Tamper-Resilient and Sensor-Spoofing-Resistant Authentication for 5G-Connected Vehicular Edge Systems

Sarah Al-Hilfi
Computer Engineering Department, College of Engineering, University of Basrah, Basra, Iraq
sara.aziz@uobasrah.edu.iq

Mohammed Yousif
Department of Computer Engineering Techniques, College of Technical Engineering, University of Al Maarif, Al Anbar, Iraq
Mohammed.alyousif1991@gmail.com

Huda Mohammed Alsayednoor
Shatt Al-Arab University College, Basra, Iraq
huda1994noor@gmail.com

Mahmood A. Al-Shareeda
Department of Information Technology, Management Technical College, Southern Technical University, Basrah, Iraq | College of Engineering, Al-Ayen University, Thi-Qar, Iraq
mahmood.alshareedah@stu.edu.iq (corresponding author)

Mohammed Almaayah
Department of Computer Science, King Abdullah the II IT School, The University of Jordan, Amman, Jordan
m.almaiah@ju.edu.jo

Marwan Albahar
Department of Computing, College of Engineering and Computing in Al-Lith, Umm Al-Qura University, Makkah, Saudi Arabia
mabahar@uqu.edu.sa

Received: 15 July 2025 | Revised: 15 August 2025 and 26 August 2025 | Accepted: 30 August 2025

 DOI: https://doi.org/10.48084/etasr.13431

ABSTRACT

From the perspective of vehicular fog computing enabled by 5G, fast and secure authentication between Onboard Units (OBUs) and Fog Servers (FSs) is crucial. Threats such as combined physical tampering and sensor spoofing, along with emergency message forgery, can be devastating in practice, causing traffic accidents, privacy breaches, or service interruptions. This paper presents a six-phase, tamper-resilient authentication protocol tailored for 5G vehicular networks. It integrates entropy-based sensor verification and real-time tamper detection into a unified trust mechanism, alongside emergency-aware session handling. To ensure post-quantum resilience, forward secrecy, and lightweight performance, we employ Chebyshev polynomial cryptography and hash chains. The proposed scheme reduces computational time by 32% and communication overhead by 27% compared to existing protocols, demonstrating its effectiveness and robustness for real-time vehicular edge environments.

Keywords-5G vehicular networks; fog computing; secure authentication; tamper detection; sensor spoofing; Chebyshev polynomial cryptography; emergency message integrity; post-quantum security; Trusted Execution Environment (TEE); vehicular edge computing

I. INTRODUCTION

The integration of 5G networks, edge computing, and Intelligent Transportation Systems (ITS) is revolutionizing vehicular communication [1-3]. Fog computing, as a promising paradigm, has been recently introduced to drastically decrease end-to-end latency by permitting mobile-based technologies to send their data to a nearby Fog Server (FS), allowing data analytics to be carried out quickly and transforming big data into actionable information that can be used in real time [4-6]. In such a scenario, Onboard Units (OBUs) exchange messages with infrastructure through 5G-based Vehicle-to-Infrastructure (V2I) protocols to facilitate mission-critical services such as emergency alerting, broadcasting, cooperative driving, and vehicular cloud services [7-10].

However, where wireless interfaces, high mobility speeds, and open-access hardware are pervasive, there are also notable security and privacy challenges. OBUs and fog nodes are vulnerable to both cyber and physical attacks, such as impersonation, session hijacking, sensor spoofing, and physical tampering [11-13]. These can result in severe threats to vehicular safety due to the introduction of fake data or the disruption of the authenticated message flow [14, 15]. Moreover, hard latency guarantees must be provided by 5G-based vehicle-to-everything (5G-V2X) services, which involve encryption operations such as bilinear pairings, whereas complex certification chains are not applicable [16-18]. Thus, there is an urgent requirement for lightweight but tamper-resilient authentication protocols designed for the operational conditions of vehicular fog environments [19-21].

Attacks such as sensor-generated fake data or malicious message modification can directly impact safety, leading to accidents or delayed emergency responses. This motivates the immediate requirement for lightweight and efficient authentication mechanisms for vehicular fog networks operating over 5G.

To address the gap, this paper introduces a new tamper-resilient, sensor-aware authentication framework for 5G-based vehicular fog systems. The scheme operates based on a six-phase architecture, from secure bootstrapping to mutual authentication, spoofing detection, emergency request handling, and post-session audit logging. Every vehicle has a Trusted Execution Environment (TEE) for secure storage of keys, real-time feedback of the physical state, and cryptographic operations. The sensor data are validated utilizing entropy and cross-modality correlation to identify forged inputs, and all messages are authenticated utilizing Chebyshev polynomial-based signatures and lightweight hash functions. The main contributions of this paper are summarized as follows:

- We propose a lightweight and performance-efficient authentication scheme that integrates real-time physical tamper detection and entropy-based sensor spoofing resistance into the vehicular communication process.
- A mixed cryptographic design based on Chebyshev polynomials and hash chains ensures forward secrecy, message integrity, and post-quantum robustness.
- Emergency requests are supported through session-isolated key derivation and sensor-based verification to reduce false positives and malicious alerts.
- Secure session logs generated by hash-chained audit trails allow for revocation, accountability, and forensics.

II. RELATED WORK

Secure and efficient authentication continues to be critical for vehicular fog computing, and it has become even more challenging in the era of 5G, where high-speed mobility, device diversity, and real-time response are considered new constraints. Recent works on lightweight cryptographic designs [22, 23], sensor integrity, and post-quantum resistance [24, 25] for vehicular edge networks are surveyed in this section.

The Fog Computing-based Pseudonym Authentication (FC-PA) protocol proposed by authors in [26] employs fog computing and pseudonym-based authentication procedures for V2I communication. ECA-VFog, proposed by authors in [27], adopts certificateless public key cryptography to eliminate certificate handling overhead. Authors in [28] proposed an Oblivious Transfer-based Authentication (OTAuth) protocol, which uses post-quantum secure primitives in fog-based vehicular networks. Despite being secure against quantum-powered adversaries, the scheme leads to large message and storage overhead and does not mitigate sensor spoofing attacks in real time. Authors in [29] advocate a privacy-preserving mutual authentication mechanism along with multi-service access and security handover with gNB authentication for 5G-based Vehicle-to-Network (5G-V2N) environments. Their protocol fortifies primary secrecy, confronts malicious base stations, and facilitates mobility. Authors in [30] present a lightweight 5G vehicular network authentication protocol based on a hybrid chaotic map using Elliptic Curve Cryptography (ECC). Authors in [31] present a secure smart irrigation system using Internet of Things-Vehicular Ad Hoc Network (IoT-VANET), fuzzy routing, and neural networks to optimize water management. This protocol guarantees authenticated key agreement, one-step real-time monitoring with mobile devices, and improved energy efficiency. Authors in [32] present a lightweight blockchain-based authentication protocol for VANETs with an emphasis on user privacy, replay attack resistance, and access control efficiency. Authors in [33] present a multi-factor blockchain-based fog authentication scheme for VANETs based on fingerprints and QR codes. It achieves low latency and communication overhead while preserving privacy. Authors in [34] present a Certificateless Aggregate Signature (CLAS)-based authentication scheme for VANETs that supports dynamic anonymity as well as private key updating, ensuring that private keys remain secure.

