IAES International Journal of Robotics and Automation (IJRA)
Vol. 15, No. 4, December 2026, pp. 913∼926
ISSN: 2722-2586, DOI: 10.11591/ijra.v15i4.pp913-926

CLAS-KPV: A certificateless aggregate signature scheme with key binding and pre-verification for secure VANETs

Saima Anwar Lashari[1], Zahraa T. Hano[2], Abdulnasser AbdulJabbar Abbood[3], Murtaja Ali Saare[4], Mohammed Amin Almaiah[5], Rami Shehab[6], Mahmood A. Al-Shareeda[3,7]

[1]Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
[2]Department of Medical Instrumentation Engineering Techniques, Shatt Al-Arab University College, Basra, Iraq
[3]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq
[4]Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[5]Faculty of Artificial Intelligence, Applied Science Private University, Amman, Jordan
[6]Department of Information Systems, King Faisal University, Al-Ahsa, Saudi Arabia
[7]College of Engineering, Al-Ayen University, Thi-Qar, Iraq

Article Info

Article history:

Received Jul 26, 2026
Revised Sep 23, 2026
Accepted Nov 10, 2026

Keywords:

Aggregate signature
Certificateless cryptography
Internal threats
Key binding
Lightweight authentication
Pre-verification
Rogue key attack
Vehicular ad hoc networks

ABSTRACT

Vehicular ad hoc networks (VANETs) require efficient message authentication while preserving vehicle privacy and supporting accountability. Existing certificateless aggregate signature (CLAS) schemes reduce certificate and verification overhead, but invalid signatures and manipulated public-key components may still enter the aggregation process before their validity is established. This paper proposes CLAS-KPV, a certificateless aggregate signature scheme that combines authenticated pseudonymous key binding with aggregator-side pre-verification. The scheme binds the pseudonym PID_i to the public components X_i, D_i, and R_i, while keeping the real identity RID_i unavailable to aggregators and roadside units during routine verification. Each signature is verified before aggregation, allowing malformed or invalid signatures to be rejected before they contaminate an aggregate. The construction is analyzed under Type-I and Type-II certificateless adversary models, including public-key replacement, rogue-key manipulation, forgery, replay, and malicious-insider attacks. Analytical performance evaluation shows that online signature generation requires one elliptic-curve scalar multiplication, individual pre-verification requires four, and batch verification for n signatures requires $3n+1$, resulting in linear $O(n)$ verification complexity. These results characterize the explicit security–performance trade-off of pre-aggregation filtering and support the applicability of CLAS-KPV to scalable privacy-preserving VANET authentication.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Mahmood A. Al-Shareeda
Department of Electronic Technologies, Basra Technical Institute, Southern Technical University
Basra, Iraq
Email: mahmood.alshareedah@stu.edu.iq

1. INTRODUCTION

Vehicular ad hoc networks (VANETs) constitute an important communication component of intelligent transportation systems (ITS), enabling real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication for applications such as collision avoidance, cooperative driving, emergency warning,

and traffic-congestion management [1]–[4]. The reliability of these applications depends strongly on the authenticity and integrity of the exchanged safety messages. A forged, modified, or replayed message may cause vehicles or roadside infrastructure to make incorrect decisions, potentially resulting in traffic disruption or safety risks [5]–[7].

Conventional public key infrastructure (PKI)-based authentication provides well-established mechanisms for message authentication but introduces certificate-management, storage, verification, distribution, and revocation overhead in highly dynamic vehicular environments [8]–[10]. These costs become particularly relevant when an RSU must process a large number of safety messages within a short time interval [11]–[13]. Identity-based cryptography (IBC) eliminates conventional public-key certificates but introduces the key-escrow problem because the private key generator (PKG) can derive the complete private key of a user [14], [15]. Certificateless public key cryptography (CL-PKC) provides an alternative by dividing private-key generation between a key generation center (KGC) and the user, thereby avoiding conventional certificates while preventing the KGC from possessing the user's complete private key [16], [17].

To further reduce authentication overhead in dense vehicular environments, certificateless aggregate signature (CLAS) schemes combine multiple individual signatures into an aggregate that can be verified using a common verification procedure [18], [19]. Recent CLAS constructions have improved pairing-free computation, conditional privacy, traceability, and invalid-signature detection. Nevertheless, these properties do not by themselves resolve an important problem that arises when an intermediate aggregator collects signatures from many vehicles: an invalid or manipulated signature may be admitted to an aggregate before its validity is established.

The main contributions of this work are an authenticated pseudonymous key-binding mechanism that removes the need for RID_i during online authentication, an aggregator-side pre-verification procedure that filters invalid signatures, and reproducible CLAS-KPV signing and verification algorithms. We further provide a security analysis under type-I and type-II adversaries and a performance evaluation showing $O(n)$ batch-verification complexity.

2. RELATED WORK

VANETs require authentication mechanisms that can simultaneously provide message integrity, conditional privacy, traceability, and low verification latency under highly dynamic network conditions. Conventional public key infrastructure (PKI)-based approaches provide mature identity and credential management but introduce certificate storage, verification, distribution, and revocation overhead when a large number of vehicles exchange safety messages frequently [20]–[22]. Identity-based cryptography (IBC) reduces certificate-management requirements by deriving cryptographic credentials from identity information; however, the dependence on a private key generator introduces the key-escrow problem.

CL-PKC, originally introduced by Al-Riyami and Paterson [23], addresses these limitations by dividing private-key generation between the KGC and the user. Several studies have investigated lightweight and security-enhanced authentication for resource-constrained networks. Al-Mekhlafi *et al.* [24] proposed ChebIoD, a Chebyshev-polynomial-based authentication and session-key establishment protocol for Internet of Drones environments. Post-quantum authentication has also received increasing attention. Al-Shareeda *et al.* [25] experimentally evaluated the NIST-standardized Dilithium digital-signature variants on Raspberry Pi hardware and demonstrated the feasibility and performance implications of lattice-based signatures on resource-constrained platforms. Similarly, Al-Mekhlafi *et al.* [26] investigated a lattice-based security framework for Internet of Medical Things environments. Within the CLAS literature, Zheng *et al.* [27] proposed a security-enhanced pairing-free certificateless aggregate signature scheme for VANETs. Zhu *et al.* [28] developed a certificateless conditional privacy-preserving authentication scheme that strengthens vehicular privacy while maintaining accountability. Its design demonstrates the importance of balancing anonymity with traceability in VANET authentication. More recently, Wang *et al.* [29] proposed a privacy-preserving certificateless aggregate signature scheme with detectable invalid signatures for VANETs. This work is particularly relevant because it recognizes that invalid signatures can undermine aggregate verification.

