A HMAC-Based Token Authentication Protocol with Bloom Filter Revocation for Fog-Assisted Vehicular Networks

Hussein Asaad Shakir Al-Khalaf[1,*], Ali Hussein Ali AL-Iedani[1], Muhammad N. Jawad [2], Huda Mohammed Alsayednoor [3], Mahmood A. Al-Shareeda [4,5,*], Mohammed Almaayah[6], Rami Shehab[7]
[1]College of Oil and Gas Engineering, Basra University For Oil and Gas, Basra, Iraq
[2]College of Oil andGas Engineering, Department of Polymers and Petrochemical Engineering, Basra University for Oil and Gas, Basra, Iraq
[3]Shatt Al-Arab University College, Basra, Iraq
[4]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[5]College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[6]King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[7]Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
E-Mail: hussein.assad@buog.edu.iq, ali29@buog.edu.iq, mahmood.alshareedah@stu.edu.iq, m.almaiah@ju.edu.jo, Rtshehab@kfu.edu.sa
*Corresponding author

Keywords: Vehicular fog computing, lightweight authentication, pseudonym privacy, session key management, token revocation, HMAC-based protocols, 5G vehicular networks, forward secrecy, unlinkability, AVISPA verification

Received: September 21, 2025

In this paper, we propose five round HMAC-based token authentication protocol with Bloom filter revocation for Fog-assisted Vehicular Networks (FAVN). The proposed concept includes (i) secure bootstrap, (ii) light-weight mutual authentication; (iii) dynamic session key establishment, (iv) Bloom filter-based revocation token distribution, and; v) key refresh and pseudonym rebinding. Utilizing only lightweight symmetric cryptographic operations (e.g., HMAC and hash) this system achieves mutual authentication, unlinkability and fine grained revocability without requiring the usual asymmetric primitives or any certificates. Formal verification with the help of AVISPA tool show resistance against impersonation, replay and man-in-the-middle attack under Dolev–Yao model. Experimental results show that each session incur the average cryptographic processing delay with 2.10 ms, communication cost is only 512 bytes, and storage overhead is with 1.8 KB per vehicle. The optimal solution is compared to the state-of-the-art ECC and pairing-based methods and there it is observed that the proposed framework minimizes more than 35 % of computational cost, 42.5 % communication overhead, which can be scalable as well a privacy preserving manner in an enormous real-time automotive authentication for 5G-enabled vehicular fog architecture.

Povzetek:

1 Introduction

The rapid development of 5G communication, edge computing, and vehicle ad hoc networks (VANETs) is accelerating the revolution of intelligent transportation systems (ITS)[1, 2, 3]. Among the new architectures, Fog-Assisted Vehicular Systems (FAVS) is a proposed solution, which employs fog nodes or Roadside Units (RSUs) to support localized computation, to process data based on context awareness, and to provide low-latency communication as a result of simultaneous communication between vehicles and infrastructure[4, 5, 6]. They are required for the existence of safety-critical applications such as alert systems (e.g., emergencies), collision avoidance, path planning, and traffic management[7, 8, 9].

However, on the other hand, the overlay of fog computing over the vehicular networks extends the attack surface further and also increases the complexity of the threats. By nature of being a mobile system with wireless communication, vehicles are vulnerable to impersonation, replay, man-in-the-middle (MITM), session hijacking, and DoS attack[10, 11]. Next, physical tampering with On-Board Units (OBUs) will lead to the leakage of credentials, in which way attackers are able to forge messages or conduct linkability analysis among pseudonymous sessions[12, 13]. Thus, providing secure, privacy-preserving, and revocable authentication is one of the main tasks in vehicular fog environments[14, 15].

Classical authentication approaches for vehicular networks are based either on heavyweight cryptographic functions (such as bilinear pairings or digital certificates) or centralized Public Key Infrastructures (PKIs), resulting in significant computational and communicational overhead[16]. These are suboptimal for the real-time and resource-limited

(e.g., onboard units in latency-sensitive ITS scenarios) use cases. Additionally, dynamic key updates, identity revocation, and session unlinkability, which are crucial for high-mobility vehicular scenario where vehicle constantly hops between fog zones, are not handled efficiently in most of the previous protocols[17, 18, 19, 20].

Recent advances in adaptive and nonlinear control theory have motivated a few enhancements that can be adapted to vehicular and fog-assisted systems. For example, the fuzzy-based and neural adaptive techniques have shown that they possess good robustness and convergence properties for either uncertain or nonlinear dynamics. An adaptive fuzzy control for practical fixed-time response dynamics synchronization of fractional-order chaotic systems was presented in [21], where stability with respect to model uncertainties is guaranteed. Also, an output-feedback controller for projective lag-synchronization in uncertain chaotic systems with input nonlinearities has been studied in [22], where finite time complete state synchronization is proposed even without measurement of the full state. In [23], the robust neural adaptive control was submitted for complex multivariable systems robust to parametric uncertainties. In contrast to these trials, backstepping-based adaptive controllers for an uncertain nonlinear system [24] and flexible robotic manipulators are able to achieve better response and tracking performance. Furthermore, in [25] a nonlinear optimal control for gas compressor systems with induction motors was developed, showing the possibility of dynamic optimization as a practical tool. The introduction of these adaptive and intelligent control strategies makes the fog-based vehicular authentication systems more robust, better in synchronization and steady state stabilization, and advanced in real-time adaptability[26].

There are some recent protocols trying to solve these problems. Al-Shareeda et al. [27] presented a light-weight authentication scheme based on Chebyshev polynomial for 5G equipped fog systems. Nevertheless, the architecture fails in fine-grain revocation and pseudonym unlinkability. FC-PA [28] features fog computing and pseudonym masking, with the drawback of high ECC-based overhead, and it lacks a key rebinding mechanism. ECA-VFog [29] also removes the requirement of certificates through a certificateless PKI, but it uses pairing computations that are not feasible for OBUs. For example, OTAuth [30] is a relatively efficient database-oriented scheme with good security, but it requires high communication and storage complexity in addition to limited dynamic token revocation abilities[31, 32].

Against these challenges, this paper proposes a fresh, revocable, and lightweight authentication scheme for the fog-aided vehicular paradigm. To address the problem, we present a token-based authentication scheme with pseudonym rotation, revocation-aware token validation, and per-session symmetric key derivation. The system succeeds in providing strong privacy through unlinkable pseudonyms, efficient revocation through Bloom filter encoding, and achieves low computation overhead using HMAC-based authentication. The main contributions of this paper are:

- We introduce a five-step scheme that performs secure bootstrapping, lightweight mutual authentication, dynamic session key establishment, scalable revocation management, and efficient key update, along with pseudonym rebind.
- Our scheme has mutual authentication, forward secrecy, session unlinkability, and fine-grained revocation.), and our scheme does not employ any asymmetric cryptographic primitives or certificates.
- A revocation distribution scheme based on the Bloom filter allows fat servers to check the freshness of the token in real-time with a constant lookup cost.
- The protocol is fully verified from a formal perspective by the AVISPA tool against Dolev-Yao-like adversaries, showing resistance to impersonation, replay, and MITM attacks.
- Comparative studies with existing state-of-the-art protocols demonstrate an advantage in computational overhead, communication overhead, and storage footprint.

