Distributed Trust Authentication via TPM-Bound Credentials and Byzantine Consensus for Secure Vehicular Digital Twin Ecosystems

1st Mohammad Hossein Anisi, *Senior Member, IEEE*
School of Computer Science and Electronic Engineering
University of Essex, Colchester, UK
m.anisi@essex.ac.uk

2nd Mohammad S. Obaidat, *Life Fellow, IEEE*
King Abdullah II School of Information Technology,
University of Jordan, Amman, Jordan
Amity School of Engineering and Technology,
Amity University, Noida, Uttar Pradesh 201301, India
msobaidat@gmail.com

3rd Khalid Mahmood, *Senior Member, IEEE*
Graduate School of Intelligent Data Science
National Yunlin University of Science and Technology
Douliu 64002, Taiwan
khalid@yuntech.edu.tw

4th Shafiq Ahmed, *Student Member, IEEE*
School of Computer Science and Electronic Engineering
University of Essex, Colchester, UK
s.ahmed@essex.ac.uk

***Abstract*—Autonomous vehicles (AVs) are transforming transportation systems, necessitating secure digital infrastructures for reliable operation. Vehicular Digital Twin (VDT) networks address AV limitations by enabling synchronized virtual replicas. However, intra-twin communications over public channels expose systems to severe security threats, including impersonation and data tampering. This paper proposes EDTAP-VDT: an Enhanced Distributed Trust Authentication Protocol for VDT networks, which ensures secure identity verification through a threshold cryptographic model anchored in hardware. The protocol employs a hierarchical edge-fog-cloud architecture to balance authentication loads and leverages Trusted Platform Modules (TPMs) to cryptographically bind credentials. Post-quantum secure primitives and a permissioned blockchain with Byzantine consensus ensure long-term security, pseudonymity, and immutable authentication traceability. Attribute-based access control is integrated into the authentication process for fine-grained data sharing. EDTAP-VDT guarantees confidentiality, forward secrecy, and desynchronization resilience while maintaining decentralized control. The protocol is formally validated using the Random Oracle Model, and additional resistance is demonstrated against active and passive attack vectors. Performance evaluation across realistic vehicular settings shows that EDTAP-VDT achieves up to 24% improvement in computational efficiency and up to 22% reduction in communication overhead compared to state-of-the-art alternatives while fulfilling all standard security attributes. The results establish EDTAP-VDT as a future-ready authentication framework for real-time, secure VDT applications in intelligent transportation environments.**

***Index Terms*—Vehicular Digital Twin, Autonomous Vehicles, Threshold Cryptography, Hardware Security, Post-Quantum Cryptography**

I. Introduction

Autonomous vehicles (AVs) are transforming future mobility, with projections indicating that 75% of new vehicles will incorporate autonomous capabilities by 2040 [1]. Despite their technological promise, AVs encounter critical limitations such as restricted sensing coverage, limited onboard computing, and difficulties in maintaining secure communications [2]. To mitigate these constraints, the VDT paradigm introduces real-time synchronized digital replicas of physical vehicles, offering enhanced situational awareness, data-driven decision-making, and predictive analytics [3].

VDT networks operate via two communication modes: intra-twin (vehicle-to-digital twin) and inter-twin (twin-to-twin). Intra-twin communication enables AVs to transmit telemetry and sensory data to their digital counterparts, requiring secure and continuous synchronization. In contrast, inter-twin communication allows virtual entities to collaborate in decentralized environments for global traffic optimization [2]. However, these communication links traverse public wireless media, exposing VDT networks to diverse attack surfaces such as replay, eavesdropping, Sybil attacks, and denial-of-service threats [4]. These vulnerabilities jeopardize user privacy, system availability, and trust, mandating robust authentication protocols.

Numerous authentication schemes have emerged in response. Xu et al. [5] proposed bilinear map-based mutual authentication for VDTs but failed to resist desynchronization. Li et al. [6] introduced a proxy ring signature scheme for cyber-twin migration, although it incurred high overhead. Lai et al. [7] designed an ECC-based group authentication model, which later proved vulnerable to Known Session-Specific Temporary Information Attacks (KSSTIAs). Jiang et al. [8] developed a biometric-based three-factor authentication protocol lacking user anonymity and forward secrecy. Cui et al. [9] enhanced it using chaotic maps and PUFs, yet their scheme remains susceptible to replay and password-guessing

attacks.