Complementary VANET security mechanisms have also been investigated outside the CLAS setting. Blockchain-assisted trust and revocation mechanisms can provide decentralized accountability and tamper-resistant records [30], while intrusion-detection approaches can identify malicious network behavior using traffic characteristics [31]. These mechanisms address different layers of vehicular security and can comple-

ment cryptographic message authentication, but they do not replace a lightweight signature-verification mechanism at the message-authentication layer. Table 1 summarizes the principal design differences among the most directly related CLAS schemes.

Table 1. Comparison with closely related CLAS schemes

Scheme	CLAS	Pairing-Free	Conditional Privacy	Traceability	Pre-verification	Explicit Key Binding
Zheng *et al.* [27]	Yes	Yes	Yes	–	No	No
Zhu *et al.* [28]	Yes	–	Yes	Yes	No	No
Wang *et al.* [29]	Yes	–	Yes	Yes	No	–
CLAS-KPV	Yes	Yes	Yes	Yes	Yes	Yes

3. PRELIMINARIES

This section introduces the mathematical notation, cryptographic assumptions, and basic concepts used in the design and security analysis of the proposed CLAS-KPV scheme.

3.1. Cryptographic assumptions

The security of CLAS-KPV is based primarily on the computational hardness of the elliptic curve discrete logarithm problem (ECDLP), together with standard cryptographic properties of the employed hash functions.

- Elliptic curve discrete logarithm problem (ECDLP) [32], [33]: Given points $P, Q \in G$, where $Q = xP$ for an unknown $x \in \mathbb{Z}_q^*$, determining x from P and Q is assumed to be computationally infeasible.
- Computational Diffie–Hellman problem (CDHP) [34]: Given $P, aP, bP \in G$ for unknown $a, b \in \mathbb{Z}_q^*$, computing abP without knowledge of either scalar is assumed to be computationally infeasible.
- Cryptographic hash functions [35], [36]: The hash functions H_0, H_1, H_2, and H_3 are assumed to provide pre-image resistance, second-pre-image resistance, and collision resistance.

3.2. Certificateless signature model

In certificateless public-key cryptography (CL-PKC), a user's signing capability is derived from two independent secret components: a partial private key issued by the key generation center (KGC) and a secret value independently selected by the user [37], [38]. Consequently, possession of the KGC master secret alone does not reveal the user's complete signing key. This construction mitigates the key-escrow limitation of identity-based cryptography while avoiding the certificate-management overhead associated with conventional public-key infrastructure.

3.3. Aggregate signature concepts

An aggregate signature combines multiple valid individual signatures into a compact aggregate representation that can be verified collectively. In CLAS-KPV, aggregation is deliberately performed only after individual pre-verification. For each received message, the aggregator first validates credential binding, freshness, revocation status, and signature correctness. Only signatures that successfully pass these checks are admitted to the aggregation process.

4. SYSTEM AND THREAT MODEL

This section defines the entities participating in CLAS-KPV, their trust assumptions, communication relationships, and the adversarial capabilities considered in the security analysis.

4.1. System model

The proposed CLAS-KPV scheme operates in a VANET environment consisting of five principal entities: the trusted authority (TA), key generation center (KGC), vehicles equipped with on-board units (OBUs), aggregators, and roadside units (RSUs).

a. Trusted authority (TA): The TA is responsible for vehicle registration support, pseudonym generation, identity tracing, and credential revocation. The TA reveals the corresponding identity only when authorized tracing is required [39], [40].

b. Key generation center (KGC): The KGC generates the certificateless partial private key of each registered vehicle. It selects the master secret a and publishes $K_{pub} = aP$. For vehicle V_i, the KGC derives the partial private key d_i and its corresponding public verification component $D_i = d_iP$. Because the vehicle independently selects its secret values x_i and r_i, the KGC does not possess the complete vehicle signing key [41], [42].

c. Vehicles (OBUs): each vehicle V_i is equipped with an OBU capable of performing elliptic-curve and hash operations. The vehicle independently generates the secret values x_i and r_i, with corresponding public components $X_i = x_iP$ and $R_i = r_iP$. To authenticate a safety message M_i, the OBU generates a fresh nonce u_i, computes $U_i = u_iP$, and produces the individual signature $\sigma_i = (U_i, s_i)$. The vehicle communicates using its temporary pseudonym PID_i rather than its real identity RID_i.

d. Aggregators: an aggregator collects signed safety messages from nearby vehicles and performs pre-verification before aggregation. For each received message, it checks timestamp freshness, pseudonym and revocation status, authenticated key binding, and signature validity.

e. Roadside units (RSUs): RSUs are infrastructure nodes responsible for final aggregate-signature verification. An RSU validates the received pseudonymous credentials and checks the aggregate verification equation [43], [44]. If aggregate verification fails, the RSU can perform individual verification to isolate invalid signatures.

4.2. Trust assumptions

CLAS-KPV assumes a trusted TA, an honest KGC except under the Type-II model, and correctly operating RSUs. Vehicles and aggregators may be compromised, but they cannot forge or modify authenticated messages without the required secrets. Full compromise of the TA or RSU infrastructure is outside the protocol scope.

4.3. Threat model

CLAS-KPV considers external attackers, malicious insiders, compromised aggregators, and the standard Type-I and Type-II adversaries defined for certificateless cryptography.

a. External adversary: An external adversary does not possess a legitimate vehicle's secret credentials but has access to the public wireless channel [45], [46].

b. Malicious insider: A malicious insider represents a registered or compromised vehicle that possesses its own valid credentials [47], [48]. It may generate malformed messages, replay previously authenticated messages, manipulate transmitted public components, or attempt to impersonate another vehicle.

c. Rogue-key and public-key replacement adversary: An adversary may attempt to replace one or more public components such as X_i, D_i, or R_i, or associate attacker-controlled components with a legitimate pseudonym PID_i. CLAS-KPV addresses this threat through the authenticated binding $B_i = H_2(PID_i, X_i, D_i, R_i)$. A modified component changes the corresponding binding value and should therefore fail credential validation unless the attacker can also produce a valid authenticated registration record.

d. Replay adversary: An adversary may capture a previously valid signed message and retransmit it at a later time. CLAS-KPV includes the timestamp t_i in the signature challenges, and the aggregator and RSU verify its freshness before accepting the message.

e. Malicious aggregator: A compromised aggregator may attempt to inject an invalid signature into an aggregate, alter received messages, or selectively omit legitimate messages. Modification or injection is detectable through individual or final signature verification. Selective message dropping, however, is primarily an availability attack and cannot be prevented solely by a digital signature scheme; it requires complementary redundancy, auditing, or trust-management mechanisms.

f. Type-I adversary $\mathcal{A}_I$: The Type-I adversary models an outside attacker with public-key replacement capability.

g. Type-II adversary $\mathcal{A}_{II}$: The Type-II adversary models a malicious or compromised KGC. It knows the master secret a and can therefore derive partial private keys d_i.