In contrast to the above approaches, the proposed framework introduces a six-phase design that consists of TEE-supported tamper detection, entropy-driven sensor integrity validation, emergency message session isolation, and secure log auditing. Based on lightweight Chebyshev-based cryptography and the rejection of heavy cryptographic pairings, the protocol remains lightweight and robust, which is particularly desirable for novel 5G-V2X applications that require low latency but high assurance in authentication.

III. SYSTEM AND THREAT MODEL

A. System Model

As shown in Figure 1, the proposed architecture is tailored for a 5G-enabled vehicular fog computing model consisting of the following core components:

- Trusted Authority (TA): A highly trusted backend entity responsible for onboarding, key creation, provisioning sensor profiles, and issuing certificates. It also serves as the auditor and revocation authority.
- Vehicle OBUs: Mobile units installed in vehicles, equipped with a TEE, onboard sensors (e.g., GPS, Inertial Measurement Unit (IMU), brake sensors), and wireless transceivers. OBUs mutually authenticate with Fog Nodes and originate or respond to emergency requests [35, 36].
- FSs: Infrastructure nodes deployed at roadside units, including solar roadways, or base stations. FSs are responsible for local authentication, sensor validation, tamper detection, and assisting with emergency message processing in coordination with the TA [37].
- 5G core network: Provides high-speed, low-latency communication among OBUs, fog nodes, and the TA. Network slicing and dedicated channels are also considered for safety-critical traffic [38].

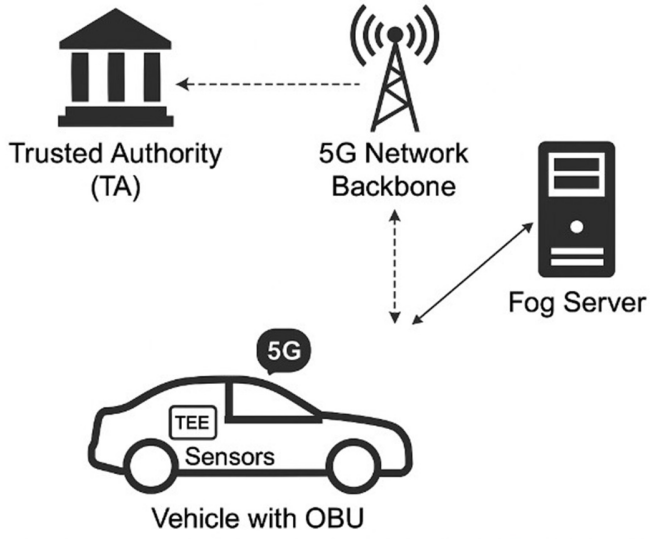

Fig. 1. System model of the proposed 5G-enabled vehicular fog architecture.

B. Assumptions

OBUs and FSs both utilize dedicated hardware components (e.g., TEE or Trusted Platform Module (TPM)) to securely store cryptographic keys in isolation and perform secure operations. The TA is considered a perfectly secure and trusted entity, providing synchronized timing via GPS or network signals to maintain the validity of authentication sessions. The first potential attack on device-to-device (D2D)-enabled communication is eavesdropping, interception, or modification of wireless signals by an adversary.

Although this work treats the TA as an ideal secure module, such guarantees are difficult to achieve in real-world scenarios. A compromised TA may leak cryptographic keys, sensor profiles, and the revocation list, weakening the overall security framework. To mitigate these issues, possible research directions include exploring decentralized or blockchain-based TA architectures, multi-TA federations, and hardware-assisted root-of-trust mechanisms to reduce Single Points of Failures SPOFs and improve operational resilience.

C. Threat Model

The adversary, denoted as $\mathcal{A}$, is considered strong but non-omnipotent and possesses the following abilities:

- Eavesdropping and replay: $\mathcal{A}$ can overhear messages transmitted over wireless channels and may replay them in subsequent sessions.
- Message modification: $\mathcal{A}$ can modify message content, inject fabricated packets, or try to perform Man-in-the-Middle (MITM) attacks to act as the vehicle or fog node.
- Physical and sensor-level manipulation: $\mathcal{A}$ may gain temporary or sustained physical access to an OBU (e.g., through theft or roadside access) to extract cryptographic material or tamper with firmware. $\mathcal{A}$ may also inject false sensor data, such as forged GPS coordinates, manipulated speed, or IMU readings, to spoof the system, fabricate emergencies, or bypass authentication mechanisms [39, 40].
- Sensor spoofing: $\mathcal{A}$ can attempt to trick the system by injecting bogus GPS coordinates, speed, or acceleration data, or by generating fake sensor signals to fabricate an emergency or bypass authentication [41, 42].
- Corrupted (obedient) devices: $\mathcal{A}$ can compromise one or several correct OBUs or fog nodes and use them to perform insider attacks, such as replay or data inference [43].
- Linkability attacks: $\mathcal{A}$ can analyze multiple sessions to identify or deduce a vehicle's accounts or behavior, thereby compromising privacy and anonymity goals [44-47].

IV. PROPOSED SCHEME

Our propose scheme introduces a secure, lightweight, and tamper-resilient authentication architecture for 5G-enabled vehicular fog computing systems. It addresses the challenges of real-time authentication, physical tamper resistance, and sensor spoofing in the vehicular environment. The architecture revolves around a multi-phase security model consisting of the TA, OBUs, and fog nodes, as shown in Figure 2.

A. Phase 1: Secure Bootstrapping and Enrollment

First, the TA securely and verifiably initializes all vehicular and edge devices. This stage ensures that all devices are uniquely identified, cryptographically provisioned, and rooted (with tamper-detection included) before entering operational mode.

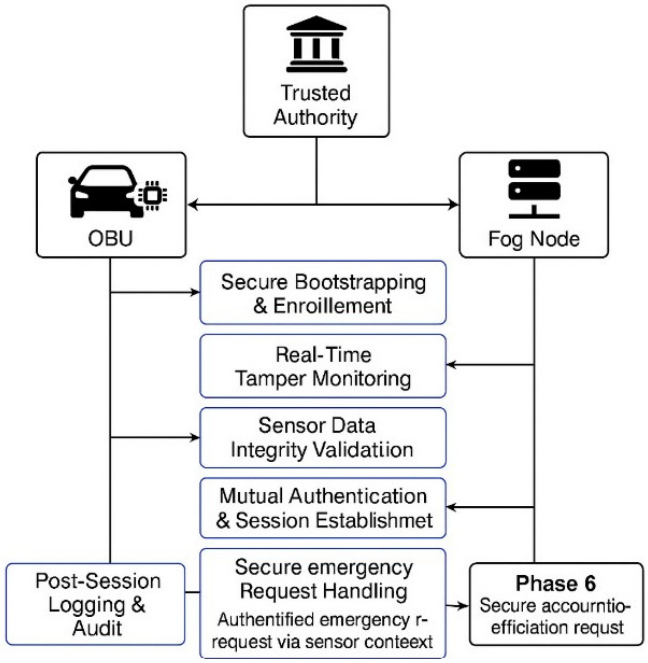

Fig. 2. Overview of the proposed 5G-enabled vehicular fog authentication scheme.

- Entity setup and key generation: The TA selects public cryptographic parameters for the system: A large prime number p, a base point ω, and a chaotic map parameter ρ. Each entity $x \in \{\text{Vehicle}, \text{Fog}\}$ receives a private key $k_x \in \mathbb{Z}_p^*$. The corresponding public key is computed as:

$$K_x = T^{\rho_{kx}(\omega)} \bmod p \quad (1)$$

where $T^{\rho_{kx}(\omega)}$ is the ρ -degree Chebyshev polynomial evaluated at point ω with exponent k_x. These parameters are securely pre-installed in each device's TEE.