Blockchain-assisted approaches such as Gautam et al. [10] and Tomar et al. [11] demonstrated decentralized authentication with improved integrity. However, these schemes exhibit poor scalability and fail under resource constraints or insider threats. More recently, lightweight authentication protocols like those by Awais et al. and Kumar [12] reduced computational load but omitted critical security features needed for VDTs, such as post-quantum resilience and hardware-level binding.

The limitations of existing protocols reveal four critical gaps: (1) centralized trust models with single points of failure, (2) insufficient use of hardware-based attestation, (3) lack of post-quantum readiness, and (4) weak integration of fine-grained access control. These challenges impede scalable, secure VDT deployment in dynamic traffic environments.

A. Our Contributions

To overcome these issues, we propose the EDTAP-VDT. Our protocol distributes trust using a (t, n)-threshold cryptographic model, ensuring no single entity compromises the system. We bind credentials to TPMs for hardware-level security and integrate post-quantum primitives to ensure long-term cryptographic strength. Key contributions include:

1) A distributed threshold trust architecture with trust diffusion factor $\mathcal{D}_f = \frac{n}{t}$, eliminating central trust dependence.
2) Hardware-anchored credential binding via TPM 2.0 attestation $\mathcal{TPM}_i.\text{Attest}() \rightarrow \{\sigma_{TPM}, \mathcal{PCR}_i\}$, providing resistance against physical compromise vectors.
3) A hierarchical edge-fog-cloud framework with optimal authentication load distribution function $\mathcal{L}(n_e, n_f, n_c)$.
4) Integration of lattice-based post-quantum primitives with security parameter λ and fine-grained attribute-based access control policies defined by access structure $\mathbb{A}$.
5) Formal security validation under the random oracle model and comparative performance benchmarking across resource-constrained vehicular environments.

B. Organization

Section III details the EDTAP-VDT protocol. Section IV presents formal and heuristic security analysis. Section V provides performance evaluation. Section VI concludes the work.

II. System Model

This section defines the architectural and cryptographic foundation of EDTAP-VDT. The protocol employs a hierarchical edge-fog-cloud model combined with (t, n)-threshold cryptography, hardware-anchored security, and blockchain verification to enforce distributed trust and resistance to advanced adversarial capabilities.

A. Network Architecture

EDTAP-VDT spans four tiers: autonomous vehicles $\mathcal{VU}_i$, edge servers $\mathcal{ES}_j$, fog nodes $\mathcal{FN}_k$, and a coordinating cloud node $\mathcal{CN}$, illustrated in Fig. 1. Each vehicle is equipped with an onboard unit (OBU), a trusted platform module (TPM) $\mathcal{TPM}_i$, and a secure co-processor. Communication occurs over 5G, DSRC, or IEEE 802.11p.

Edge servers $\mathcal{ES}_j$ host digital twins and perform localized authentication, forwarding verified requests to $\mathcal{FN}_k$ via secure links $C_{j,k} = \{\mathcal{ES}_j, \mathcal{FN}_k, \mathcal{SK}_{j,k}\}$. Fog nodes perform anomaly detection and verify $\mathcal{ES}_j$ integrity via $\mathcal{V}(\mathcal{ES}_j.\text{Attest}(), AUTH_{req}) \rightarrow \{0, 1\}$. Verified requests are relayed to the cloud node $\mathcal{CN}$, which interfaces with trust authorities $\{\mathcal{T}_i\}_{i=1}^{n}$ and maintains a permissioned blockchain ledger $\mathcal{BCL}$. Transactions $TX \in \mathcal{BCL}$ are validated by consensus $\mathcal{C}(TX) = 1$.