4.4. Security objectives

Under the above threat model, CLAS-KPV is designed to provide the following security properties:

a. Message authenticity and integrity: A valid signature should be generated only using the secret components associated with the authenticated pseudonymous credential, and modification of the protected message or signature inputs should invalidate verification.
b. Resistance to public-key replacement and rogue-key attacks: An attacker should not be able to substitute X_i, D_i, or R_i while retaining a valid binding to PID_i.
c. Pre-aggregation invalid-signature filtering: The aggregator should identify invalid signatures before admitting them to the aggregate.
d. Replay resistance: Previously valid messages retransmitted outside the accepted freshness interval should be rejected.
e. Conditional privacy: Aggregators, RSUs, and external observers should authenticate messages using PID_i without requiring access to RID_i during normal operation.
f. Authorized traceability: When verified evidence of misbehavior is available, the TA should be able to resolve the corresponding pseudonym to the registered real identity.
g. Resistance to Type-I and Type-II forgery: Neither a public-key replacement adversary nor a malicious KGC should be able to generate a valid signature for an uncompromised target vehicle without obtaining the required user-controlled signing secrets.

The security analysis in section 6 evaluates these objectives under the stated assumptions and adversarial capabilities.

5. PROPOSED CLAS-KPV SCHEME

This section presents the proposed CLAS-KPV scheme in a formal and reproducible manner. The scheme combines certificateless authentication, authenticated key binding, lightweight pre-verification, and linear signature aggregation.

5.1. System initialization

Let (G) be an additive cyclic group of prime order (q), generated by (P). All scalar arithmetic is performed in ($\mathbb{Z}_q^*$). The elliptic-curve parameters are selected according to the target security level. The system initialization procedure is summarized in Algorithm 1.

Algorithm 1. CLAS-KPV system setup

Require: Security parameter λ
Ensure: Public parameters $params$ and master secrets (a, b)
1: Select an additive cyclic group G of prime order q with generator P.
2: KGC randomly selects $a \in \mathbb{Z}_q^*$.
3: Compute $K_{pub} = aP$.
4: TA randomly selects $b \in \mathbb{Z}_q^*$.
5: Compute $T_{pub} = bP$.
6: Define hash functions H_0, H_1, H_2, and H_3.
7: Set $params = \{G, q, P, K_{pub}, T_{pub}, H_0, H_1, H_2, H_3\}$.
8: Publish $params$.
9: Keep a and b secret at the KGC and TA, respectively.
10: return $params$

5.2. Vehicle registration and partial-key generation

Let (V_i) denote a vehicle with real identity (RID_i). Registration is performed through an authenticated confidential channel. The vehicle registration and partial-key generation procedure is presented in Algorithm 2.

5.3. Pseudonym generation and authenticated key binding

Algorithm 3 describes pseudonym generation and the authenticated binding of the vehicle's public-key components.

Algorithm 2. Vehicle registration and partial-key generation

Require: RID_i, public parameters $params$
Ensure: Vehicle secret components (x_i, d_i) and public components (X_i, D_i)
1: Vehicle V_i randomly selects $x_i \in \mathbb{Z}_q^*$.
2: Compute $X_i = x_i P$.
3: Send (RID_i, X_i) to the KGC through an authenticated secure channel.
4: KGC verifies the registration request.
5: Compute $\alpha_i = H_0(RID_i, X_i)$.
6: Compute the partial private key $d_i = a\alpha_i \bmod q$.
7: Compute the public partial-key component $D_i = d_i P$.
8: Securely transmit d_i to V_i.
9: Register D_i as the authenticated public verification component.
10: return (x_i, d_i, X_i, D_i)

Algorithm 3. Pseudonym generation and authenticated key binding

Require: RID_i, X_i, D_i, validity interval T_i
Ensure: Pseudonymous credential $\mathcal{C}_i$
1: TA generates a fresh registration timestamp t_i^{reg}.
2: Compute $PID_i = RID_i \oplus H_1(bX_i \| T_i \| t_i^{reg})$.
3: Vehicle V_i randomly selects $r_i \in \mathbb{Z}_q^*$.
4: Compute $R_i = r_i P$.
5: Compute $B_i = H_2(PID_i, X_i, D_i, R_i)$.
6: Construct $\mathcal{C}_i = (PID_i, X_i, D_i, R_i, B_i, T_i)$.
7: Authenticate and register $\mathcal{C}_i$.
8: Make $\mathcal{C}_i$ available to authorized aggregators and RSUs.
9: return $\mathcal{C}_i$

5.4. Signature generation

The message-signing procedure executed by vehicle V_i is detailed in Algorithm 4.

Algorithm 4. CLAS-KPV signature generation

Require: Message M_i, PID_i, (x_i, d_i, r_i), $\mathcal{C}_i$, timestamp t_i
Ensure: Individual signature $\sigma_i = (U_i, s_i)$
1: Verify that PID_i and $\mathcal{C}_i$ are valid.
2: Randomly select a fresh nonce $u_i \in \mathbb{Z}_q^*$.
3: Compute $U_i = u_i P$.
4: Compute $\beta_i = H_2(PID_i, X_i, D_i, R_i)$.
5: Compute $h_{1,i} = H_3(\texttt{SIG1} \| M_i \| PID_i \| X_i \| D_i \| R_i \| U_i \| t_i)$.
6: Compute $h_{2,i} = H_3(\texttt{SIG2} \| \beta_i \| M_i \| PID_i \| U_i \| t_i)$.
7: Compute $s_i = u_i + h_{1,i} x_i + h_{2,i} d_i + \beta_i r_i \bmod q$.
8: Set $\sigma_i = (U_i, s_i)$.
9: return σ_i

5.5. Correctness of individual verification

For a legitimately generated signature, $s_i = u_i + h_{1,i} x_i + h_{2,i} d_i + \beta_i r_i \pmod q$. Multiplication by (P) gives

$$\begin{aligned} s_i P &= (u_i + h_{1,i} x_i + h_{2,i} d_i + \beta_i r_i) P \\ &= u_i P + h_{1,i} x_i P + h_{2,i} d_i P + \beta_i r_i P \\ &= U_i + h_{1,i} X_i + h_{2,i} D_i + \beta_i R_i. \end{aligned} \tag{1}$$

Hence, the individual verification equation is $s_iP \stackrel{?}{=} U_i+h_{1,i}X_i+h_{2,i}D_i+\beta_iR_i$. This equation is algebraically consistent with the signing procedure and requires only public pseudonymous information.