- Secure boot and hash measurement: At startup, the TEE executes a secure bootloader and generates an integrity measurement hash:

$$H = h(\text{bootloader}||\text{firmware}||\text{configs}) \quad (2)$$

which is signed using the entity's private key k_x: $\sigma_x = \text{Sign}_{k_x}(H)$. This signed attestation proves that the device is running unmodified software.

- Remote attestation protocol: Each entity x sends an attestation request to the TA: $\text{Req\_attest} = \{ID_x, K_x, H, \sigma_x\}$. The TA verifies the signature: $\text{Verify}_{K_x(H,\sigma_x)}? = \text{TRUE}$. If valid, the TA issues a certificate by signing the identity, public key, and current hash: $\text{Cert}_x = \text{Sign}_{k_{TA}}(ID_x, K_x, H)$. It also generates a one-time sensor seed vector ψ_x for initial calibration: $\psi_x = \text{PRNG}(k_{TA}, ID_x||\text{timestamp})$. The TA responds with: $\text{Resp}_{\text{attest}} = \{\text{Cert}_x, \psi_x\}$.

- Sensor fingerprint initialization: Each OBU, after receiving ψ_x, enters a secure calibration mode to collect ground-truth sensor values under TA supervision. It captures baseline data from multiple trusted sensors: $\psi_{base_x} = \{\text{GPS}_{\text{ref}}, \text{IMU}_{\text{ref}}, \text{LIDAR}_{\text{ref}}\}$. A hashed summary of the baseline sensor profile is computed and securely stored:

$$\Psi_x = h(\psi_{base_x}||\psi_x) \quad (3)$$

This hash Ψ_x is saved within the TEE and used later to verify real-time sensor data.

- Completion of enrollment: After these steps, the TA records the tuple $\{ID_x, K_x, \text{Cert}_x, \Psi_x\}$. This stage verifies the authentication of all system nodes and provides hardware protections and pre-qualified sensor profiles, enabling secure real-time operation. OBUs and FSs are now in active status and can proceed with mutual authentication and emergency communication protocols.

B. Phase 2: Tamper Monitoring at Run Time

In this step, the proposed architecture guarantees the ongoing physical integrity of vehicles and fog nodes using hardware-aided tamper sensing and real-time trust monitoring. This is important in vehicular systems that are exposed, open, or public, where adversaries may gain physical access.

- TEE integration: All OBUs and FSs possess hardware support for trusted execution (e.g., ARM TrustZone, TPM, or Intel SGX). This secure area isolates and controls: (i) storage of private keys k_x and sensor profile hash Ψ_x; (ii) execution of operations with high security requirements (e.g., signing, attestation); and (iii) monitoring of internal hardware state and reacting to attacks. Depending on the hardware of the device, the TEE collects integrity signals in real time, including power oscillation records $\delta_P(t)$, clock interval deviations $\delta_C(t)$, and variations in bus/memory activity $\delta_M(t)$. The combined tamper evidence vector is computed as:

$$\tau_x(t) = h(\delta_P(t)||\delta_C(t)||\delta_M(t)) \quad (4)$$

This value is compared to a tamper threshold θ_{tamper} set during manufacturing: $\tau_x(t)? < \theta_{\text{tamper}}$. If this condition fails, a tamper event is generated.

- Impair response mechanism: TEE executes the following countermeasures in response to an intervention event: (i) forget all volatile keys and session material: $\text{erase}(k_x)$, $\text{erase}(SK)$, $\text{erase}(\psi_x)$; (ii) create a tamper alert message: $\text{Alert}_x = \text{Sign}_{k_x}(ID_x||t||\tau_x(t))$; (iii) send Alert_x to the TA and nearest FS: $\text{Alert}_x \rightarrow \{TA, FS_j\}$; (iv) enter quarantine mode, denying all operations until reset by the TA.

- Validation of tamper alerts: FSs and the TA process tamper alerts by verifying the digital signature: $\text{Verify\_K}_x(ID_x||t||\tau_x(t), \text{Alert}_x)? = \text{TRUE}$. If verification fails, the TA revokes Cert_x, propagates a signed Certificate Revocation List (CRL), and blacklists the entity and its hardware ID.

- Recovery and reinitialization: Once physical integrity is restored (e.g., through service or inspection), the device should be reenrolled as in Phase 1. This includes generating new keys (k'_x, K'_x,), and regenerating a new sensor profile ψ'_x.

C. Phase 3: Sensor Data Integrity Validation

In vehicular systems, the authenticity and trustworthiness of sensor data are critical for making safety decisions and ensuring accurate situational awareness. This phase introduces a lightweight yet effective mechanism to detect and prevent sensor spoofing attacks in real time.

- Sensor data signing mechanism: Each sensor reading $S_i(t)$ from sensor i at time t is signed within the TEE. The signed payload is: $Msg_i(t) = \{S_i(t), t, ID_x\}$. This message is digitally signed using the device's private key k_x: $\sigma_i(t) = Sign_{k_x}(Msg_i(t))$. The final transmitted packet is: $Pkt_i(t) = \{Msg_i(t), \sigma_i(t)\}$.
- Cross-sensor validation via entropy and correlation: To detect spoofing, FSs verify received data both cryptographically and statistically:
  1. Entropy-based anomaly detection: The entropy of sensor i over a sliding window T is computed:

     $$H(S_i) = -\sum P_j \log_2 P_j \quad (5)$$

     If entropy drops below a predefined threshold θ_H : $H(S_i)? < \theta_H$, the sensor S_i is marked as suspicious.
  2. Multi-sensor correlation check: Let S_{GPS} , S_{IMU} , and S_{Speed} denote readings from different sensors. The correlation coefficient between sensors i and j is:

     $$\rho_{ij} = \frac{cov(S_i, S_j)}{\sigma_{S_i} \sigma_{S_j}} \quad (6)$$

     If $\rho_{ij} < \theta_{corr}$, this indicates inconsistency and potential spoofing.
- Profile-based sensor matching: FSs retrieve the expected sensor profile hash Ψ_x from enrollment (Phase 1). A fresh sensor snapshot $\psi_{live_x}(t)$ is hashed and compared to the baseline:

  $$\Psi_{live_x}(t) = h(\psi_{live_x}(t) || \psi_x) \quad (7)$$

  If $\Psi_{live_x(t)} \neq \Psi_x$, the sensor data deviate from trusted patterns, indicating a potential spoofing attempt.
- FS validation process: Upon receiving a signed packet $Pkt_i(t)$ from a vehicle, the FS: (i) verifies the signature: $Verify_{K_x}(Msg_i(t), \sigma_i(t))? = TRUE$; (ii) computes entropy and correlation across sensor streams; and (iii) compares $\Psi_{live_x}(t)$ with Ψ_x. If any check fails, FS triggers a spoofing response: $Flag(ID_x, S_i(t), "Spoofing\ Detected")$.
- Spoofing response mechanism: If spoofing is confirmed, the FS notifies the TA and surrounding roadside units. The vehicle session is quarantined and flagged, and an incident record is stored for post-event forensic analysis.

D. Phase 4: Mutual Authentication and Session Establishment

This phase enables vehicles and FSs to establish a secure communication session over the 5G network, ensuring mutual authenticity and session freshness. The protocol combines lightweight cryptographic primitives with sensor-backed trust anchors established in prior phases.