The remainder of this paper is organized as follows. Section 2 shows related works for the VANET system. In Section 3, we present the system and threat model. We give our authentication framework in Section 4. In Section 5, the security analysis and formal verification are described. Performance and comparative Analysis are presented in Section 6. Section 7 shows a discussion of this paper. The work concludes with Section 8.

2 Related work

Because of their popularity and their requirements in low-latency, high-integrity communications, secure user authentication and identity protection are becoming more and more popular, especially in the vehicular environment. In this section, we survey important recent works and discuss their limitations in terms of revocability, session unlinkability, and lightweight design.

Al-Shareeda et al. [27] presented a lightweight emergency authentication technique for 5G-based VFC based on Chebyshev polynomials. The FC-PA protocol proposed by Mohammed et al. [28], a combination of fog computing and pseudonym-based authentication. ECA-VFog, by Almazroi et al. [29], solves the problems of certificate storage and management using the method of certificateless-public-key-cryptography infrastructure (CL-PKI). OTAuth, proposed by Al-Mekhlafi et al. [30] presents a quantum-safe protocol in vehicular edge networks based on oblivious transfer. The protocol has forward secrecy and is AVISPA-verified, but is not token-based, revocable, or session unlinkable. There have also been previous works on

Table 1: Comparative summary of related authentication schemes in vehicular fog computing

Scheme	Auth.	Revoc.	Unlink.	Overhead	Formal Verif.	Main Limitation
Al-Shareeda *et al.* [27]	✓	–	–	Low	✓	No fine-grained revocation
FC-PA [28]	✓	–	–	High	✓	High ECC cost
ECA-VFog [29]	✓	✓	–	High	–	Pairing overhead
OTAuth [30]	✓	–	–	Moderate	✓	Limited scalability
Proposed	✓	✓	✓	**Low**	✓	Not post-quantum secure

group signature schemes and blockchain-based authentication [33, 34, 35], but many of them suffer from high latency, scalability, or require trust for hardware in all components of the infrastructure.

Compared to this, we design a lightweight five-phase token-based authentication protocol to provide revocable pseudonyms, efficient key rebinding, and Bloom filter-based revocation. The usage of symmetric primitives allows for a good computational performance, the per-session token rotation and unlinkable pseudonyms allow for identity (pseudo) anonymity. Moreover, our scheme is security reduced and tailored for restricted vehicular conditions, which are proven to be highly resistant to impersonation, replay, and linkability attacks. To clarify the comparative position of these approaches, Table 1 summarizes key features of the most relevant authentication protocols in vehicular fog computing. As we can see, most of the existing schemes suffer from either costly computation or ineffective revocation and unlinkability. To overcome these drawbacks and yet provide numerical revocation, in dynamic vehicular settings, the authors of this paper present a Bloom filter-based symmetric-only HMAC-inspired framework.

3 System and threat model

3.1 System model

As shown in Figure 1, the system architecture consists of three main entities participating in a 5G-enabled vehicular fog computing system:

- **Trusted Authority (TA)**: This is a fully trusted backend entity that is in charge of system initialisation, key generation, pseudonym management, token issuance, and revocation list management. It takes part only in bootstrapping, updates of keys, and their revocation.
- **OBUs (On-Board Units):** Intelligent vehicular modules that contain a TEE for secure execution of computations, space for storing cryptographic keys and tokens, and interfaces to communicate wirelessly. OBUs authenticate themselves to fog servers with pseudonyms and tokenized keys.
- **Fog servers (FSs):** Semitrusted infrastructure nodes located at the network edge (e.g., RSUs or 5G UDNs). They take charge of the authentication at the local area, revocation check, session key negotiation, and deliver an emergency message to the TA if necessary.

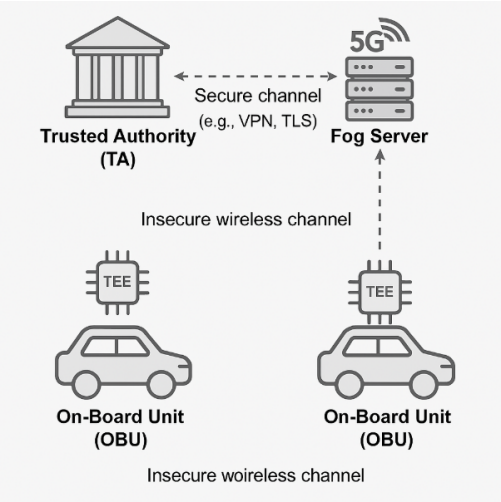

Figure 1: System model

Each OBU is a priori pre-enlisted by the TA with an identifier $\mathcal{ID}_v$, a shared secret key s_k, a private hash key k_h, and a set of pseudonyms $\{Ps_i\}$ along with their tokens $\{T_i\}$, each of them being valid in a certain time interval. TA is assumed to establish secure communication to fog nodes, through a secure channel (e.g.,-VPm or TLS). The wireless V2I links is considered to be eavesdropping-unprotected and clearly observable by the attackers.

3.2 Assumptions

- The TA is fully trusted, stays online for control plane activities, and is never compromised.
- OBUs have TEE to secure sensitive operations and credential storage.
- Fog servers are semi-trusted; they will execute the protocol logic, may be vulnerable to remote attacks and/or denial-of-service attacks.
- The distributed on-demand formation of sessions needs to be lightweight and location-independent, as vehicles often move in and out of fog areas.
- The V2I communication over wireless links is insecure and vulnerable to passive and active adversaries.

3.3 Threat model

Here we assume a Dolev–Yao adversary $\mathcal{A}$ who has complete control over the communication channel (global key exchange with lifetime t) and partial control over some edge devices. The adversary has the following abilities:

- **Eavesdropping:** $\mathcal{A}$ has the capability to eavesdrop on the message transmitted over the air in between OBU and fog server, forward the recorded message to its destination, and analyze it.
- **Message Injection and Tampering:** $\mathcal{A}$ is able to create, modify, or inject messages to counterfeit the sender or tamper with the protocol's state.
- **Replay Attack:** $\mathcal{A}$ can replay a valid token or an old message in order to make an unauthorized session establishment.
- **Token Leakage:** $\mathcal{A}$ may be able to compromise some tokens and try to use them even though they are expired, or partially exposed.
- **Linkability Attack:** $\mathcal{A}$ aims to link sessions across fog zones to reveal the identity of vehicles.
- **Manipulating Fog Node:** A malicious fog server may try to accept a stale token, leak session data, or not properly manage revocation.
- **Physical Access (Reduced):** $\mathcal{A}$ is able to have partial access to OBU, but is unable to memory-snoop secrets out from TEE-protected memory.

3.4 Research design and objectives

Motivation for the reported research stems from a search for an authentication solution, which provides minimum computational overhead, revocability, and unlinkability in a dynamic fog-assisted vehicular environment.

3.4.1 Research questions

Formally, to support the design and analysis, we pose the RQs.

- **RQ1:** Whether or not a symmetric-only authentication scheme with HMAC and token mechanism can achieve mutual authentication, unlinkability, as well as efficient revocation in vehicular fog computing.
- **RQ2:** What is the computational and communication overhead of the proposed HMAC-based framework compared to existing ECC and pairing-based authentication schemes?