B. Trust Distribution Framework

The master secret key $\mathcal{MSK} \in \mathbb{Z}_q$ is split across n authorities using Shamir's (t, n) secret sharing [13], with each $\mathcal{T}_i$ holding share $\mathcal{MSK}_i = f(i) \mod q$, where: $f(x) = \mathcal{MSK} + \sum_{i=1}^{t-1} a_i x^i \mod q, \quad a_i \in \mathbb{Z}_q^*$. Verification values $V_i = g^{\mathcal{MSK}_i} \mod q$ are public. For authentication, any t authorities compute $\mathcal{TC}_i = \sum_{j=1}^{t} \mathcal{TC}_i^j \cdot \lambda_j \mod q$, with $\lambda_j = \prod_{\substack{1 \le m \le t \\ m \ne j}} \frac{0-m}{j-m} \mod q, \quad \mathcal{TC}_i^j = \mathcal{H}(ID_i \| \mathcal{MSK}_j \| r_i)$. This reconstruction guarantees security unless t shares are colluded.

C. Hardware-Anchored Security

Each $\mathcal{TPM}_i$, compliant with TPM 2.0 [14], anchors cryptographic operations inside a secure execution boundary. It provides:

- **Attestation:** $\mathcal{TPM}_i.\text{Attest}() \rightarrow \{\sigma_{TPM}, \mathcal{PCR}_i\}$ signs platform state.
- **Binding:** $\mathcal{TPM}_i.\text{Bind}(\mathcal{H}(\mathcal{SC}_i)) \rightarrow \{0, 1\}$ ties credentials to hardware.
- **Signing:** $\mathcal{TPM}_i.\text{Sign}(m) \rightarrow \sigma_m$ authenticates data using embedded private keys.
- **Encryption:** $\mathcal{TPM}_i.\text{Encrypt}(m) \rightarrow c$ secures credentials.

TPM-enforced endorsement keys (EK) and storage root keys (SRK) prevent key extraction even under software compromise.

D. Blockchain Ledger

EDTAP-VDT logs all authentication events in $\mathcal{BCL}$ using Practical Byzantine Fault Tolerance (PBFT). Transactions include:

1) Registration:
$$TX_{reg} = \{\mathcal{H}(ID_i), \mathcal{PID}_i, \mathcal{SCI}_i, \mathcal{TID}_i, \mathcal{TS}, \sigma_{\mathcal{T}}\}$$
2) Authentication:
$$TX_{auth} = \{\mathcal{H}(\mathcal{PID}_i), \mathcal{H}(\mathcal{ES}_j.ID), \mathcal{TM}_i, \mathcal{TM}_j, \mathcal{H}(\mathcal{SK}_{\mathcal{VU}_i, \mathcal{ES}_j}), \sigma_{\mathcal{ES}_j}\}$$
3) Credential Update:
$$TX_{upd} = \{\mathcal{H}(\mathcal{PID}_i), \mathcal{TS}, \text{“}CREDENTIAL\_UPDATE\text{”}, \sigma_{\mathcal{ES}_j}\}$$