5.6. Lightweight pre-verification at the aggregator

The objective of pre-verification is to reject malformed, replayed, key-substituted, or invalidly signed messages before they contaminate an aggregate signature. After receiving $(\mathcal{M}_i)$, the aggregator performs the following operations. First, it verifies that (t_i) falls within the permitted freshness window and that (PID_i) has neither expired nor appeared on the current revocation list. Second, it obtains the authenticated credential $\mathcal{C}_i = (PID_i, X_i, D_i, R_i, B_i, T_i)$ and recomputes $B_i^* = H_2(PID_i, X_i, D_i, R_i)$. It requires $B_i^* = B_i$. The aggregator then computes (β_i), $(h_{1,i})$, and $(h_{2,i})$ using the same inputs as the signer and checks $s_iP \stackrel{?}{=} U_i + h_{1,i}X_i + h_{2,i}D_i + \beta_iR_i$. If all checks succeed, the message is admitted to the aggregation set. Otherwise, it is discarded and may be reported as suspicious. This construction removes (RID_i) from aggregator-side verification. Moreover, pre-verification prevents one invalid signature from contaminating an entire batch and shifts invalid-message filtering away from the final RSU.

5.7. Signature aggregation

The lightweight filtering operation performed before aggregation is formalized in Algorithm 5.

Algorithm 5. Aggregator-side pre-verification

Require: Signed message $\mathcal{M}_i$, authenticated credential $\mathcal{C}_i$
Ensure: Accept or reject decision
Check freshness of timestamp t_i.
if t_i is expired then
  reject $\mathcal{M}_i$.
end if
Check validity and revocation status of PID_i.
if PID_i is invalid or revoked then
  reject $\mathcal{M}_i$.
end if
Compute $B_i^* = H_2(PID_i, X_i, D_i, R_i)$.
if $B_i^* \neq B_i$ then
  reject $\mathcal{M}_i$.
end if
Compute $\beta_i = H_2(PID_i, X_i, D_i, R_i)$.
Compute $h_{1,i} = H_3(\texttt{SIG1}\|M_i\|PID_i\|X_i\|D_i\|R_i\|U_i\|t_i)$.
Compute $h_{2,i} = H_3(\texttt{SIG2}\|\beta_i\|M_i\|PID_i\|U_i\|t_i)$.
if $s_iP = U_i + h_{1,i}X_i + h_{2,i}D_i + \beta_iR_i$ then
  accept $\mathcal{M}_i$ for aggregation.
else
  reject $\mathcal{M}_i$.
end if

5.8. Final batch verification at the RSU

The aggregation and RSU-side batch-verification procedures are summarized in Algorithm 6.

5.9. Misbehavior detection, traceability, and revocation

The misbehavior identification, identity tracing, and credential revocation procedure is presented in Algorithm 7.

Algorithm 6. Signature aggregation and batch verification

Require: n pre-verified signatures $\{\sigma_i = (U_i, s_i)\}_{i=1}^{n}$
Ensure: Aggregate verification decision
Compute $S = \sum_{i=1}^{n} s_i \bmod q$.
Compute $U = \sum_{i=1}^{n} U_i$.
Set aggregate signature $\Sigma = (U, S)$.
Forward Σ and associated message information to the RSU.
for $i = 1$ to n do
    Validate the authenticated credential $\mathcal{C}_i$.
    Compute $\beta_i = H_2(PID_i, X_i, D_i, R_i)$.
    Compute $h_{1,i} = H_3(\texttt{SIG1} \| M_i \| PID_i \| X_i \| D_i \| R_i \| U_i \| t_i)$.
    Compute $h_{2,i} = H_3(\texttt{SIG2} \| \beta_i \| M_i \| PID_i \| U_i \| t_i)$.
end for
Compute $Q = U + \sum_{i=1}^{n} (h_{1,i} X_i + h_{2,i} D_i + \beta_i R_i)$.
if $SP = Q$ then
    accept the aggregate signature.
else
    reject the aggregate and initiate misbehavior detection.
end if

Algorithm 7. Misbehavior detection, traceability, and revocation

Require: Failed aggregate batch and corresponding pseudonymous credentials
Ensure: Identification and revocation of malicious vehicle(s)
for $i = 1$ to n do
    Recompute β_i, $h_{1,i}$, and $h_{2,i}$.
    Verify $s_i P \stackrel{?}{=} U_i + h_{1,i} X_i + h_{2,i} D_i + \beta_i R_i$.
    if individual verification fails then
        Mark PID_i as suspicious.
        Send PID_i and verification evidence to the TA.
        TA retrieves (T_i, t_i^{reg}) from the registration record.
        Recover $RID_i = PID_i \oplus H_1(bX_i \| T_i \| t_i^{reg})$.
        Verify the reported evidence.
        Revoke the credential associated with PID_i.
        Update the revocation information distributed to RSUs and aggregators.
    end if
end for
return Updated revocation status

6. SECURITY ANALYSIS

This section analyzes the security properties of the proposed CLAS-KPV scheme under the threat model defined in section 4.

a. Resistance to signature forgery: CLAS-KPV is designed to provide existential unforgeability against adaptive chosen-message attacks. A valid signature requires the scalar $s_i = u_i + h_{1,i} x_i + h_{2,i} d_i + \beta_i r_i \pmod q$. A Type-I adversary may replace public keys but does not know the KGC master secret a. Therefore, it cannot derive a valid partial private key d_i corresponding to the authenticated component D_i. Moreover, replacing X_i, D_i, R_i, or PID_i changes $\beta_i = H_2(PID_i, X_i, D_i, R_i)$, and causes the credential-binding check to fail.