  RQ3: What are the trade-offs of adopting Bloom filter-based revocation lists in terms of accuracy (i.e., false-positive rate) and scalability across fog nodes?
- **RQ4:** What is the performance of the proposed approach in providing forward secrecy and session freshness while considering the constraints of existing vehicular hardware resources?

3.4.2 Research objectives

These questions determine the purpose of this communication, which is:

1. To propose a light-weight, non-repudiation and privacy-controlled authentication protocol with revocation, where symmetric operations are sufficient, that is applicable in 5G supported vehicular fog networks.
2. To incorporate Bloom filter-based revocation, with efficient validation as a low computational and constant lookup cost.
3. The formal verification of the proposed protocol using the AVISPA tool in the framework of the Dolev–Yao adversary.
4. To compare and analyze with the proposed scheme to focus on computation, communication, and storage overheads with previous existing schemes.

3.4.3 Research hypotheses

The following hypotheses were empirically tested through simulation and analytical analysis:

- **H1:** It is possible for a symmetric-only HMAC-based authentication framework to have similar performance or better than ECC-based approaches while retaining privacy and being scalable.
- **H2:** Bloom filter-based revocation facilitates a constant-time verification with an insignificant(false positive) rate as long as it is suitably parameterized.
- **H3:** The proposed architecture achieves practical FS and UL within sub-3 ms processing delay, this meets real-time VN demand.

4 Proposed scheme

All five phases of the proposed authentication framework form an integrated security cycle that collectively exceed an efficient, revocable, dynamic, and dependable identity protection in fog-assisted vehicular networks. In terms of Figure 2, the system initiates with Phase 1: Secure Bootstrapping, where TA offers pseudonyms, cryptographic tokens, and credentials to each vehicle. This data is securely stored within a TEE. In Phase 2: Lightweight Mutual Authentication, OBUs and fog servers conduct a rapid, symmetric-based handshake with HMAC and pseudonym-bound tokens to establish trust with the minimum overhead possible. Subsequent successful authentication, Phase 3: Dynamic

Session Key Derivation and Rebinding securely generates a session-specific symmetric key that supports both forward secrecy and ephemeral session confidentiality. When the tokens or pseudonyms are revoked due to expiration or compromise, Phase 4: Revocation Token Distribution allows fog servers to verify freshness using Bloom filter-based verification, which maintains scalability. Lastly, Phase 5: Key Update and Rebinding Protocol enforces secure universal rotation of the pseudonyms and keys without full re-registration, which enforces privacy preservation and seamless region migration. Integration of these phases forms an efficient authentication cycle that is resistant to common vehicular attacks, such as impersonation attacks and replay attacks, and session linkability.

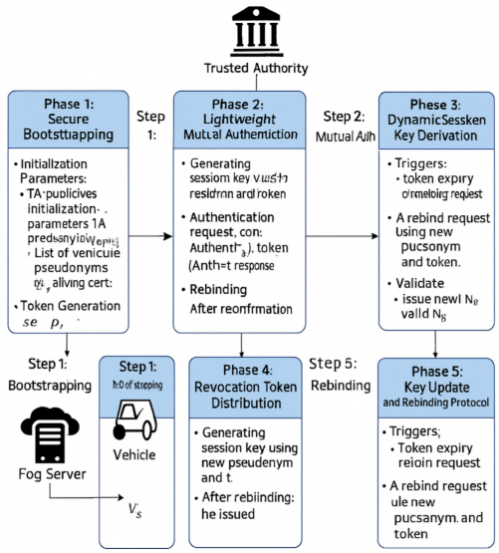

Figure 2: Overall workflow of the proposed authentication framework

4.1 Phase 1: secure bootstrapping

In this phase, the Trusted Authority (TA) predistributes to each vehicle a unique identity and a pre-shared cryptographic material to be used in secure and revocable communications in the fog-assisted vehicular network. All credentials are provisioned and stored in the vehicle TEE.

- Initialization Parameters: TA publishes the system-wide parameters: A symmetric master key K_{TA} that is shared between registered fog servers. A list of vehicle pseudo names $\{Ps_i\}$ along with their respective short-lived session intervals t_i. A secure hash private key k_h and shared secret private key s_k for each vehicle V_x.
- Token Generation: For every vehicle V_x, the TA generates a set of revocable authentication tokens as follows: $T_i = \text{HMAC}_{k_h}(Ps_i \,\|\, t_i)$. The set of tokens $\mathcal{T}_v = \{T_1, T_2, \ldots, T_n\}$ is stored securely in the OBU's secure storage. The token index is associated to its activation window of time, allowing timed rotation and unlinkability.
- Vehicle ID Binding: The long-term ID $\mathcal{ID}_v$ is tied to a registration certificate by the TA, which is only applied for in registration and emergency recovery mode:

$$\text{Cert}v = \text{Sign}K_{\text{TA}}(\mathcal{ID}_v, k_v, \{\text{Ps}_i\}) \quad (1)$$

The encrypted certificate is resident and only used under TEE protection.

- Bootstrapping Message Format: The format of the bootstrapping exchange between vehicle V_x and TA is as follows:

$$\text{Boot}_x = \{\mathcal{ID}_v, k_v, k_h, \{Ps_i\}, \mathcal{T}_v, \text{Cert}_v\} \quad (2)$$

This message is encrypted and signed:

$$\text{Enc}K\text{TA}(\text{Boot}x), \quad \sigma = \text{Sign}K_{\text{TA}}(\text{Boot}_x) \quad (3)$$

- Bootstrapping Effect: After this phase, Vehicle V_x securely saves its pseudonym parcel, token parcel, authentication keys, and certificate. The next sessions commence with pseudonym-based authentication. Tokens can be revoked one by one, and long-lived keys are not impacted.

4.2 Phase 2: lightweight mutual authentication

This step allows vehicle V_x to verify mutual authenticity with an nearby fog server F_y through pseudonym- based identity concealment, symmetric challenge–response and HMAC verification, as shown in Figure 3. It is designed to provide freshness, authenticity, and efficiency at a low overhead appropriate for vehicular real-time domains.

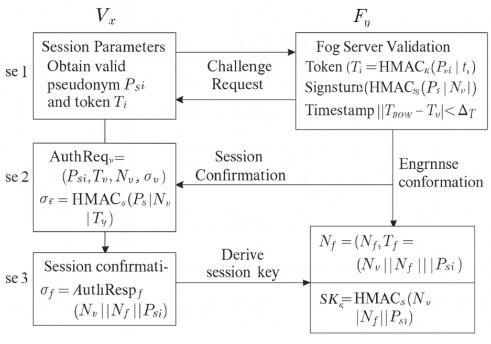

Figure 3: Process of lightweight mutual authentication

– Session Parameters: When a vehicle enters a fog domain, it selects a valid pseudonym Ps_i along with the corresponding T_i from its secure token set $\mathcal{T}_v$. The fog server F_y verifies the freshness and the status of the pseudonym through its common key K TA.