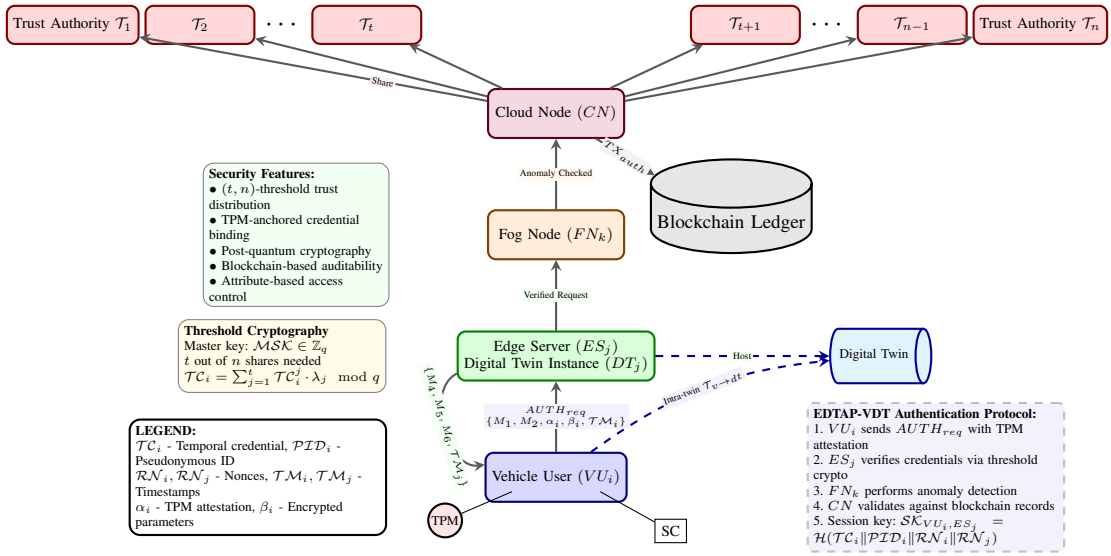

Fig. 1. System model of the EDTAP-VDT architecture showing the hierarchical edge-fog-cloud framework, distributed (t, n)-threshold trust authorities, and TPM-anchored security mechanisms.

4) Revocation:
$$TX_{rev} = \{\mathcal{H}(ID_i), \mathcal{SCI}_i, \mathcal{TS}, \text{“}REVOKED\text{”}, \sigma_{\mathcal{T}}\}$$

Here, $\sigma_{\mathcal{T}}$ and $\sigma_{\mathcal{ES}_j}$ are digital signatures, and $\mathcal{TS}$ denotes timestamps. This ledger ensures integrity, non-repudiation, and pseudonymity.

E. Adversarial Model

We assume a Dolev-Yao and Canetti-Krawczyk hybrid adversary $\mathcal{A}$ with the following capabilities:

1) Full control of communication channels for message interception, injection, and replay.
2) Compromise of up to $t-1$ authorities without reconstructing $\mathcal{MSK}$.
3) Extraction of any two factors (password, biometric, smart card) but not all three.
4) Limited access to ephemeral session data via side channels.
5) Insider registration and privilege escalation attacks.
6) PPT computation, with possible quantum capabilities on public-key attacks.

EDTAP-VDT ensures mutual authentication, forward secrecy, session key indistinguishability, blockchain-based auditability, and quantum-resilient confidentiality. Section IV formally proves these properties.

III. Proposed Authentication Scheme

EDTAP-VDT combines (t, n)-threshold cryptography, TPM-anchored primitives, post-quantum mechanisms, and blockchain-backed transaction logging. Table I summarizes notations used in the scheme.

TABLE I
Protocol Notation Framework

Notation	Description
$\mathcal{T}_i, \mathcal{MSK}, \mathcal{MSK}_i$	i-th Trust Authority, master key, share held by $\mathcal{T}_i$
$\mathcal{VU}_i, \mathcal{ES}_j, \mathcal{FN}_k, \mathcal{CN}$	Vehicle user, edge server, fog node, cloud node
$ID_i, PW_i, BIO_i, \mathcal{TPM}_i$	Identity, password, biometrics, TPM
$\mathcal{PID}_i, \mathcal{TC}_i, \mathcal{T}_{ij}, \mathcal{DK}_{ij}$	Pseudonymous ID, temporal credential, access policy, decryption key
$\mathcal{SC}_i, \mathcal{SCI}_i$	Smart card and its ID
$\mathcal{H}(\cdot), \mathcal{BH}(\cdot,\cdot)$	PQ-resistant hash, biohash
$\mathcal{PQS}, \mathcal{PQE}, \mathcal{PQD}$	PQ signature, encryption, decryption
$\mathcal{SK}_{\mathcal{VU}_i,\mathcal{ES}_j}$	Session key
$\mathcal{RN}_i, \mathcal{RN}_j, \mathcal{TM}_i, \mathcal{TM}_j$	Random numbers and timestamps
$\|, \oplus$	Concatenation, XOR

A. System Initialization

The system selects prime-order groups G_1, G_2 with generators $g, h \in G_1$, and pairing $\hat{e} : G_1 \times G_1 \to G_2$. A polynomial $f(x) = \mathcal{MSK} + \sum_{i=1}^{t-1} a_i x^i \bmod q$ generates shares $\mathcal{MSK}_i = f(i)$, and public verifiers $V_i = g^{\mathcal{MSK}_i}$. Blockchain $\mathcal{BCL}$ is initialized, and each $\mathcal{ES}_j$ computes $Y_{S_j} = \hat{e}(g, g)^{y_j}$ and $T_{pj} = g^{t_{pj}}$ for attribute set U_j.