b. Resistance to rogue-key and key-replacement attacks: CLAS-KPV explicitly binds the pseudonym and public credential components through $B_i = H_2(PID_i, X_i, D_i, R_i)$. The authenticated credential $\mathcal{C}_i = (PID_i, X_i, D_i, R_i, B_i, T_i)$ is registered before online authentication. During pre-verification, the aggre-

gator recomputes $B_i^* = H_2(PID_i, X_i, D_i, R_i)$ and requires $B_i^* = B_i$. Thus, an adversary cannot independently replace X_i, D_i, R_i, or PID_i while preserving the authenticated binding, except with negligible probability of finding a hash collision.

c. Replay-attack resistance: Before accepting a message, the aggregator verifies that t_i lies within the permitted freshness window. Consequently, replaying an expired signed message results in rejection. Modifying the timestamp of an old message also changes the signature challenges and invalidates the verification equation.

d. Anonymity and conditional traceability: During normal authentication, vehicles use temporary pseudonyms rather than their real identities. The TA generates $PID_i = RID_i \oplus H_1(bX_i \| T_i \| t_i^{reg})$. The real identity RID_i is not included in the public credential $\mathcal{C}_i$ and is not required by aggregators or RSUs during routine authentication.

e. Resistance to internal and aggregator attacks: CLAS-KPV considers compromised vehicles and malicious aggregators as potential internal adversaries. A compromised vehicle cannot generate a valid signature on behalf of another uncompromised vehicle without obtaining the corresponding secret components. Similarly, modification of another vehicle's authenticated credential is detected by the binding verification.

The aggregator performs individual pre-verification before admitting a signature to the aggregation set. Therefore, malformed, replayed, key-substituted, or cryptographically invalid signatures can be rejected before they contaminate the aggregate signature. This mechanism also mitigates invalid-signature flooding against the final RSU.

6.1. Pre-verification security

The pre-verification mechanism provides an early filtering layer without replacing final RSU verification. For every received message, the aggregator first checks pseudonym validity, revocation status, timestamp freshness, and the authenticated binding B_i.

6.2. Security comparison

Table 2 compares the principal security properties of CLAS-KPV with representative existing CLAS schemes.

Table 2. Security comparison with existing schemes

Scheme	Rogue Key	Pre-ver.	Anonymity	Traceability	Internal Forgery
Zheng *et al.* [27]	✗	✗	✓	✗	✗
Zhu *et al.* [28]	✓	✗	✓	✓	✗
Wang *et al.* [29]	✓	✗	✓	✓	✗
CLAS-KPV (Proposed)	✓	✓	✓	✓	✓

7. PERFORMANCE EVALUATION

7.1. Evaluation methodology

The computational evaluation is based on the cryptographic operations required during signature generation, individual pre-verification, aggregation, and final batch verification. Let T_{sm} denote the execution cost of one elliptic-curve scalar multiplication, T_{pa} denote one elliptic-curve point addition, and T_h denote one cryptographic hash operation. Modular additions and XOR operations are considered negligible compared with elliptic-curve scalar multiplication.

7.2. Computational cost comparison

Table 3 summarizes the analytical computational costs of the proposed scheme.

Table 3. Analytical computational cost of CLAS-KPV

Operation	EC Scalar Multiplications	Dominant Cost
Signature generation	1	T_{sm}
Pre-verification	4	$4T_{sm}$
Aggregation	0	Point/scalar additions
Batch verification	$3n + 1$	$(3n + 1)T_{sm}$

7.3. Communication overhead comparison

Communication overhead is evaluated analytically from the elements transmitted in each authenticated message. According to Algorithm 4, vehicle V_i transmits $\mathcal{M}_i = M_i, PID_i, X_i, D_i, R_i, U_i, s_i, t_i$.

Let $|M|$ denote the application-message size, $|PID|$ the pseudonym size, $|G|$ the encoded size of an elliptic-curve point, $|q|$ the size of a scalar, and $|t|$ the timestamp size. Since X_i, D_i, R_i, and U_i are elliptic-curve points and s_i is a scalar, the total transmitted size of one authenticated message is $C_{\text{msg}} = |M| + |PID| + 4|G| + |q| + |t|$.

When the application payload is excluded, the cryptographic authentication overhead becomes $C_{\text{auth}} = |PID| + 4|G| + |q| + |t|$. After successful pre-verification of n messages, the aggregator combines the individual signature scalars into $S = \sum_{i=1}^{n} s_i \pmod q$ and the ephemeral public components into $U = \sum_{i=1}^{n} U_i$. The aggregate signature is therefore represented as $\Sigma = (U, S)$. However, the message-specific values PID_i, X_i, D_i, R_i, M_i, and t_i remain necessary at the RSU because they are required to reconstruct the corresponding hash challenges. Consequently, communication efficiency is determined not only by signature aggregation but also by the serialization of the public authentication information.

7.4. Scalability analysis

The scalability of CLAS-KPV is evaluated according to the number of signatures processed by the aggregator and RSU. For n incoming messages, independent pre-verification requires $C_{\text{pre}}(n) = 4nT_{sm}$. Therefore, $C_{\text{pre}}(n) \in O(n)$. Similarly, aggregate verification requires $C_{\text{batch}}(n) = (3n + 1)T_{sm}$, which also gives $C_{\text{batch}}(n) \in O(n)$. Thus, both pre-verification and final batch verification scale linearly with the number of participating vehicles.

The security benefit of pre-verification becomes particularly relevant when the incoming traffic contains invalid signatures. Let ρ represent the fraction of received signatures that fail pre-verification. For n received messages, the expected number of signatures admitted to the aggregate is $n_v = n(1 - \rho)$. The corresponding final verification cost for the admitted signatures becomes $C_{\text{batch}}(n_v) = [3n(1 - \rho) + 1]\, T_{sm}$.

7.5. Comparison with existing CLAS schemes

Table 4 therefore presents a design-level comparison emphasizing the functions directly relevant to the contribution of CLAS-KPV.

