2020.

[29] I. Ali and F. Li, ''An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs,'' *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100228.

[30] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, ''SE-CPPA: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,'' *Sensors*, vol. 21, no. 24, p. 8206, Dec. 2021.

[31] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, ''RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks,'' *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6417–6428, Aug. 2019.

[32] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, ''A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography,'' *IEEE Access*, vol. 9, pp. 15633–15642, 2021.

[33] M. Al-Shareeda, M. Anbar, S. Manickam, and I. Hasbullah, ''Password-guessing attack-aware authentication scheme based on Chinese remainder theorem for 5G-enabled vehicular networks,'' *Appl. Sci.*, vol. 12, no. 3, p. 1383, 2022.

[34] D. Pointcheval and J. Stern, ''Security arguments for digital signatures and blind signatures,'' *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, Mar. 2000.

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 Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He is currently a Postdoctoral Fellow with the National Advanced IPv6 Centre (NAv6), USM. His current research interests include network monitoring, the Internet of Things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security.

SELVAKUMAR MANICKAM is the Director of the National Advanced IPv6 Centre and an Associate Professor specializing in cybersecurity, the Internet of Things, industry 4.0, cloud computing, big data, and machine learning. He has authored and coauthored more than 220 articles in journals, conference proceedings, and book reviews. He has graduated 18 Ph.D. students in addition to master's and bachelor's students. He has given several keynote speeches and dozens of invited lectures and workshops at conferences, international universities, and industry. He has given talks and training on internet security, the Internet of Things, industry 4.0, IPv6, machine learning, software development, and embedded and OS kernel technologies at various organizations and seminars. He also lectures in various computer science and IT courses, including developing new courseware in tandem with current technology trends. He is involved in various organizations and forums locally and globally. Previously, he was with Intel Corporation and a few start-ups working in related areas before moving to academia. While building his profile academically, he is still very involved in industrial projects involving industrial communication protocol, robotic process automation, machine learning, and data analytics using open-source platforms. He also has experience in the building IoT, embedded, server, mobile, and web-based applications.

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 Assistance 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 standard.

ABDULRAHMAN ALRESHIDI received the Ph.D. degree in computer science from King's College London, U.K. He has been an Assistant Professor of software engineering with the College of Computer Science and Engineering, University of Ha'il, Saudi Arabia, since 2016. His current research interests include mobile computing and the Internet of Things.

MESHARI ALAZMI received the B.S. degree in computer science from the University of Ha'il, Saudi Arabia, the M.S. degree in computer science from the University of Missouri, and the Ph.D. degree in computer science from the King Abdullah University of Science and Technology (KAUST), Saudi Arabia. He is currently an Assistant Professor with the College of Computer Science and Engineering, University of Ha'il, where he is also the Vice Dean of the Research and Consulting Studies Institute. His research interests include bioinformatics and machine.

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.

MOHAMMAD ALSAFFAR received the B.Sc. degree in computer science from the University of Ha'il, Saudi Arabia, in 2008, the M.Sc. degree from De Montfort University, U.K., in 2011, and the Ph.D. degree from Brighton University, U.K., in 2019. He is currently an Assistant Professor with the Computer Science and Engineering College, University of Ha'il. He is also the Vice Dean of Community Service and Continuing Education Deanship. His research interests include user experience, human–computer interaction, usability, interface design, and cyber security.