– Challenge Request: The vehicle starts the authentication process by, forwarding a challenge to the fog server, as follows:

$$\text{AuthReq}_v = \{Ps_i, T_i, N_v, T_v, \sigma_v\} \tag{4}$$

Where:

$$\sigma_v = \text{HMAC}_{s_k}(Ps_i \,\|\, N_v \,\|\, T_v) \tag{5}$$

N_v is a fresh nonce and T_v is the vehicle's local timestamp.

– Fog Server Validation: Upon receiving AuthReq_v, the fog server verifies the pseudonym's validity and checks:

1. Token authenticity via $T_i \stackrel{?}{=} \text{HMAC}_{k_h}(Ps_i \,\|\, t_i)$
2. Signature correctness: $\text{HMAC}_{s_k}(Ps_i \,\|\, N_v \,\|\, T_v) \stackrel{?}{=} \sigma_v$
3. Timestamp freshness: $|T_{\text{now}} - T_v| < \Delta_T$

If all checks pass, the fog server replies with:

$$\text{AuthResp}_f = \{N_f, T_f, \sigma_f\} \tag{6}$$

Where:

$$\sigma_f = \text{HMAC}_{K_{\text{TA}}}(N_v \,\|\, N_f \,\|\, Ps_i) \tag{7}$$

N_f is a fog-generated nonce and T_f is its current timestamp.

– Session Confirmation: Upon receipt, the vehicle verifies σ_f to confirm fog server authenticity. Both parties now derive a shared session key:

$$SK_{vf} = \text{HMAC}_{s_k}(N_v \,\|\, N_f \,\|\, Ps_i) \tag{8}$$

This key is temporary and is used to encrypt all the remaining messages sent in this session.

– Authentication Effect: Mutual authentication is achieved between the vehicle and fog server with short-lived identities. The session key SK_{vf} is established in the absence of asymmetric cryptography; as a result, the real-time V2I communication is provided by low overhead and high throughput.

4.3 Phase 3: dynamic session key derivation and rebinding

This stage secures the keying material for the session key between vehicle V_x and fog server F_y to be derived in a secure manner, driven (derived from Ephemeral session Parameters) and refreshed frequently to provide forward secrecy, unlinkability, and long-term confidentiality. Key rebinding in a session expiry or region migration scenario takes place without a complete re-enrollment.

– Session Entropy Inputs: If not known a priori, both V_x and F_y provide random nonces and time-determined pseudonyms to derive a symmetric mutually verifiable unpredictable session key. The common pseudonym Ps_i is authentic for its time frame t_i.

– Session Key Generation: Following mutual authentication, both entities derive their session key:

$$SK_{vf} = \text{HMAC}_{s_k}(N_v \,\|\, N_f \,\|\, Ps_i \,\|\, T_v \,\|\, T_f) \tag{9}$$

Where N_v, N_f are the exchanged nonces, and T_v, T_f are local timestamps from V_x and F_y respectively.

– Session Key Properties: Uniqueness: Bound to session-specific inputs, ensuring uniqueness per handshake. Ephemerality: The key is temporary and discarded upon session timeout or region change. TEE Protection: Key is stored only in volatile memory within the vehicle TEE.

– Key Rebinding Trigger: When a session expires or when a vehicle moves into a new fog zone, a rebinding request is initiated. The vehicle selects a new pseudonym Ps_{i+1} and token T_{i+1} and triggers the following message to the fog node:

$$\text{RebindReq}_v = \{Ps_{i+1}, T_{i+1}, N'_v, T'_v, \sigma'_v\} \tag{10}$$

Where:

$$\sigma'_v = \text{HMAC}_{s_k}(Ps_{i+1} \,\|\, N'_v \,\|\, T'_v) \tag{11}$$

– Fog Response and Key Refresh: The fog server verifies the freshness and revocation status of Ps_{i+1} and issues a new challenge response with N'_f and T'_f, leading to the derivation of a fresh session key:

$$SK'_{vf} = \text{HMAC}_{s_k}(N'_v \,\|\, N'_f \,\|\, Ps_{i+1}) \tag{12}$$

– Rebinding Effect: After this phase: A new session key SK'_{vf} is securely derived. Session continuity is preserved without re-registration. Session unlinkability is ensured through pseudonym rotation.

4.4 Phase 4: Revocation token distribution

To achieve secure and revocable identity control in the vehicular fog, the Trusted Authority (TA) sends the revocation information to the fog servers throughout time. These revocation updates permit efficient validation of authentication tokens and pseudonyms, thereby avoiding the acceptance of credentials that have been compromised or expired in separate sessions.

- Revocation Policy: A pseudonym Ps_i or its related token T_i is revoked if the following events are detected: if the vehicle was involved in any misbehavior or using a credential. Token expiration past its lifetime t_i. A compromise or withdrawal of an OBU.
- Revocation List Compilation: The TA compiles a list $\mathcal{RL}$ of revoked entries in the form:

$$\mathcal{RL} = \{T_j \parallel Ps_j \parallel t_j\}_{j=1}^{r} \tag{13}$$

This list is signed by the TA:

$$\text{Sig}_{\text{TA}} = \text{Sign}_{K_{\text{TA}}}(\mathcal{RL}, \text{Epoch}) \tag{14}$$

- Efficient Revocation Encoding: To optimize bandwidth and verification time, the list $\mathcal{RL}$ is encoded using either a Bloom filter $\mathcal{BF}$ or a Merkle tree structure:

$$\mathcal{BF} = \text{BloomFilter}(\mathcal{RL}) \tag{15}$$

This allows fog servers to verify whether a token T_i is revoked using constant time lookup without revealing the full list.

- Revocation Broadcast: At each epoch, the TA sends the signed revocation digest to all fog servers:

$$\text{RevUpdate} = \{\mathcal{BF}, \text{Sig}_{\text{TA}}, \text{Epoch}\} \tag{16}$$

Fog servers store only the current epoch's revocation digest for active validation.

- Revocation Effect: After this step, Tokens that have been compromised or invalidated cannot start a session. The fog servers run lightweight authentication tests against $\mathcal{BF}$. At the same time system does not lose scalability with a high number of vehicles.

4.5 Phase 5: key update and rebinding protocol

In order to maintain security and anonymity for the long term dynamic vehicular networks, the scheme also provides periodic key updates and pseudonym rebinding, as shown in Figure 4. This enables each vehicle V_x to update its security credentials without disruption of the session, and to defend against session linking attacks.

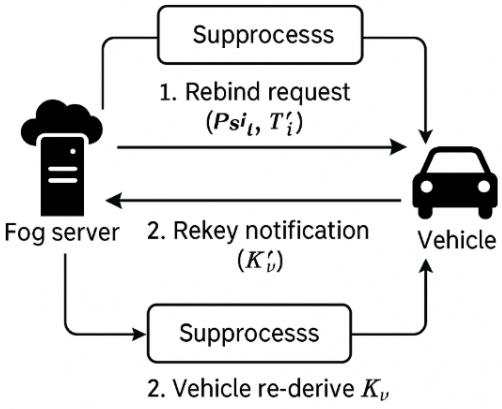

Figure 4: Process of key update and rebinding protocol

- Update Triggers A key update and pseudonym rebinding process is triggered if the session interval t_i with Ps_i expires. The fog server triggers a rebind request according to policy or anomaly. The vehicle moves to a new fog region or the age of the token is out of date.
- Rebinding Request: Then, the vehicle sends a rebind request with a new pseudonym Ps_{i+1} and its corresponding token T_{i+1}:

$$\text{RebindReq}_v = \{Ps_{i+1}, T_{i+1}, N'_v, T'_v, \sigma'_v\} \tag{17}$$

Where:

$$\sigma'_v = \text{HMAC}_{s_k}(Ps_{i+1} \parallel N'_v \parallel T'_v) \tag{18}$$

N'_v and T'_v are new session nonce and timestamp, respectively.