Table 4. Design-level comparison with existing CLAS schemes

Scheme	CLAS	Aggregation	Pre-verification	Key binding	Invalid signature handling
Zheng *et al.* [27]	Yes	Yes	No	No	Verification stage
Zhu *et al.* [28]	Yes	Yes	No	No	Verification stage
Wang *et al.* [29]	Yes	Yes	No	No	Detectable invalid signatures
CLAS-KPV	Yes	Yes	Yes	Yes	Before aggregation

7.6. Practical deployment considerations

CLAS-KPV is designed for VANET authentication environments in which vehicles transmit pseudonymously authenticated safety messages through aggregators or RSUs. Its use of temporary pseudonyms, timestamps, authenticated public-key components, and revocation information is consistent with the general security requirements of modern vehicular communication systems. Nevertheless, conceptual compatibility should not be interpreted as direct compliance with IEEE 1609.2 or ETSI ITS security specifications. Practical deployment would require mapping PID_i, X_i, D_i, R_i, and Σ to standardized vehicular message and credential formats. The lifetime of PID_i must also be coordinated with pseudonym-certificate management, while TA-generated revocation information must be integrated with the corresponding credential-management infrastructure. These deployment requirements do not modify the underlying CLAS-KPV signing and verification equations, but they represent necessary engineering steps before implementation in a standards-compliant vehicular environment.

7.7. Discussion

CLAS-KPV introduces aggregator-side pre-verification to reject invalid, replayed, or key-substituted signatures before aggregation, trading additional computation for stronger security. It preserves privacy by enabling verification through PID_i, X_i, D_i, and R_i, while restricting real-identity access to the TA. Both pre-verification and aggregate verification scale linearly with vehicle density. However, the current evaluation is analytical and excludes hardware, mobility, channel, memory, and energy effects. Future work will validate the scheme on common vehicular platforms under varying traffic densities and attack ratios.

8. CONCLUSION AND FUTURE WORK

This paper presented CLAS-KPV, a privacy-preserving certificateless aggregate signature scheme combining authenticated pseudonymous key binding with aggregator-side pre-verification. The scheme supports identity-hidden authentication, filters invalid signatures before aggregation, and resists major certificateless and VANET attacks. Its verification complexity is linear, requiring $3n + 1$ scalar multiplications for n signatures. Future work will evaluate the scheme on vehicular hardware, integrate it with IEEE 1609.2 and ETSI ITS frameworks, and explore post-quantum alternatives.

FUNDING INFORMATION

Authors state yes funding involved.

AUTHOR CONTRIBUTIONS STATEMENT (MANDATORY)

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Saima Anwar Lashari	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Zahraa T. Hano		✓		✓	✓	✓		✓	✓	✓	✓			
Abdulnasser AbdulJabbar Abbood	✓	✓	✓	✓	✓	✓		✓	✓	✓				
Murtaja Ali Saare	✓	✓		✓	✓	✓	✓			✓		✓		
Mohammed Amin Almaiah	✓	✓		✓	✓	✓	✓			✓		✓	✓	
Rami Shehab	✓	✓		✓	✓	✓			✓	✓		✓		
Mahmood A. Al-Shareeda	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT (MANDATORY)

Authors state no conflict of interest.

DATA AVAILABILITY (MANDATORY)

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] B. A. Mohammed *et al.*, "Service based VEINS framework for vehicular ad-hoc network (VANET): A systematic review of state-of-the-art," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 2259–2281, 2024, doi: 10.1007/s12083-024-01692-0.

[2] A. Khan, A. Junaid, G. Husnain, K. J. Alzahrani, and H. K. Alkahtani, "An efficient intrusion detection system using domain-aware meta-learning with adapter-based few-shot adaptation in vehicular ad-hoc networks (VANETs)," *IET Intelligent Transport Systems*, vol. 20, no. 1, p. e70182, 2026, doi: 10.1049/itr2.70182.

[3] M. Alrajeh, M. Almaiah, and U. Mamodiya, "Cyber risk analysis and security practices in industrial manufacturing: Empirical evidence and literature insights," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2026, no. 1, 2026.

[4] V. Lode and A. Pinapati, "A comprehensive review of ECC-based certificateless aggregate signature for vehicular ad-hoc networks (VANETs) and cryptanalysis of quantum-secure CLAS," *Computers and Electrical Engineering*, vol. 135, p. 111174, 2026, doi: 10.1016/j.compeleceng.2026.111174.

[5] A. G. Hameed and M. S. Mahmoud, "Vehicular ad-hoc network (VANET)–a review," in *2022 Iraqi International Conference on Communication and Information Technologies (IICCIT)*, 2022, pp. 367–372.

[6] L. S. Mezher, "An overview on vehicular ad hoc networks security," *Journal of Engineering Research and Reports*, vol. 28, no. 1, pp. 189–204, 2026, doi: 10.9734/jerr/2026/v28i11769.

[7] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE Access*, vol. 9, pp. 31309–31321, 2021, doi: 10.1109/ACCESS.2021.3060046.

[8] M. AlMarshoud, "Vehicular ad hoc networks security and privacy issues," *AI-Enabled Transportation Electrification - Advanced Energy Systems, Smart Infrastructure and Sustainable Mobility for Next-Generation Transportation*, 2026, doi: 10.5772/intechopen.1015308.

[9] M. A. Almaiah and M. C. Ghanem, "Deep learning-based adaptive intrusion detection for next-generation network security," *Journal of Information and Cybersecurity*, vol. 2026, no. 1, pp. 16–31, 2026.

[10] E. R. Agustina *et al.*, "A lightweight post-quantum anonymous attestation framework for traceable and comprehensive privacy preservation in VANETs," *Journal of Cybersecurity and Privacy*, vol. 6, no. 2, p. 44, 2026, doi: 10.3390/jcp6020044.

[11] S. Mittal *et al.*, "Using identity-based cryptography as a foundation for an effective and secure cloud model for e-health," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 7016554, 2022, doi: 10.1155/2022/7016554.

[12] R. Li, J. Cui, L. Wei, I. Bolodurina, J. Zhang, and H. Zhong, "Privacy-accountable distributed collaborative authentication for malicious node resistance in vehicular ad hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 3, pp. 5718–5733, 2026, doi: 10.1109/TDSC.2026.3658515.

[13] Y. Zhou, B. Yang, Z. Qiao, Z. Xia, M. Zhang, and Y. Mu, "Leakage-resilient identity-based cryptography from minimal assumptions," *Designs, Codes, and Cryptography*, vol. 91, no. 11, pp. 3757–3801, 2023, doi: 10.1007/s10623-023-01268-8.

[14] L. Soni, H. Chandra, and D. S. Gupta, "SmartAgri-IDQ: Quantum-resistant identity-based data authentication protocol for smart agriculture IoT," *Security and Privacy*, vol. 9, no. 2, p. e70189, 2026, doi: 10.1002/spy2.70189.