- The protocol steps are:
  1. Vehicle → FS: The vehicle initiates the authentication by sending:

     $$Msg_1 = \{ID_v, N_v, T_v, \sigma_v\},$$

     $$\sigma_v = Sign_{k_v}(ID_v || N_v || T_v) \quad (8)$$
  2. FS → Vehicle: The FS verifies σ_v using K_v. If valid, it generates a nonce N_f and timestamp T_f, then replies:

     $$Msg_2 = \{ID_f, N_f, T_f, \sigma_f\}, \ \sigma_f = Sign_{k_f}(ID_f || N_f || T_f || N_v) \quad (9)$$
  3. Vehicle → FS (session confirmation): Upon verifying σ_f, the vehicle computes the session key:

     $$SK_{vf} = h\left(T^{\rho k_v(N_f)} || T^{\rho k_f(N_v)}\right) \quad (10)$$

     and confirms the session by sending:

     $$Msg_3 = (Auth_{vf} = \{h(SK_{vf} || T_v || T_f)\} \quad (11)$$

     The FS computes the same SK_{vf} using its key and verifies $Auth_{vf}$. If matched, the session is mutually authenticated and active.
- Session key properties: The session key SK_{vf} satisfies the following:
  1. Forward secrecy: Since N_v and N_f are random per session, past sessions cannot be decrypted even if keys are compromised.
  2. Lightweight computation: Only Chebyshev polynomials and hash functions are used, avoiding ECC or pairing operations.
  3. Sensor binding: Each message is indirectly tied to verified sensors through prior validation (Phase 3).
- Replay and freshness protection: All messages contain nonces (N_v, N_f) and timestamps (T_v, T_f) to prevent replay attacks. A strict window-based freshness check is enforced: $|T_{recv} - T_{sent}| < \Delta_T$, where Δ_T is a preconfigured threshold (e.g., 2 s).
- Failure and recovery procedure: If signature verification or freshness checks fail, the protocol is aborted. The device logs the failure and initiates a short exponential backoff before retrying.

This protocol combines hardware-assisted tamper detection and sensor integrity validation based on entropy to address both physical and data-level threats, ensuring trustworthy communication in vehicular fog environments. This two-level trust model allows the system to distinguish between authorized and unauthorized physical access, as well as reject fake sensor input in real time. Phase 3 measures the entropy and correlation of sensor data, whereas Phase 4 establishes a secure session anchored in both verified sensor states and

physical ties of the communication endpoints. This joint treatment enhances resilience and situational awareness across diverse adversary scenarios.

E. Phase 5: Secure Emergency Request Handling

In vehicular environments, emergencies such as accidents, health events, or infrastructure failures demand rapid, secure communication between vehicles and the fog infrastructure. This phase ensures authenticated and integrity-protected emergency message delivery with verified sensor context and minimal delay.

- Emergency trigger and context gathering: An emergency is detected by the OBU via internal triggers or critical sensor thresholds (e.g., collision sensors, brake pressure, abnormal heart rate). The TEE initiates emergency protocol preparation by: (i) capturing the contextual sensor set $\psi_{\mathrm{emg_x}}$ (e.g., GPS, speed, IMU); (ii) recording the current timestamp $\mathrm{T_{emg}}$; and (iii) computing an integrity hash: $\Psi_{\mathrm{emg_x}} = \mathrm{h}\left(\psi_{\mathrm{emg_x}} \,||\, \mathrm{T_{emg}}\right)$.
- Emergency message construction: The emergency request is constructed as:

$$\mathrm{EMG_{req}} = \left\{\mathrm{ID_v}, \mathrm{Type_{emg}}, \mathrm{T_{emg}}, \Psi_{\mathrm{emg_x}}\right\} \quad (12)$$

  This message is signed to ensure authenticity and integrity: $\sigma_{\mathrm{emg}} = \mathrm{Sign_{k_v}}\left(\mathrm{EMG_{req}}\right)$. The final emergency packet is: $\mathrm{Pkt_{emg}} =, \left\{\mathrm{EMG_{req}}, \sigma_{\mathrm{emg}}\right\}$.
- FS verification and response: Upon receiving $\mathrm{Pkt_{emg}}$, the FS: (i) verifies the signature: $\mathrm{Verify_{K_v}}\left(\mathrm{EMG_{req}}, \sigma_{\mathrm{emg}}\right) =? = \mathrm{TRUE}$; compares $\Psi_{\mathrm{emg_x}}$ with the expected sensor profile Ψ_{x}: $\Psi_{\mathrm{emg_x}} ? = \Psi_{\mathrm{x}}$; and (iii) validates timestamp freshness: $|\mathrm{T_{recv}} - \mathrm{T_{emg}}| < \Delta_{\mathrm{T}}$. If all checks pass, the FS prioritizes message delivery across the 5G slice, notifies emergency response units (e.g., police, ambulance), and broadcasts $\mathrm{EMG_{req}}$ to nearby vehicles and roadside units.
- Emergency session isolation: To protect emergency communications from potential misuse, a session-isolation strategy is enforced. A separate short-lived key is derived:

$$\mathrm{SK_{emg\_vf}} = \mathrm{h}\left(\mathrm{SK_{vf}} \,||\, \mathrm{EMG_{req}}\right) \quad (13)$$

  All emergency packets are then encrypted using the key: $\mathrm{C} = \mathrm{Enc_{SK_{emg\_vf}}}(\mathrm{payload})$. Upon emergency session termination, $\mathrm{SK_{emg\_vf}}$ is securely erased.
- Logging and forensic traceability: Every verified emergency event is logged as:

$$\mathrm{L_{emg}} = \left\{\mathrm{ID_v}, \mathrm{T\_emg}, \mathrm{Type_{emg}}, \Psi_{\mathrm{emg_x}}, \sigma_{\mathrm{emg}}\right\} \quad (14)$$

  These logs are stored securely within the fog node storage and periodically transmitted to the TA for audit and forensic validation. They are also accessible to authorized responders for liability tracing.

F. Phase 6: Post-Session Logging and Audit

This final phase addresses the need for accountability, traceability, and long-term analysis of authentication sessions and emergency events. All critical operations are securely logged by the FS and periodically audited by the TA to detect misbehavior, support forensic investigation, and enable system-wide trust assessment.