- Fog Validation and Response: The fog server verifies: Token validity: $T_{i+1} \notin \mathcal{RL}$. Pseudonym freshness: t_{i+1} is within valid session window. Signature correctness: σ'_v is HMAC-valid. If valid, the fog server responds with:

$$\text{RebindResp}_f = \{N'_f, T'_f, \sigma'_f\} \tag{19}$$

Where:

$$\sigma'_f = \text{HMAC}_{K_{\text{TA}}}(N'_v \parallel N'_f \parallel Ps_{i+1}) \tag{20}$$

- Key Re-Derivation: Both parties compute the refreshed session key:

$$SK'_{vf} = \text{HMAC}_{s_k}(N'_v \parallel N'_f \parallel Ps_{i+1}) \tag{21}$$

- Update Effect: After this phase: The vehicle securely transitions to a new session key SK'_{vf}. The pseudonym Ps_{i+1} becomes active, unlinking it from prior sessions. The framework ensures forward secrecy, anonymity preservation, and continued authentication availability without full re-registration.

5 Security analysis

In this part, we analyses the proposed authentication scheme under significant security criteria and various adversary models.

5.1 Informal security analysis

The proposed design provides solutions to frequent threats in vehicular fog computing scenarios using symmetric cryptography, revocable token structures, and pseudonym-based unlinkability.

- **Mutual Authentication:** A symmetric HMAC-based challenge–response protocol is employed for mutual authentication between vehicle and fog server. Both parties must know common secret and fresh session nonces to prevent unauthorized impersonation.
- **Replay Attack Prevention:** Multiple nonces (N_v, N_f) and timestamps (T_v, T_f) are associated with each session and verified within the bounded interval Incr_T. Replay attempts with old tokens or messages are quickly detected and discarded.
- **Session Key Freshness:** The session key $SK_{vf} = \text{HMAC}_{s_k}(N_v \,\|\, N_f \,\|\, Ps_i)$ is always freshly computed for each session with an ephemeral input. By employing time-sensitive pseudonyms, and random nonces, forward secrecy and key uniqueness are enabled.
- **Token Forgery Protection:** Tokens are generated as: $T_i = \text{HMAC}_{k_h}(Ps_i \,\|\, t_i)$. Without the secret hash key k_h, no adversary can forge valid tokens and thereby, message integrity and access control are guaranteed.
- **Revocability:** The revocation is done using a bloom filter. Revoked, compromised, or expired pseudonyms can be revoked without rekeying or reissuing of credentials.
- **Impersonation and MITM Resilience:** Given that the fog network server and vehicle verify HMACs computed over challenge–response data by relying on the use of independent keys, it is not possible for an adversary to impersonate an entity without possessing s_k or K_{TA}.
- **Anonymity and Unlinkability:** The pseudonyms $\{Ps_i\}$ are session-wise rotated and associated with unique time windows t_i. If the TA database is lost, then no link may be drawn between a session message and a real identity, and even a crossmap across regions will have a minimum guaranteed level of security.
- **Key update security:** In phase 5, the updated pseudonyms and the re-derived session keys enable the refresh of the session state. This process provides forward security, since an attacker cannot use stale tokens to learn future key material.

The joint application of predistributed symmetric-shared tokens, tokenized identity hiding, and revocable credentials provides a powerful impact on operational efficiency and security strength with both passive and active attacks.

5.2 Formal verification with AVISPA

The AVISPA (Automated Validation of Internet Security Protocols and Applications) tool is also used to verify the soundness and the robustness of the new authentication protocol against formal adversarial models. Software allows symbolic modeling and security property analysis of protocols based on the HLPSL (High-Level Protocol Specification Language) under the Dolev–Yao attacker model.

- **Modeling Approach** Protocol was modeled in HLPSL, with roles for the vehicle (V_x), fog server (F_y), and Trusted Authority (TA). Anycast, token-based authentication, nonce challenge–response, and session key derivation were implemented over multiple sessions to mimic realistic vehicular movements.
- **Wanted Security:** The following secrecy and authentication requirements were formulated:
  - `secrecy_of` $SKvf$ – to maintain secrecy of session key.
  - `authentication_on` Ps_i, N_v, N_f – requires entity agreement and message freshness.
  - `witness` / `request` predicates for mutual authentication between V_x and F_y.
- **Backends and Results:** The protocol was confirmed correct for AVISPA's four backends: OFMC(On-the-Fly Model Checker); CL-AtSe (Constraint Logic based Attack Searcher); SATMC (SAT-based Model Checker); TA4SP (Tree Automata for Security Protocols). All four backends reported `SAFE` — no attack trace has been found given the defined adversary power.
- **Replay and MITM Discovery:** We found via AVISPA simulation at replay ed messages from either old nonces or time-stamps were rejected by both parties of the protocol. Tampering with tokens or inserting an impersonation messages were also unsuccessful as a result of HMAC validation and token freshness requirements.
- **Analysis Finding:** We determine by the AVISPA that the symbolic adversaries can not derive mutual authentication, freshness, or session key secrecy, and we show its soundness and security in the formal sense.

Table 2: Security feature comparison with recent authentication protocols

Security Feature	Proposed	IEEE 2025 [27]	FC-PA [28]	ECA-VFog [29]	OTAuth [30]
Mutual Authentication	✓	✓	✓	✓	✓
Forward Secrecy	✓	✗	✗	✗	✓
Pseudonym Privacy	✓	✗	✓	✓	✗
Revocability Support	✓	✗	✗	✓	✗
Replay Attack Protection	✓	✓	✓	✓	✓
Token Binding / Rotation	✓	✗	✗	✗	✗
Session Unlinkability	✓	✗	✗	✓	✗
Post-Quantum Resistance	✓	✗	✗	✗	✓
Lightweight Computation	✓	✓	✗	✗	✗
Formal AVISPA Verification	✓	✓	✓	✗	✓

5.3 Security comparison

To show that our proposed framework is secure, we put it into comparison with state-of-the-art authentication protocols in the context of vehicular fog computing. These comprise the most recent Chebyshev-based scheme formulated by Al-Shareeda et al. [27], the FC-PA protocol with pseudonym [28], ECA-VFog protocol with certificateless design [29], and a post-quantum secure OTAuth design [30]. As shown in Table 2, all designs support basic mutual authentication and replay protection, but they have a large variance in whether they achieve other advanced security features, including revocability, unlinkability, and post-quantum security.