[15] W. Yang, Y. Cai, Q. Ou, F. Zhang, and A. Yang, "Forward-secure identity-based signcryption with equality test for social recommendation on smart IoT devices," *IEEE Internet of Things Journal*, vol. 13, no. 13, pp. 29342–29356, 2026, doi: 10.1109/JIOT.2026.3685126.

[16] S. Shajil, P. T. Johnpaul, and M. Sangeetha, "Privacy-preserving public complaint platform using certificateless cryptography," in *3rd International Conference on Electronics and Renewable Systems, ICEARS 2025 - Proceedings*, 2025, pp. 906–911, doi: 10.1109/ICEARS64219.2025.10941091.

[17] W. Cui, R. Cheng, K. Wu, Y. Su, and Y. Lei, "A certificateless authenticated key agreement scheme for the power IoT," *Energies*, vol. 14, no. 19, p. 6317, 2021, doi: 10.3390/en14196317.

[18] M. Malik, Kamaldeep, and M. Dutta, "On the applicability of certificateless public key cryptography (CL-PKC) for securing the internet of things (IoT)," in *Lecture Notes in Networks and Systems*, 2020, vol. 116, pp. 43–50, doi: 10.1007/978-981-15-3020-3_5.

[19] R. Elhabob, Y. Zhao, I. Sella, and H. Xiong, "Efficient certificateless public key cryptography with equality test for internet of vehicles," *IEEE Access*, vol. 7, pp. 68957–68969, 2019, doi: 10.1109/ACCESS.2019.2917326.

[20] S. Khan, F. Luo, Z. Zhang, M. A. Rahim, M. Ahmad, and K. Wu, "Survey on issues and recent advances in vehicular public-key infrastructure (VPKI)," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 3, pp. 1574–1601, 2022, doi: 10.1109/COMST.2022.3178081.

[21] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the internet of things: A systematic literature review," *Journal of Industrial Information Integration*, vol. 41, p. 100670, 2024, doi: 10.1016/j.jii.2024.100670.

[22] A. Faisal and M. Zulkernine, "DKS-PKI: A distributed key server architecture for public key infrastructure," in *Lecture Notes in Computer Science*, 2022, vol. 13784 LNCS, pp. 23–43, doi: 10.1007/978-3-031-23690-7_2.

[23] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2003, vol. 2894, pp. 452–473, doi: 10.1007/978-3-540-40061-5_29.

[24] Z. G. Al-Mekhlafi *et al.*, "ChebIoD: A Chebyshev polynomial-based lightweight authentication scheme for internet of drones environments," *Scientific Reports*, vol. 15, no. 1, p. 32897, 2025, doi: 10.1038/s41598-025-18387-y.

[25] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on Raspberry Pi," *Discover Applied Sciences*, vol. 7, no. 6, p. 597, 2025, doi: 10.1007/s42452-025-07201-z.

[26] Z. G. Al-Mekhlafi *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, pp. 1–19, 2025, doi: 10.1007/s44443-025-00140-0.

[27] H. Zheng, M. Luo, Y. Zhang, C. Peng, and Q. Feng, "A security-enhanced pairing-free certificateless aggregate signature for vehicular ad-hoc networks," *IEEE Systems Journal*, vol. 17, no. 3, pp. 3822–3833, 2023, doi: 10.1109/JSYST.2022.3220869.

[28] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, and F. Xu, "A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10456–10466, 2023, doi: 10.1109/TITS.2023.3275077.

[29] X. Wang *et al.*, "A privacy-preserving certificate-less aggregate signature scheme with detectable invalid signatures for VANETs," *Journal of Information Security and Applications*, vol. 89, p. 104001, 2025, doi: 10.1016/j.jisa.2025.104001.

[30] S. Pooja and C. B. Chandrakala, "Secure reviewing and data sharing in scientific collaboration: Leveraging blockchain and zero trust architecture," *IEEE Access*, vol. 12, pp. 92386–92399, 2024, doi: 10.1109/ACCESS.2024.3423338.

[31] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503–531, 2022.

[32] M. Wroński and Ł. Dzierzkowski, "Base of exponent representation matters-more efficient reduction of discrete logarithm problem and elliptic curve discrete logarithm problem to the QUBO problem," *Quantum Information and Computation*, vol. 24, no. 7–8, pp. 541–564, 2024, doi: 10.26421/QIC24.7-8-1.

[33] M. N. Udin and E. S. Ismail, "A new signcryption scheme using elliptic curve discrete logarithm problem," *Journal of Quality Measurement and Analysis*, vol. 21, no. 4, pp. 299–312, 2025, doi: 10.17576/jqma.2104.2025.15.

[34] J. Meers and J. Nowakowski, "Solving the hidden number problem for CSIDH and CSURF via automated Coppersmith," in *Lecture Notes in Computer Science*, 2023, vol. 14441 LNCS, pp. 39–71, doi: 10.1007/978-981-99-8730-6_2.

[35] S. K. Azmi, "Cryptographic hashing beyond SHA: Designing collision-resistant, quantum-resilient hash functions," *International Journal of Science and Research Archive*, vol. 12, no. 2, pp. 3119–3127, 2024, doi: 10.30574/ijsra.2024.12.2.1238.

[36] S. P. Cohen and M. Naor, "Low communication complexity protocols, collision resistant hash functions and secret key-agreement protocols," in *Lecture Notes in Computer Science*, 2022, vol. 13509 LNCS, pp. 252–281, doi: 10.1007/978-3-031-15982-4_9.