- Logging architecture and content: Every session between a vehicle OBU and a fog node results in a structured log entry $\mathrm{L_x}$ capturing essential elements:

$$\mathrm{L_x} = \{\mathrm{ID_v}, \mathrm{ID_f}, \mathrm{T_{start}}, \mathrm{T_{end}}, \mathrm{SK_{vf}^{hash}}, \Psi_{\mathrm{live_x}}, \mathrm{Status}, \sigma_{\mathrm{log}}\} \quad (15)$$

  where $\mathrm{T_{start}}, \mathrm{T_{end}}$ are the session timestamps, $\mathrm{SK_{vf}^{hash}} = \mathrm{h}(\mathrm{SK_{vf}})$ stores a hashed fingerprint of the session key, $\Psi_{\mathrm{live_x}}$ is the validated sensor profile, $\mathrm{Status} \in \{\mathrm{Valid}, \mathrm{Tamper\ Detected}, \mathrm{SpoofFlagged}, \mathrm{EmergencyTriggered}\}$, and $\sigma_{\mathrm{log}} = \mathrm{Sign_{k_f}}(\mathrm{L_x})$ is a digital signature by the fog node.
- Secure log storage and access control: Fog nodes append log entries to a secure log file $\mathrm{F_{log}}$, protected by write-once hash chains:

$$\mathrm{H_i} = \mathrm{h}(\mathrm{L_i} \,||\, \mathrm{H_{i-1}}), \;\; \mathrm{H_0} = \mathrm{h}(\mathrm{Init}) \quad (16)$$

  The access to the logs is controlled via role-based permissions. Only authorized auditors (TA, certified investigators) can read logs, which are encrypted using the TA's public key $\mathrm{K_{TA}}$.
- Periodic audit and forensic validation: At regular intervals, Δ_{audit}, the FS transmits logs to the TA for verification and archival. The TA performs: (i) signature verification: $\mathrm{Verify_{K_f}}(\mathrm{L_x}, \sigma_{\mathrm{log}}) ? = \mathrm{TRUE}$; (ii) log consistency check: $\mathrm{H_i} ? = \mathrm{h}(\mathrm{L_i} \,||\, \mathrm{H_{i-1}})$; and (iii) statistical anomaly analysis to detect malicious patterns.
- Emergency session flagging and compliance: For sessions marked as emergency, $\mathrm{L_{emg}} \subset \mathrm{L_x}$ is extracted and flagged for priority handling. A compliance report is auto-generated to ensure proper key usage, timestamp validation, and responder alert generation. Reports are forwarded to authorized public safety units for policy and legal compliance.
- Log retention and blockchain extension (optional): To extend trust and resilience, logs may optionally be committed to a consortium blockchain:

$$\mathrm{Tx_{log}} = \mathrm{Commit}(\mathrm{L_x}, \mathrm{H_i}) \quad (17)$$

  Each block is signed by the TA and timestamped. Privacy-preserving techniques (e.g., zero-knowledge proofs or anonymized logs) can be applied to comply with regional data regulations.

V. SECURITY ANALYSIS

In this section, we discuss the security goals and threat models for the proposed model in the context of vehicular fog computing. We prove that the system can withstand different attack vectors and provide formal security guarantees both from cryptographic construction and behavioral integrity validation.

A. Threat Model

The adversary $\mathcal{A}$ is assumed to have the following capabilities:

- Eavesdropping on wireless channels between OBUs and fog nodes.
- Message injection, modification, or replay.
- Physical access to OBUs (e.g., stolen vehicle or roadside tampering).
- Attempting to spoof sensor data (e.g., GPS, IMU, LiDAR) using relay attacks or falsified signals.
- Internal misbehavior by compromised OBUs or rogue fog nodes.

The system must remain secure even in partial compromise scenarios.

B. Security Goals Achieved

The proposed framework achieves the following core security properties:

- Mutual authentication: Vehicles and fog nodes exchange digital signatures over Chebyshev polynomial-derived key materials and verified public keys:

$$\text{Verify}_{K_v}(\sigma_v) \Rightarrow \text{Authentic Vehicle},$$

$$\text{Verify}_{K_f}(\sigma_f) \Rightarrow \text{Authentic Fog} \quad (18)$$

This ensures both parties are authenticated before session key establishment.

- Perfect forward secrecy: Session key SK_{vf} is derived using ephemeral nonces:

$$SK_{vf} = h(T^{\rho k_v}(N_f) \,||\, T^{\rho k_f}(N_v)) \quad (19)$$

Even if long-term keys are compromised, past session keys remain secure.

- Replay resistance: All messages include fresh timestamps and nonces (T_v, T_f, N_v, N_f) and are discarded if: $|T_{recv} - T_{sent}| > \Delta_T$.
- Tamper detection: Runtime hardware integrity is monitored via the signal hash:

$$\tau_x(t) = h(\delta_{P(t)} \,||\, \delta_{C(t)} \,||\, \delta_{M(t)}),\ \tau_x(t) ?< \theta_{tamper} \quad (20)$$

Exceeding this threshold triggers alerts and key erasure.

- Sensor spoofing resistance: Verified by: (i) entropy check: $H(S_i) ?> \theta_H$; (ii) multi-sensor correlation: $\rho_{ij} ?> \theta_{corr}$, and (iii) profile hash validation: $\Psi_{live_x}(t) ?= \Psi_x$.
- Emergency message integrity: Emergency requests are signed and encrypted with ephemeral keys:

$$\sigma_{emg} = \text{Sign}_{K_v}(EMR_{req}), SK_{emg} = h(SK_{vf} \,||\, EMR_{req}) \quad (21)$$

- Traceability and accountability: Actions are logged as:

$$L_x = \{ID_v, ID_f, \Psi_{live}, \text{Status}, \sigma_{log}\} \quad (22)$$

Chained hashes ensure log integrity: $H_i = h(L_i \,||\, H_{i-1})$.

C. Security Comparison

To demonstrate the advantages of the proposed authentication scheme, we compare it with several state-of-the-art schemes for 5G-based vehicular fog computing. These include the most recent Chebyshev-based methods: the fog-based pseudonym scheme FC-PA [26], certificateless authentication ECA-VFog [27], and post-quantum security OTAuth [28]. From the comparison shown in Table I, some existing solutions satisfy minimum requirements such as mutual authentication and replay protection. However, they do not address critical threats including sensor spoofing, physical tampering, or emergency-aware message integrity.

TABLE I. SECURITY FEATURE COMPARISON WITH EXISTING SCHEMES

Security feature	Proposed	FC-PA [26]	ECA-VFog [27]	OTAuth [28]
Post-quantum resistance	✓	✗	✗	✓
Tamper & spoofing detection	✓	✗	✗	✓
Mutual authentication	✓	✓	✓	✓
Forward Secrecy (PFS)	✓	✗	✗	✓
Linkability resistance	✓	✗	✓	✓
Key revocation support	✓	✗	✓	✓
Emergency message integrity	✓	✗	✗	✓
Replay attack protection	✓	✓	✓	✓
Privacy preservation	✓	✓	✓	✓
Auditability / logs	✓	✗	✓	✓
Formal security verification	✓	✓	✓	✓

VI. PERFORMANCE EVALUATION

In this section, we evaluate the computational efficiency, communication overhead, and scalability of the proposed authentication scheme. The results are compared against recent benchmark schemes, including FC-PA [26], ECA-VFog [27], and OTAuth [28]. The evaluation of the proposed authentication scheme was carried out using a hybrid approach combining simulation modeling and empirical micro-benchmarking of cryptographic primitives. The testbed was modeled to reflect a typical vehicular fog computing setup, where Raspberry Pi 4 Model B devices (4 GB RAM, Quad-core Cortex-A72, 1.5 GHz) were used to emulate OBUs, and edge servers with Intel Core i7-10700 CPUs (8 cores, 2.9 GHz, 16 GB RAM) represented the fog nodes.

Cryptographic primitives used in the protocol, namely Chebyshev polynomial evaluation, hash computation, digital signature generation and verification, and symmetric encryption, were implemented in Python 3.10, with cryptographic functions executed through the cryptography, numpy, and secrets libraries. Each primitive was run in

isolation over 10,000 iterations to collect average operation times, which were then used to parameterize a custom discrete-event simulation model developed in SimPy.