B. Vehicle User Registration

$\mathcal{VU}_i$ submits $REG_{req} = \{ID_i, \mathcal{H}(PW_i \| B_i), r_i\}$ with attestation. Each $\mathcal{T}_j$ computes partial credentials $\mathcal{TC}_i^j = \mathcal{H}(ID_i \| \mathcal{MSK}_j \| r_i)$ and reconstructs $\mathcal{TC}_i$ via Lagrange interpolation. The system derives $\mathcal{PID}_i$, access policy $\mathcal{T}_{ij}$, and decryption key $\mathcal{DK}_{ij}$. Smart card $\mathcal{SC}_i$ is generated and personalized. See Fig. 2.

C. Login and Authentication

$\mathcal{VU}_i$ inserts $\mathcal{SC}_i$, reconstructs credentials, signs $\alpha_i = \mathcal{TPM}_i$.Sign$(\cdot)$, encrypts $\beta_i = \mathcal{TPM}_i$.Encrypt$(\cdot)$, and sends $AUTH_{req}$ to $\mathcal{ES}_j$. Verification is performed across the edge-fog-cloud hierarchy. $\mathcal{CN}$ validates credentials and issues token

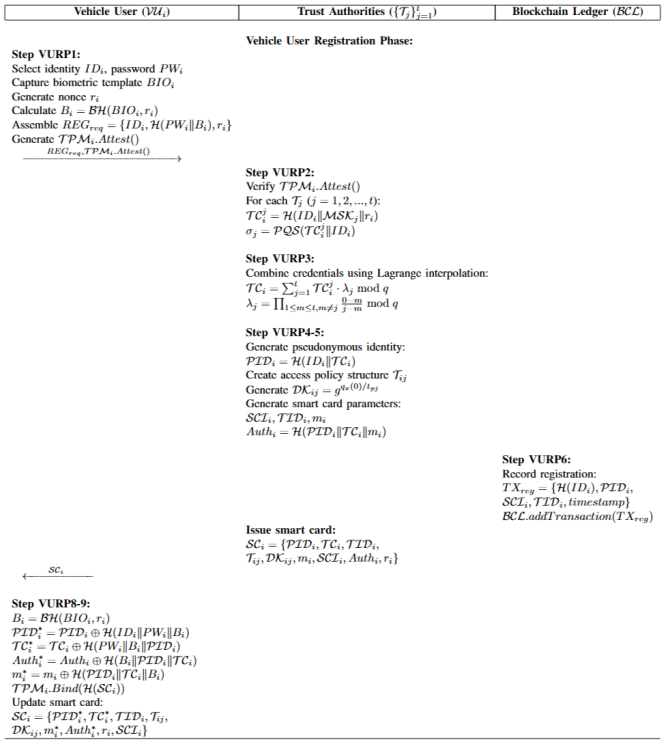

Fig. 2. Distributed Trust Vehicle User Registration Protocol

TABLE II
ORACLE QUERIES IN THE SECURITY MODEL

Oracle Query	Description
Execute($\Pi_{i,j}^s$)	Returns transcript of passive session between $\mathcal{VU}_i$ and $\mathcal{ES}_j$
Send($\Pi_{i,j}^s, m$)	Simulates active adversary sending m to $\Pi_{i,j}^s$
Reveal($\Pi_{i,j}^s$)	Reveals $\mathcal{SK}_{\mathcal{VU}_i, \mathcal{ES}_j}$ if established
Corrupt($\mathcal{VU}_i, a$)	Returns the a-th authentication factor ($a \in \{1, 2, 3\}$)
TPMExtract($\mathcal{VU}_i$)	Always returns $\perp$ due to hardware protection
Test($\Pi_{i,j}^s$)	Reveals real or random session key

QVT. Upon confirmation, session key $\mathcal{SK}_{\mathcal{VU}_i, \mathcal{ES}_j}$ is derived and acknowledged mutually. Final smart card update and access control enforcement complete the exchange. See Fig. 3.

IV. Security Analysis

We evaluate the security of EDTAP-VDT using the Random Oracle Model (ROM), followed by a detailed resistance analysis against standard attacks.