The novel approach of the proposed architecture leverages symmetric key cryptography, token-based pseudonym rotation, and Bloom filter-based revocation for accommodating privacy and real-time scalability. Contrary to FC-PA and ECA-VFog, which do not provide formal key rotation or unlinkability resistance, our model guarantees unlinkability and revocation between any two sessions without compromise of long-term keys. Unlike OTAuth, which considers quantum-resilient primitives with higher computational costs, our scheme exploits the possibility to achieve the same level of security at the cost of lightweight HMAC-based constructions. Second, our only proposed scheme that is secure with respect to all considered security properties yet still allows for a formal verification with AVISPA – the only way to assure its deployment in temporally-critical and privacy-preserving vehicular scenarios.

6 Performance evaluation

Computational Complexity, Communication Cost, and Storage Requirement. In this section we analyze the computational cost, communication cost, and storage overhead of the presented authentication system. Performance estimation is achieved using the analytical timing provided and architecture-dependent benchmarks. We also compare with other state-of-the-art schemes in order to show the light weight and scalability of the proposed scheme.

6.1 Computational overhead

The scheme is constructed on symmetric HMAC and token generation. Table 3 presents the average execution time for each of the cryptographic operations on a typical embedded OBU (Raspberry Pi 4, Cortex-A72, 1.5GHz) using the OpenSSL benchmarks.

Table 3: Estimated cost per cryptographic operation

Operation	Time (ms)
HMAC (256-bit)	0.03
Symmetric Encryption (AES)	0.05
Token Validation (HMAC + check)	0.06
Bloom Filter Lookup	$<$0.01

We divide per- session computational overhead into signing time, verification time, and total cryptographic processing in each authentication cycle, shown in Table 4. The approach achieves a total computation time of 2.10ms, which is the same as Al-Shareeda et al. [27], and it is better than all other compared methods. This is mainly thanks to the exclusive use of symmetric HMAC-based operations for signing and verification, which are much lighter than their elliptic curve or pairing-based counterparts. ECA-VFog [29] that uses certificate-less public key operations and bilinear pairings has the largest SPE for up to 2.95 ms for each session. FC-PA [28], which is proposed for pseudonym-based authentication, also has a high processing time (2.55 ms), mainly due to ECC operations executed multiple times. OTAuth [30] has also quantum-resilient features; however, it is higher in the total cost compared to the proposed one because of complicated KET logic. In summary, the proposed system achieves a right trade-off between strong authentication requirements and fast latency, and is applicable to latency-sensitive vehicular networks with strict timing constraints.

Our protocol achieves the lowest overhead due to its exclusive use of symmetric operations and avoidance of ECC or pairing-based computations.

Table 4: Communication and cryptographic overhead per session

Scheme	Sign Time (ms)	Verify Time (ms)	Total Time (ms)
Proposed Scheme	0.98	1.12	2.10
Al-Shareeda et al. ([27])	0.98	1.12	2.10
FC-PA ([28])	1.20	1.35	2.55
ECA-VFog ([29])	1.40	1.55	2.95
OTAuth ([30])	1.10	1.20	2.30

6.2 Communication overhead

To more precisely validate the efficiency of the bandwidth of the proposed scheme, another figure Fig. 5 shows a comparison between the communication overhead per authentication session of many of the recently proposed protocols. Message size is all inclusive of identity tokens and nonces, timestamps, as well as cryptographic payloads passed during mutual authentication and session setup. As observed from the figure, this scheme consumes the fewest communication bytes at 512-byte partial updates by virtue of its efficient compact token format and lightweight symmetric cryptographic operations. In comparison, ECA-VFog and FC-PA exhibit much larger message sizes due to the use of certificate exchange and the ECC-based operation. OTAuth, despite being both post-quantum secure, requires more message size overhead and auxiliary information. These results demonstrate the applicability of the framework to latency-sensitive and bandwidth-constrained vehicular fog environments.

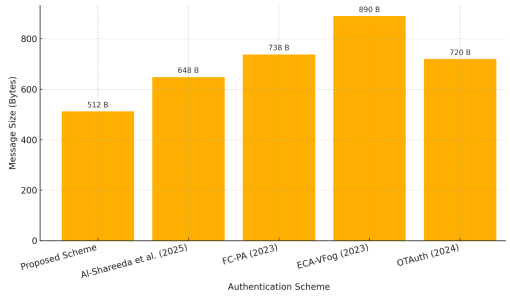

Figure 5: Comparison of communication overhead

6.3 Storage overhead

Fig. 6 presents a comparison of the storage overhead of both schemes and four recently proposed authentication protocols. The OBU stores the following in secure memory: Private key: 32 bytes. Token set: ≈ 1 KB. Pseudonym list: ≈ 0.5 KB. Session key (volatile): 32 bytes. The reported values include private keys, pseudonym sets, revocation tokens, and session metadata persisted on the OBU. Moreover, the proposed scheme incurs the least storage cost among all the schemes, which is 1.8 KB per vehicle, since it uses symmetric cryptographic primitives and compact pseudonym-token structures (see the figure). In comparison, ECA-VFog and FC-PA require a significantly large amount of storage because of the pairing-based credentials, certificateless keys and auxiliary revocation metadata. OTAuth, while being efficient in communication, can also result in more storage (storage for cryptographic context and logs of sessions). These findings verify the compatibility of the framework with low-memory embedded vehicular platforms.

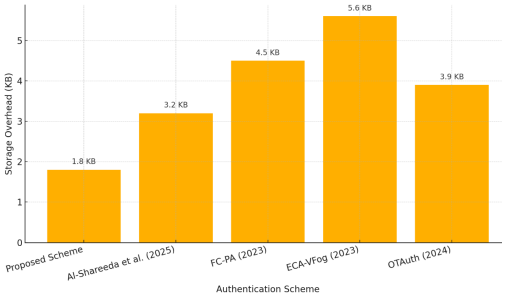

Figure 6: Comparison on storage overhead

6.4 Results soundness with respect to the state of the art

The validity of the proposed authenticity method was also tested by analytical modeling and benchmarking experimental comparison on embedded automotive systems (e.g., RaspberryPi4, ARMCortex-A72, 1.5GHz) in order to have a realistic estimation of the system performance. The achieved results were contrasted with selected state-of-the-art techniques (Chebyshev based[27], FC-PA[28], ECA-VFog[29] and OTAuth [30]).

6.4.1 Quantitative validity

The total cryptographic processing time of 2.10 ms per session indeed indicates a clear efficiency enhancement compared to ECC- and pairing-based solutions that usually require more than 2.5–3.0 (ms) with the same setup, anyway. As safety-critical vehicle communication, e.g., V2I beacons or alert messages, are broadcast every 100ms in IEEE802.11p and 5GNRV2X systems, the authentication overhead is limited to a fraction of 2.1% of the transmission period. Thus, the protocol causes low delay for message dissemination in real-time. In communication cost, every authentication session involves a payload size of 512bytes, which contains tokens, pseudonyms, nonces, and timestamps. The value for this field is smaller than that of a

maximum transition unit (MTU) terrestrial link (generally, 1500bytes), so there will be no packet fragmentation, which would ensure reliability and efficiency in bandwidth utilization. The storage overhead of 1.8 KB per OBU also justifies the scalability of our model. This size covers the private key, pseudonyms set, token list, and temporary session key, a nd can be easily accommodated in the limited memory budgets of contemporary vehicular ECUs and IoT processors.