Communication overhead was estimated by serializing actual protocol messages (containing identity tags, nonces, timestamps, sensor hashes, and signatures) into JSON format and computing their byte sizes. Storage overhead was derived by summing the memory requirements of static credentials, sensor profile hashes, and session-specific ephemeral keys. Logging overhead was excluded from the primary storage metrics but considered separately in the audit model.

All simulation runs were repeated five times under consistent environmental conditions to ensure reproducibility and statistical stability. The resulting performance metrics, including computation time, communication volume, and storage footprint, were then compared against benchmark values reported in existing protocols (FC-PA, ECA-VFog, OTAuth) under similar hardware assumptions.

A. Computation Time Comparison

We use standard operation-time benchmarks for cryptographic primitives: a hash operation (h) requires 0.03 ms, a Chebyshev polynomial (T^{pk}) requires 0.21 ms, a signature generation (Sign) requires 0.98 ms, a signature verification (Verify) requires 1.12 ms, and symmetric encryption/decryption requires 0.05 ms. Based on these operation-time benchmarks, the total computation time per authentication session (vehicle and fog node) is evaluated.

The proposed scheme achieves lightweight processing by restricting the use of computationally expensive asymmetric cryptography to the session initialization phase only. As shown in Figure 3, the proposed authentication scheme outperforms existing methodologies in terms of computation time. In particular, the proposed scheme achieves 3.61 ms, OTAuth achieves 7.18 ms, ECA-VFog achieves 6.41 ms, and FC-PA achieves 5.34 ms. The lower computational complexity of the proposed scheme demonstrates its efficiency and suitability for vehicular fog computing environments, which have limited computing resources and strict low-latency requirements. This efficiency is key to ensuring reliable and secure data communications.

B. Communication Overhead Comparison

Communication overhead is a critical performance metric in vehicular networks due to limited bandwidth and latency sensitivity, especially in 5G-assisted scenarios. The total message size per authentication session includes identity tags, nonces, timestamps, signatures, sensor profile hashes, and encrypted payloads. The proposed scheme reduces this overhead by using lightweight Chebyshev polynomial-based computations and hash chaining, instead of heavy certificates or pairing-based primitives.

A comparison of the communication overhead per session (sum of all messages exchanged between OBU and FS) with state-of-the-art protocols is shown in Figure 4. The proposed scheme achieves minimal communication cost due to a hash-based sensor profile representation instead of transmitting raw sensor data, a compact Chebyshev-based public key instead of elliptic curve or pairing-based keys, and low overhead for headers in emergency session isolation due to symmetric key derivation. These optimizations render the scheme highly suitable for 5G-V2X environments, where low message latency and minimal channel contention are essential.

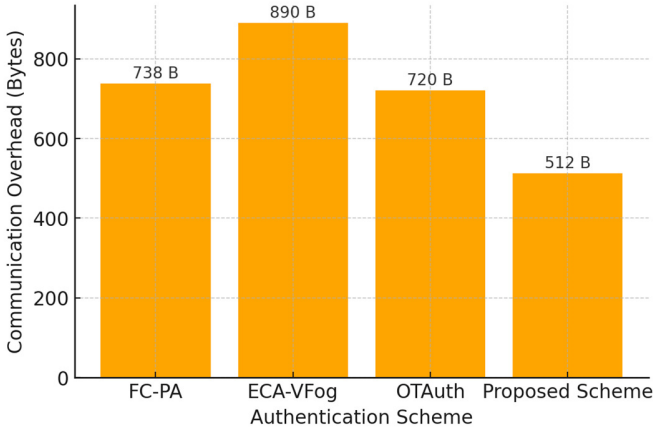

Fig. 3. Communication overhead for the proposed scheme and benchmark methods.

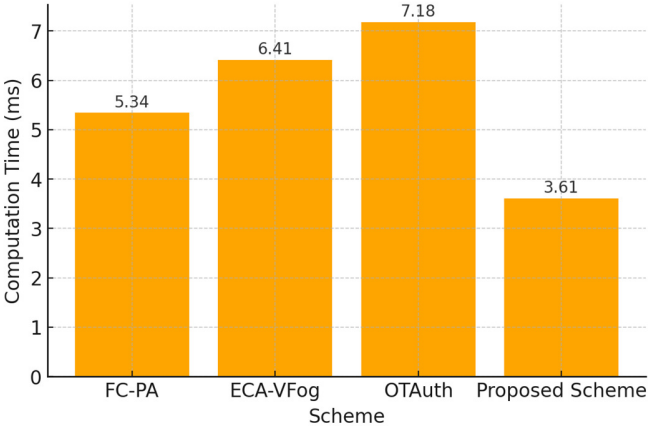

Fig. 4. Computation time for the proposed scheme and benchmark methods.

C. Storage Overhead Comparison

Storage efficiency is a critical factor in vehicular applications, especially for OBUs that operate in resource-constrained environments with limited memory and processing capacity. Excessive storage overhead not only increases implementation costs but can also negatively impact performance and scalability in large-scale vehicular networks. This subsection examines the storage requirements for cryptographic keys, session states, and dynamic data in state-of-the-art stateful authentication protocols.

In the proposed design, the OBU and fog node cache only the minimal necessary data, including credentials, sensor hashes, and short-term session keys. Only fingerprints of certificates and essential shared information are stored locally. Figure 5 presents the total estimated storage overhead per node (excluding logs).

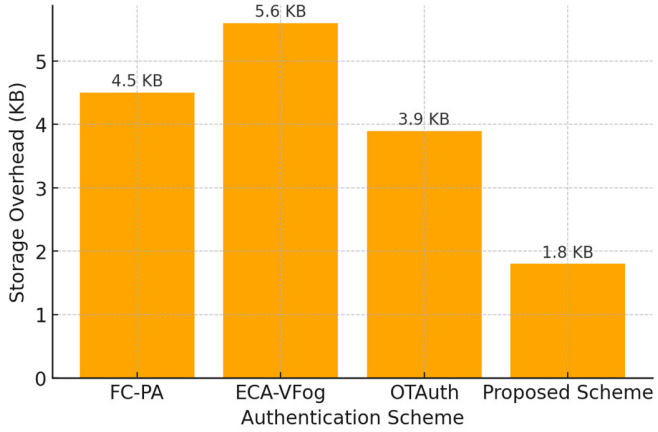

Fig. 5. Storage overhead for the proposed scheme and benchmark methods.

VII. CONCLUSION AND FUTURE WORK

We proposed an efficient, lightweight, sensor-aware authentication protocol, suitable for fog nodes with limited computational capabilities in vehicular 5G environments. The scheme overcomes key limitations of existing protocols by integrating real-time tamper detection, sensor spoofing resilience through an entropy-based algorithm, and emergency message integrity, which are absent in most prior approaches. Using Chebyshev polynomial cryptography and local Trusted Execution Environments (TEEs), the protocol achieves strong mutual authentication, session freshness, and forward secrecy with low computation and communication overhead.

The thorough security analysis demonstrates that the scheme is resilient to physical tampering, impersonation, replay, and linkability attacks. The performance evaluations indicate substantial reductions in computation time, memory utilization, and communication overhead compared to state-of-the-art approaches, suggesting that the solution is well-suited for resource-constrained vehicular networks.

Future work will focus on combining the protocol with advanced post-quantum cryptographic primitives, incorporating machine learning for dynamic anomaly detection, and evaluating performance under realistic urban mobility models to improve scalability and resilience against next-generation threats.