[37] Z. Y. Al Tmari *et al.*, "A post-quantum certificateless aggregate signature scheme for VANETs resilient to rogue-key attacks," *Journal of Communications*, vol. 21, no. 2, pp. 233–244, 2026, doi: 10.12720/jcm.21.2.233-244.
[38] L. Wang, J. Xu, B. Qin, M. Wen, and K. Chen, "An efficient fuzzy certificateless signature-based authentication scheme using anonymous biometric identities for VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 1, pp. 292–307, 2025, doi: 10.1109/TDSC.2024.3392470.
[39] H. Su, S. Dong, N. Wang, and T. Zhang, "An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs," *Vehicular Communications*, vol. 45, p. 100727, 2024, doi: 10.1016/j.vehcom.2024.100727.
[40] V. Adouth and E. Rajagopal, "QSKCG: Quantum-based secure key communication and key generation scheme for outsourced data in cloud," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 20, p. e8192, 2024, doi: 10.1002/cpe.8192.
[41] L. Wang, Z. Guan, Z. Chen, and M. Hu, "Multi-receiver signcryption scheme with multiple key generation centers through public channel in edge computing," *China Communications*, vol. 19, no. 4, pp. 177–198, 2022, doi: 10.23919/JCC.2022.04.014.
[42] M. S. M. AL-inizi and O. M. NSAIF, "Securing vehicle-to-vehicle communications: VANET challenges," *Babylonian Journal of Networking*, vol. 2023, pp. 105–111, 2023, doi: 10.58496/bjn/2023/014.
[43] T. Karunathilake and A. Förster, "A survey on mobile road side units in VANETs," *Vehicles*, vol. 4, no. 2, pp. 482–500, 2022, doi: 10.3390/vehicles4020029.
[44] L. Nagaraju, "Road side unit (RSU) misbehaviour detection in VANET using trust model," Master's thesis, *University of Windsor (Canada)*, 2024.
[45] Y. Bin Luo, B. S. Wang, X. F. Wang, X. F. Hu, G. L. Cai, and H. Sun, "RPAH: Random port and address hopping for thwarting internal and external adversaries," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 2015, vol. 1, pp. 263–270, doi: 10.1109/Trustcom.2015.383.
[46] D. Torrieri, S. Zhu, and S. Jajodia, "Cyber maneuver against external adversaries and compromised nodes," in *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*, Springer, 2013, pp. 87–96, doi: 10.1007/978-1-4614-5416-8_5.
[47] M. A. Al-Shareeda and S. Manickam, "A systematic literature review on security of vehicular ad-hoc network (VANET) based on VEINS framework," *IEEE Access*, vol. 11, pp. 46218–46228, 2023.
[48] X. Dang, G. Zhang, K. Sun, and Y. Li, "A trust model for VANETs using malicious-aware multiple routing," *Computers and Security*, vol. 148, p. 104145, 2025, doi: 10.1016/j.cose.2024.104145.

BIOGRAPHIES OF AUTHORS



Saima Anwar Lashari is an assistant professor in the College of Computing and Informatics, Saudi Electronic University. She received her B.Sc. (Hons.) in computer science from the University of Engineering and Technology (UET), Lahore, Pakistan, in 2004, the M.S. degree in information technology from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia, in 2012, and the Ph.D. degree in information technology from UTHM in 2016. She also served as a postdoctoral researcher at UTHM before joining Saudi Electronic University. She can be contacted at email: s.lashari@seu.edu.sa.



Zahraa T. Hano is a lecturer at Shatt Al-Arab University College, Basra, Iraq. She received her B.Sc. and M.Sc. degrees in chemistry from the University of Basrah, Iraq. Her research interests include biopolymers, in vitro drug delivery systems, and biological applications of plant extracts. She can be contacted at email: zahraa.talb.hano@sa-uc.edu.iq.



Abdulnasser AbdulJabbar Abbood is an academic staff member in the Department of Electronic Technologies at the Basra Technical Institute, Southern Technical University, Basra, Iraq, where he also serves as the assistant dean for scientific affairs. He received his B.Sc. degree in electrical engineering and his M.Sc. and Ph.D. degrees in electrical engineering with a specialization in communications and computer engineering. His research interests include communication systems, wireless communications, computer networks, digital signal processing, network optimization, cybersecurity, authentication protocols, and resource-constrained computing. He has authored and co-authored numerous publications in international peer-reviewed journals and actively contributes to research in secure communication systems and intelligent networking technologies. He can be contacted at email: abdulnasser.abbood@stu.edu.iq.



Murtaja Ali Saare is an assistant professor with the Department of Computer Technology Engineering, Shatt Al-Arab University, Basra, Iraq. He received his B.Sc. degree in computer science, his M.Sc. degree in information technology from Universiti Utara Malaysia in 2017, and his Ph.D. degree in computing from the School of Computing, Universiti Utara Malaysia, Malaysia, in 2021. His research interests include the Internet of Things (IoT), e-health, human-centered computing, artificial intelligence, cybersecurity, wireless sensor networks, blockchain, and smart healthcare systems. He has authored numerous publications in reputable Scopus-indexed journals and actively contributes to research in intelligent computing and emerging communication technologies. He can be contacted at email: murtaja.a.sari@sa-uc.edu.iq.



Mohammed Amin Almaiah is an associate professor at the King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan. He received his Ph.D. degree in computer science from Universiti Malaysia Terengganu (UMT), Malaysia. He has extensive academic and research experience in the fields of cybersecurity, mobile learning, artificial intelligence, cloud computing, Internet of Things (IoT), e-learning systems, and software quality. He has published numerous scientific articles in highly ranked international journals indexed in Scopus and Web of Science. His current research interests include cybersecurity applications, artificial intelligence in education, smart learning environments, blockchain technology, cloud and mobile computing, and digital transformation technologies. He can be contacted at email: m.almaiah@ju.edu.jo.



Rami Shehab is a researcher and academic affiliated with King Faisal University, Al-Ahsa, Saudi Arabia, where he is currently associated with the Vice-Presidency for Postgraduate Studies and Scientific Research. His research focuses on cybersecurity, Internet of Medical Things (IoMT), lightweight authentication protocols, artificial intelligence applications, and intelligent healthcare systems. He has contributed to several scientific publications in international journals and conferences indexed in Scopus and other reputable databases. His recent research interests include lightweight cryptography, secure authentication for IoT environments, sustainable healthcare security systems, and intelligent computing technologies. He can be contacted at email: Rtshehab@kfu.edu.sa.



Mahmood A. Al-Shareeda is a distinguished academic and researcher, currently serving as a lecturer at Southern Technical University in Basra, Iraq. He previously held a postdoctoral fellowship at the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), in Penang, Malaysia. He completed his B.Sc., M.Sc., and Ph.D. degrees in Iraq, Lebanon, and Malaysia, respectively, reflecting a rich and diverse educational background across three nations. His outstanding contributions to research and academia have earned him global recognition, including being listed among the top 2% of scientists worldwide by Stanford University/Elsevier for the significant impact of his scholarly work. His expertise encompasses a wide range of research areas, including network monitoring, Internet of Things (IoT), vehicular ad-hoc network (VANET) security, and IPv6 security. He can be contacted at email: Mahmood.alshareedah@stu.edu.iq.