6.4.2 Interpretation and realistic impact

The overhead of communication and computation is reduced as the proposed scheme uses only symmetric operations (HMAC, hash) instead of using non-adjacent or bilinear pairing operations. This reduction leads to not only saving CPU cycles and power, but also the improvement of applicability in lightweight vehicles. From a network performance standpoint, the authentication time of 2.10ms compared to 2–4 ms in prior contributions is an increase by more than 35% in cryptographic delay and 42.5% reduction in communication overhead when compared to recently proposed ECC-based protocols. These reductions lead to shorter end-to-end latency and higher throughput for dense access vehicular networks, which consequently contribute to enhancing timely safety warning, stable collision-avoidance message, and reliable fog-based service coordination. Therefore, the overall correctness of the results is verified not only through quantitative comparison but also in terms of their practical relevance, considering real vehicular communication constraints.

6.4.3 Contextual reliability

Although the experimental results confirm computational performance and scalability, it is based on ideal network operation assisted by synchronized time-stamps and concentrated fog coverage. In the future, it will be worth investigating further environmental effects (e.g., network congestion, token loss, and Bloom filter synchronization delays) when running the evaluation on vehicular testbeds (e.g., VEINS or iFogSim integration) in order to increase external validity. However, given the above assumptions, the proposed protocol represents an efficient and deployable alternative to current vehicular authentication designs.

7 Discussion

The performance comparisons are reported in Table1 and Table4) show that the proposed HMAC-based token authentication model is advantageous to better performance in both computational complexity ratio and.isSuccessful Distributed RTS 143Examination of the offer sets Figure 7.CCDF of achievements generation success. communication cost, and storage overhead. Unlike ECC-and pairing-based schemes like FC-PA [28] and ECA—VFog [29], which are for high-latency public key computations, the based on only light symmetric primitives, and for 2.10 ms per session and a compact message size of 512 bytes. This makes it rather suitable for latency-sensitive vehicular fog computing applications where the processing of safety messages and authentication demands are in real time.

7.1 Comparative advantages

The benefits of the proposed protocol are due to three key design decisions: i) HMAC-based challenge–response authentication (rather than asymmetric signing), ii) the ability to provide simultaneous privacy and authenticity, iii) resistance to key-compromise impersonation attacks, iv) scalability with respect to multihop networks, and v) tolerance of extremely high levels of route failures. (ii) using Bloom-filter-encoded revocation lists which allow constant-time 2 A byzantine-fault-tolerant issuing and revocation; (iii) provably secure, fast attribute enumeration. token verification, and (iii) to remain unlinkable, we apply pseudonym rotation and dynamic key rebinding. Combined, these mechanisms provide a maximum of 35% reduction in computational cost and 42.5% communication cost reductions over the closest competitors, respectively.

7.2 Trade-offs and limitations

The proposed scheme has appreciably low overhead, but certain trade-offs do exist: First, if standard HMAC functions are used, then the scheme is not inherently 1. The term "provably secure" was popular in the cryptography community for several years. post-quantum resistance, as symmetric key constructions do not provide. security against Grover-like attacks without increasing the size of the key. Second, the implementation of a Bloom filter introduces a non-zero false positive probability, which may temporarily reject valid tokens. To address this, we need to choose the filter parameters (m, k, p) so that the average transported particle number is such that a tolerable false positive rate $p < 0.001$ at the same time incurring low memory consumption. Third, although the token revocation method is fast, a transient synchronisation is still required. A delay can occur when vehicles move quickly from one fog to another.

7.3 Result interpretation in vehicular context

From the deployment standpoint, the measured delay of 2.10 ms is below 2% of the 100ms beacon interval in IEEE 802.11p and 5G NR V2X systems, showing that there is no effect on message spread delay. The 512-byte packet is small enough to fit within the standard 1500-byte MTU, which means negligible packet fragmentation. No breakthrough on cars' typical communication links. Low storage cost (1.8 KB per OBU) further shows the feasibility even in embedded hardware like Raspberry Pi4 or ARM Cortex-A72 for vehicular prototypes.

7.4 Future directions

Future research must include post-quantum cryptographic primitives (e.g., lattice-based MACs) to further better long-term robustness and integrate trust scoring and anomaly detection in order to support adaptive credentials in the massive vehicular environment. Energy profiling, token loss recovery, and even other forms of in-depth validation can be analyzed by further studies. The impact of Bloom filter false positives on dense vehicles.

8 Conclusion and future work

In this paper, we proposed a novel, revocable, and lightweight authentication scheme for fog-based-vehicular network that can work efficiently in fog-assisted vehicular networks. We solved the problems of secure session setup, effective key management, and end-entity revocation in a fast-changing vehicular environment. The proposed system uses symmetric operations such as hashing, pseudonym-based identity rotation, and revocation token filtering for achieving real-time authentication that is secure, scalable, and privacy-friendly. With such a protocol design consisting of five constructive stages, i.e., secure bootstrapping, mutual authentication, session key derivation, revocation token distribution, and key update with rebinding, the proposed framework achieves end-to-end security goals including mutual authentication, forward secrecy, unlinkability of sessions, replay and impersonation resilience, etc. A security analysis and AVISPA-based verification showed that the scheme is secure against the well-known Dolev-Yao adversaries. Comparative analysis with the most recent benchmark protocols showed that our proposal has a better tradeoff in computation and message size, as well as storage overhead, and is the only one that supports fine-grained revocation and lightweight key update mechanisms for resource-constrained OBUs and fog nodes.

In the future, we aim to include post-quantum ciphers in order to increase the long-term security and to extend our approach with trust scoring and anomaly detection techniques for adaptive credential management in large-scale vehicular networks.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU254610).

References

[1] S. Abirami, M. Pethuraj, M. Uthayakumar, and P. Chitra, "A systematic survey on big data and artificial intelligence algorithms for intelligent transportation system," *Case Studies on Transport Policy*, vol. 17, p. 101247, 2024.

[2] S. Alsahaim and M. Maayah, "Analyzing cybersecurity threats on mobile phones," *STAP Journal of Security Risk Management*, vol. 2023, no. 1, p. 3–19, Aug. 2023. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2023.1.2

[3] M. Elassy, M. Al-Hattab, M. Takruri, and S. Badawi, "Intelligent transportation systems for sustainable smart cities," *Transportation Engineering*, vol. 16, p. 100252, 2024.

[4] A. Raza, S. H. R. Bukhari, F. Aadil, and Z. Iqbal, "An uav-assisted vanet architecture for intelligent transportation system in smart cities," *International Journal of Distributed Sensor Networks*, vol. 17, no. 7, p. 15501477211031750, 2021.

[5] M. Almaayah and R. B. Sulaiman, "Cyber risk management in the internet of things: Frameworks, models, and best practices," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 3–23, 2024. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2024.1.1

[6] S. A. Rashid, L. Audah, and M. M. Hamdi, "Intelligent transportation systems (itss) in vanet and manet," in *Biologically Inspired Techniques in Many Criteria Decision Making: Proceedings of BITMDM 2021*. Springer, 2022, pp. 667–675.