Although the proposed tamper-resilient and sensor-aware authentication protocol demonstrates promising results in terms of computational efficiency and security guarantees, several limitations remain. First, the evaluation was limited to analytical calculations and lightweight simulations. A more comprehensive validation using realistic Vehicular Ad Hoc Network (VANET) testbeds, such as OMNeT++ integrated with SUMO, or hardware-in-the-loop experiments with actual Onboard Units (OBUs) and Fog Servers (FSs), would strengthen practical applicability. Second, the current sensor spoofing detection relies on entropy and correlation checks, which may produce false positives or negatives in dynamic traffic environments. Incorporating machine learning-based anomaly detection could improve accuracy and adaptability. Third, while Chebyshev polynomials provide lightweight and potentially post-quantum-resilient operations, integrating standardized post-quantum cryptographic primitives such as lattice-based or hash-based signatures (e.g., Dilithium, SPHINCS+) would enhance future readiness against quantum-powered adversaries.

Additionally, the protocol has not yet addressed energy consumption trade-offs on resource-constrained OBUs, which should be analyzed alongside latency and throughput. Finally, future work should extend the comparative analysis to include more recent authentication schemes, such as lattice-based Certificate-less Post-Quantum Privacy-preserving Authentication (CPPA) and zero-trust mobility frameworks, to highlight competitiveness against state-of-the-art protocols.

AUTHOR CONTRIBUTIONS

Sarah Al-Hilfi conducted the literature review and assisted with the experimental setup and performance evaluation in the revised version. Mohammed Yousif led the cryptographic design of the authentication protocol and contributed significantly to the implementation of the Chebyshev polynomial-based framework. Huda Mohammed Alsayednoor conducted the literature review and assisted with the experimental setup and performance evaluation. Mahmood A. Al-Shareeda (corresponding author) supervised the overall research, contributed to the design of the tamper detection and audit logging mechanisms, and conducted formal protocol verification. Mohammed Almaayah contributed to the design of the entropy-based sensor spoofing detection module and provided insights into cross-sensor validation. Marwan Albahar assisted with the comparative analysis and contributed to refining the manuscript through technical review and proofreading. All authors have read and approved the final manuscript.

FUNDING

This research work was funded by Umm Al-Qura University, Saudi Arabia, under grant number 25UQU4400257GSSR56.

ACKNOWLEDGMENT

The authors extend their appreciation to Umm Al-Qura University, Saudi Arabia, for funding this research work through grant number 25UQU4400257GSSR56.

REFERENCES

[1] A. Behura, A. Kumar, and P. K. Jain, "A comparative performance analysis of vehicular routing protocols in intelligent transportation systems: A comparative performance analysis of vehicular routing protocols...," *Telecommunication Systems*, vol. 88, no. 1, Mar. 2025, Art. no. 26, https://doi.org/10.1007/s11235-024-01243-1.

[2] H. Al-Maliki, H. A. A. AL-Asadi, Z. A. Abduljabbar, and V. O. Nyangaresi, "Reliable Vehicular Ad Hoc Networks for Intelligent Transportation Systems based on the Snake Optimization Algorithm," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18631–18639, Dec. 2024, https://doi.org/10.48084/etasr.8851.

[3] Z. G. Al-Mekhlaf *et al.*, "A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems," *Journal of King Saud University Computer and Information Sciences*, vol. 37, no. 6, Jul. 2025, Art. no. 126, https://doi.org/10.1007/s44443-025-00140-0.

[4] K. S. El Gayyar, A. I. Saleh, and L. M. Labib, "A new fog-based routing strategy (FBRS) for vehicular ad-hoc networks," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 386–407, Jan. 2022, https://doi.org/10.1007/s12083-021-01197-0.

[5] O. Nazih, N. Benamar, H. Lamaazi, and H. Chaoui, "Toward Secure and Trustworthy Vehicular Fog Computing: A Survey," *IEEE Access*, vol. 12, pp. 35154–35171, 2024, https://doi.org/10.1109/ACCESS.2024.3371488.

[6] B. A. Mohammed *et al.*, "Taxonomy-Based Lightweight Cryptographic Frameworks for Secure Industrial IoT: A Survey," *IEEE Internet of Things Journal*, 2025, https://doi.org/10.1109/JIOT.2025.3595649.

[7] A. M. Farooqi, M. A. Alam, S. I. Hassan, and S. M. Idrees, "A Fog Computing Model for VANET to Reduce Latency and Delay Using 5G Network in Smart City Transportation," *Applied Sciences*, vol. 12, no. 4, Feb. 2022, Art. no. 2083, https://doi.org/10.3390/app12042083.

[8] R. Maruthamuthu, N. Patel, T. Yawanikha, S. Jayasree, Z. Alsalami, and S. P. V. SubbaRao, "A Way to Design Fog Computing Model For 5G Network using Vanet," in *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering*, Greater Noida, India, 2024, pp. 431–435, https://doi.org/10.1109/ICACITE60783.2024.10617287.

[9] G. Lippi, M. Aljawarneh, Q. Al-Na'amneh, R. Hazaymih, and L. D. Dhomeja, "Security and Privacy Challenges and Solutions in Autonomous Driving Systems: A Comprehensive Review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 23–41, May 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.3.

[10] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A Hybrid Genetic Algorithm and Hidden Markov Model-Based Hashing Technique for Robust Data Security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 42–56, May 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.6.

[11] N. Keshari, D. Singh, and A. K. Maurya, "A survey on Vehicular Fog Computing: Current state-of-the-art and future directions," *Vehicular Communications*, vol. 38, Dec. 2022, Art. no. 100512, https://doi.org/10.1016/j.vehcom.2022.100512.

[12] M. A. Al-Shareeda, A. A. Obaid, and A. A. H. Almaji, "The Role of Artificial Intelligence in Bodybuilding: A Systematic Review of Applications, Challenges, and Future Prospects," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 16–26, Feb. 2025.

[13] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 27–36, Mar. 2025.

[14] M. H. Husain, M. Ahmadi, and F. Mardukhi, "Vehicular Fog Computing: A Survey of Architectures, Resource Management, Challenges and Emerging Trends," *Wireless Personal Communications*, vol. 136, no. 4, pp. 2243–2273, Jun. 2024, https://doi.org/10.1007/s11277-024-11373-z.

[15] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions," *ACM Computing Surveys*, vol. 56, no. 10, Jun. 2024, Art. no. 260, https://doi.org/10.1145/3656166.

[16] A. A. Khan, M. Abolhasan, and W. Ni, "5G next generation VANETs using SDN and fog computing framework," in *2018 15th IEEE Annual Consumer Communications & Networking Conference*, Las Vegas, NV, USA, 2018, pp. 1–6, https://doi.org/10.1109/CCNC.2018.8319192.

[17] A. Bisht and V. Khaitan, "Reliability analysis of 5G-VANET using cloud-fog-edge based architecture," *RAIRO - Operations Research*, vol. 58, no. 1, pp. 129–149, Jan. 2024, https://doi.org/10.1051/ro/2023189.

[18] T. Alsalem and M. Amin, "Towards Trustworthy IoT Systems: Cybersecurity Threats, Frameworks, and Future Directions," *Journal of Cyber Security and Risk Auditing*, vol. 2023, no. 1, pp. 3–18, Feb. 2023, https://doi.org/10.63180/jcsra.thestap.2023.1.2.