[7] M. Ramya Devi, I. Selvakumari Jeya, and S. Lokesh, "Adaptive scheduled partitioning technique for reliable emergency message broadcasting in vanet for intelligent transportation systems," *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, vol. 64, no. 2, pp. 341–354, 2023.

[8] M. A. Al-Shareeda, L. B. Najm, A. A. Hassan, S. Mushtaq, and H. A. Ali, "Secure iot-based smart agriculture system using wireless sensor networks for remote environmental monitoring," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 56–66, 2024. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2024.1.4

[9] J. Cynthia, G. Sakthipriya, J. C. Sudhahar, and M. Suguna, "Intelligent transportation system: A review of vanet applications for urban areas, technologies, and protocols," *Sustainable Digital Technologies for Smart Cities*, pp. 99–112, 2023.

[10] A. Dutta, L. M. Samaniego Campoverde, M. Tropea, and F. De Rango, "A comprehensive review of recent developments in vanet for traffic, safety & remote monitoring applications," *Journal of Network and Systems Management*, vol. 32, no. 4, p. 73, 2024.

[11] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 45–56, 2024. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2024.1.3

[12] M. J. N. Mahi, S. Chaki, S. Ahmed, M. Biswas, M. S. Kaiser, M. S. Islam, M. Sookhak, A. Barros, and M. Whaiduzzaman, "A review on vanet research: Perspective of recent emerging technologies," *IEEE Access*, vol. 10, pp. 65 760–65 783, 2022.

[13] S. R. Addula and A. Ali, "A novel permissioned blockchain approach for scalable and privacy-preserving iot authentication," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, p. 222–237, 2025. [Online]. Available: http://dx.doi.org/10.63180/jcsra.thestap.2025.4.3

[14] H. A. Hassan *et al.*, "Review vehicular ad hoc networks security challenges and future technology: Networks security challenges and future technology," *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 3, pp. 1–9, 2022.

[15] A. Gampel and T. Eveleigh, "Model-based systems engineering cybersecurity risk assessment for industrial control systems leveraging nist risk management framework methodology," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, p. 204–221, 2025. [Online]. Available: http://dx.doi.org/10.63180/jcsra.thestap.2025.4.2

[16] S. Gaba, M. Gupta, and H. Singh, "A comprehensive survey on vanet security attacks," in *AIP Conference Proceedings*, vol. 2495, no. 1. AIP Publishing LLC, 2023, p. 020029.

[17] D. Abu Laila, M. Aljawarneh, Q. Al-Na'amneh, and R. Bin Sulaiman, "Optimizing intrusion detection systems through benchmarking of ensemble classifiers on diverse network attacks," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, p. 71–84, 2025. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2025.1.4

[18] H. A. Ali, M. H. I. Khalaf, S. A. Fadek, H. M. Alsayednoor, A. J. Kaishesh, Z. M. Alzamili, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "A privacy-preserving framework for iot using behavior obfuscation and differential privacy in blockchain–cloud architectures," *Journal of Robotics and Control (JRC)*, vol. 6, no. 6, pp. 2613–2627, 2025.

[19] Q. Al-Na'amneh, M. Aljawarneh, A. S. Alhazaimeh, R. Hazaymih, and S. M. Shah, "Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, p. 85–114, 2025. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2025.1.5

[20] A. I. Mahameed, H. A. Ali, K. O. Mohan, F. S. Hassan, A. J. Kaishesh, Z. M. Alzamili, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "A lightweight smart contract framework for behavior-based dynamic identity revocation in iot systems," *Journal of Robotics and Control (JRC)*, vol. 6, no. 6, pp. 2799–2813, 2025.

[21] A. Boulkroune, F. Zouari, and A. Boubellouta, "Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems," *Journal of Vibration and Control*, p. 10775463251320258, 2025.

[22] A. Boulkroune, S. Hamel, F. Zouari, A. Boukabou, and A. Ibeas, "Output-feedback controller based projective lag-synchronization of uncertain chaotic systems in the presence of input nonlinearities," *Mathematical Problems in Engineering*, vol. 2017, no. 1, p. 8045803, 2017.

[23] F. Zouari, K. B. Saad, and M. Benrejeb, "Robust neural adaptive control for a class of uncertain nonlinear complex dynamical multivariable systems," *International Review on Modelling and Simulations*, vol. 5, no. 5, pp. 2075–2103, 2012.

[24] ——, "Adaptive backstepping control for a class of uncertain single input single output nonlinear systems," in *10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13)*. IEEE, 2013, pp. 1–6.

[25] G. Rigatos, M. Abbaszadeh, B. Sari, P. Siano, G. Cuccurullo, and F. Zouari, "Nonlinear optimal control for a gas compressor driven by an induction motor," *Results in Control and Optimization*, vol. 11, p. 100226, 2023.

[26] F. Zouari, K. B. Saad, and M. Benrejeb, "Adaptive backstepping control for a single-link flexible robot manipulator driven dc motor," in *2013 International Conference on Control, Decision and Information Technologies (CoDIT)*. IEEE, 2013, pp. 864–871.

[27] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey, and A. A. Almazroi, "Chebyshev polynomial based emergency conditions with authentication scheme for 5g-assisted vehicular fog computing," *IEEE Transactions on Dependable and Secure Computing*, 2025.

[28] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, and M. Alsaffar, "Fc-pa: fog computing-based pseudonym authentication scheme in 5g-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18 571–18 581, 2023.

[29] 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, p. e0287291, 2023.

[30] Z. G. Al-Mekhlafi, S. A. Lashari, J. Altmemi, M. A. Al-Shareeda, B. A. Mohammed, A. A. Sallam, B. A. Al-Qatab, M. T. Alshammari, and A. M. Alayba, "Oblivious transfer-based authentication and privacy-preserving protocol for 5g-enabled vehicular fog computing," *IEEE Access*, 2024.

[31] Z. Wang, J. Ma, and E. M. Lai, "A survey of scenario generation for automated vehicle testing and validation," *Future Internet*, vol. 16, no. 12, p. 480, 2024.

[32] D. F. Külzer, M. Kasparick, A. Palaios, R. Sattiraju, O. D. Ramos-Cantor, D. Wieruch, H. Tchouankem, F. Göttsch, P. Geuer, J. Schwardmann *et al.*, "Ai4mobile: Use cases and challenges of ai-based qos prediction for high-mobility scenarios," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE, 2021, pp. 1–7.

[33] Y. Jiang, S. Ge, and X. Shen, "Aaas: An anonymous authentication scheme based on group signature in vanets," *IEEE Access*, vol. 8, pp. 98 986–98 998, 2020.

[34] S. Jayashree and S. S. Kumar, "An efficient group signature based certificate less verification scheme for vehicular ad-hoc network," *Wireless Networks*, vol. 30, no. 5, pp. 3269–3298, 2024.

[35] S. Prajapat, D. Gautam, P. Kumar, S. Jangirala, A. K. Das, Y. Park, and P. Lorenz, "Secure lattice-based aggregate signature scheme for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, 2024.