[19] A. Rachmayanti and W. Wirawan, "Elliptic Curve Cryptography (ECC) Based Authentication Scheme on IoT Networks for Health Information Systems," in *2024 International Seminar on Intelligent Technology and Its Applications*, Mataram, Indonesia, 2024, pp. 125–130, https://doi.org/10.1109/ISITIA63062.2024.10668289.

[20] V. Abdullayev, A. Khang, N. Ragimova, and M. Almaayah, "A Novel Authentication Systems in Vehicular Communication: Challenges and Future Directions," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 123–135, Aug. 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.9.

[21] S. R. Addula, S. Norozpour, and M. Amin, "Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 37–48, Mar. 2025.

[22] R. Huang and A. Sharma, "Post-Quantum Verifiable Decryption Scheme for Internet of Thing-Based Consumer Electronic Edge Device," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4903–4913, May 2025, https://doi.org/10.1109/TCE.2025.3572470.

[23] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 2, pp. 1674–1683, Feb. 2025, https://doi.org/10.1109/TII.2024.3485796.

[24] S. Ahmed and M. H. Anisi, "A Post-Quantum Secure Federated Learning Framework for Cross-Domain V2G Authentication," *IEEE Transactions on Consumer Electronics*, 2025, https://doi.org/10.1109/TCE.2025.3580338.

[25] N. N. Minhas and K. Mansoor, "Edge-Computing-Based Scheme for Post-Quantum IoT Security for e-Health," *IEEE Internet of Things Journal*, vol. 11, no. 19, pp. 31331–31337, Oct. 2024, https://doi.org/10.1109/JIOT.2024.3418959.

[26] B. A. Mohammed *et al.*, "FC-PA: Fog Computing-Based Pseudonym Authentication Scheme in 5G-Enabled Vehicular Networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023, https://doi.org/10.1109/ACCESS.2023.3247222.

[27] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *Plos One*, vol. 18, no. 6, Jun. 2023, Art. no. e0287291, https://doi.org/10.1371/journal.pone.0287291.

[28] Z. Ghaleb Al-Mekhlafi *et al.*, "Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing," *IEEE Access*, vol. 12, pp. 100152–100166, 2024, https://doi.org/10.1109/ACCESS.2024.3429179.

[29] Y. Bi and C. Jia, "Towards Resilience 5G-V2N: Efficient and Privacy-Preserving Authentication Protocol for Multi-Service Access and Handover," *IEEE Transactions on Mobile Computing*, vol. 24, no. 6, pp. 5446–5463, Jun. 2025, https://doi.org/10.1109/TMC.2025.3532120.

[30] S. K. Rajbhar, S. Singh, and D. Kumar, "Dynamic and Secure Group Authentication for 5G-Enabled Vehicular Networks," in *2025 International Conference on Electronics, AI and Computing*, Jalandhar, India, 2025, pp. 1–6, https://doi.org/10.1109/EAIC66483.2025.11101378.

[31] H. Zhang and M. Li, "Towards an intelligent and automatic irrigation system based on internet of things with authentication feature in VANET," *Journal of Information Security and Applications*, vol. 88, Feb. 2025, Art. no. 103927, https://doi.org/10.1016/j.jisa.2024.103927.

[32] P. Kumar and H. Om, "Multi-TA model-based conditional privacy-preserving authentication protocol for fog-enabled VANET," *Vehicular Communications*, vol. 47, Jun. 2024, Art. no. 100785, https://doi.org/10.1016/j.vehcom.2024.100785.

[33] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A Fog Computing and Blockchain-based Anonymous Authentication Scheme to Enhance Security in VANET Environments," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19143–19153, Feb. 2025, https://doi.org/10.48084/etasr.8663.

[34] Y. Zhou *et al.*, "An Efficient Identity Authentication Scheme With Dynamic Anonymity for VANETs," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 10052–10065, Jun. 2023, https://doi.org/10.1109/JIOT.2023.3236699.

[35] B. A. Mohammed *et al.*, "Efficient Blockchain-Based Pseudonym Authentication Scheme Supporting Revocation for 5G-Assisted Vehicular Fog Computing," *IEEE Access*, vol. 12, pp. 33089–33099, 2024, https://doi.org/10.1109/ACCESS.2024.3372390.

[36] X. Chen, A. Yang, Y. Tong, J. Weng, J. Weng, and T. Li, "A Multisignature-Based Secure and OBU-Friendly Emergency Reporting Scheme in VANET," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 23130–23141, Nov. 2022, https://doi.org/10.1109/JIOT.2022.3184991.

[37] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, M. A. Al-Shareeda, B. A. Mohammed, J. S. Alshudukhi, and K. A. Al-Dhlan, "Fog computing and blockchain technology based certificateless authentication scheme in 5G-assisted vehicular communication," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3703–3721, Nov. 2024, https://doi.org/10.1007/s12083-024-01778-9.

[38] M. Wang *et al.*, "Smart City Transportation: A VANET Edge Computing Model to Minimize Latency and Delay Utilizing 5G Network," *Journal of Grid Computing*, vol. 22, no. 1, Feb. 2024, Art. no. 25, https://doi.org/10.1007/s10723-024-09747-5.

[39] Y. Liang, E. Luo, and Y. Liu, "Physically Secure and Conditional-Privacy Authenticated Key Agreement for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 7914–7925, Jun. 2023, https://doi.org/10.1109/TVT.2023.3241882.

[40] W. Othman, M. Fuyou, K. Xue, and A. Hawbani, "Physically Secure Lightweight and Privacy-Preserving Message Authentication Protocol for VANET in Smart City," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12902–12917, Dec. 2021, https://doi.org/10.1109/TVT.2021.3121449.

[41] A. Altaweel, H. Mukkath, and I. Kamel, "GPS Spoofing Attacks in FANETs: A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 55233–55280, 2023, https://doi.org/10.1109/ACCESS.2023.3281731.

[42] K. Lim, K. M. Tuladhar, and H. Kim, "Detecting Location Spoofing using ADAS sensors in VANETs," in *2019 16th IEEE Annual Consumer Communications & Networking Conference*, Las Vegas, NV, USA, 2019, pp. 1–4, https://doi.org/10.1109/CCNC.2019.8651763.

[43] A. Nobahari, D. Bakhshayeshi Avval, A. Akhbari, and S. Nobahary, "Investigation of Different Mechanisms to Detect Misbehaving Nodes in Vehicle Ad-Hoc Networks (VANETs)," *Security and Communication Networks*, vol. 2023, no. 1, Aug. 2023, Art. no. 4020275, https://doi.org/10.1155/2023/4020275.

[44] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks," *IEEE Access*, vol. 12, pp. 6251–6261, 2024, https://doi.org/10.1109/ACCESS.2024.3351278.

[45] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-Fog: A Novel Anonymous Authentication Scheme for 5G-Enabled Vehicular Fog Computing," *Mathematics*, vol. 11, no. 6, Mar. 2023, Art. no. 1446, https://doi.org/10.3390/math11061446.

[46] Z. Ghaleb Al-Mekhlafi *et al.*, "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575–29602, Oct. 2024, https://doi.org/10.1109/JSEN.2024.3436612.

[47] T. K. Venkatasamy, M. J. Hossen, G. Ramasamy, and N. H. B. A. Aziz, "Intrusion detection system for V2X communication in VANET networks using machine learning-based cryptographic protocols," *Scientific Reports*, vol. 14, no. 1, Dec. 2024, Art. no. 31780, https://doi.org/10.1038/s41598-024-82313-x.