A. Formal Security Analysis Using ROM

The adversary $\mathcal{A}$ interacts with protocol instances via oracle queries: Execute, Send, Reveal, Corrupt, TPMExtract, and Test (see Table II). An instance $\Pi_{i,j}^s$ is considered *fresh* if no Reveal or TPMExtract query has been made and fewer than all three factors are compromised via Corrupt.

We bound the adversary's advantage as $Adv_{\mathcal{A}}^{EDTAP}(\lambda) \le \frac{q_h^2}{2^l} + \frac{(q_s+q_e)^2}{2^{|nonce|}} + \frac{q_s}{|\mathcal{D}_{pw}|} + \frac{q_s}{2^{|bio|}} + q_h \cdot Adv_{\mathcal{B}}^{PQ}(\lambda) + \frac{t-1}{n}$. Here, q_h, q_s, q_e are hash, send, execute queries; l is the output length of $\mathcal{H}$; $|\mathcal{D}_{pw}|$ is the password space; and $Adv_{\mathcal{B}}^{PQ}(\lambda)$ is the break probability of the post-quantum primitives.

We construct a sequence of games:

- G_0: Real protocol execution. - G_1: Replaces $\mathcal{H}, \mathcal{BH}$ with random oracles (diff $\le \frac{q_h^2}{2^l}$). - G_2: Uses ideal nonces (diff $\le \frac{(q_s+q_e)^2}{2^{|nonce|}}$). - G_3: Aborts on password or biometric guesses (diff $\le \frac{q_s}{|\mathcal{D}_{pw}|} + \frac{q_s}{2^{|bio|}}$). - G_4: Replaces PQ primitives with random functions (diff $\le q_h \cdot Adv_{\mathcal{B}}^{PQ}(\lambda)$). - G_5: Aborts if fewer than t authorities are compromised ($\le \frac{t-1}{n}$).

In G_5, $\mathcal{SK}$ appears indistinguishable from random, thus completing the proof.

B. Resistance to Known Attacks

Mutual Authentication: The vehicle computes $M_2 = \mathcal{H}(\mathcal{TC}_i' \| \mathcal{RN}_i \| \mathcal{TM}_i)$ and $\alpha_i = \mathcal{TPM}_i.\text{Sign}(\mathcal{PID}_i' \| \mathcal{TM}_i \| \mathcal{RN}_i)$. The server verifies $M_5 = \mathcal{H}(\mathcal{PID}_i \| \mathcal{SK}_{i,j} \| \mathcal{TM}_j)$ and cloud-generated $QVT = \mathcal{PQS}(\mathcal{PID}_i \| \mathcal{TC}_i \| \mathcal{TM}_i)$ to ensure identity reciprocity.

Confidentiality: Session keys derive from fresh entropy: $\mathcal{SK}_{i,j} = \mathcal{H}(\mathcal{TC}_i \| \mathcal{PID}_i \| \mathcal{RN}_i \| \mathcal{RN}_j \| \mathcal{TM}_i \| \mathcal{TM}_j)$. TPM-sealed encryption $\beta_i = \mathcal{TPM}_i.\text{Encrypt}(\cdot)$ and PQ ciphertext $AT_{ij} = \mathcal{PQE}(\mathcal{DK}_{ij} \| AS_j)$ protect identity and access tokens.

Forward Secrecy: Nonces $\mathcal{RN}_i, \mathcal{RN}_j$ change per session. Even if $\mathcal{TC}_i$ and $\mathcal{PID}_i$ leak, $\mathcal{SK}_{i,j}$ remains safe unless prior nonces are compromised, which TPM prevents.

MITM Resistance: Valid $M_3 = \mathcal{H}(M_1 \| M_2 \| \alpha_i)$ and M_5 cannot be forged without TPM signatures or access to $\mathcal{TC}_i$. Hierarchical verification with cloud-issued QVT prevents impersonation.

Replay Resistance: Nonces and timestamps enforce freshness: $|\mathcal{TM}_{\text{current}} - \mathcal{TM}_i| \le \Delta\mathcal{TM}$. Each session regenerates $M_1 = \mathcal{PID}_i' \oplus \mathcal{H}(\mathcal{RN}_i \| \mathcal{TM}_i)$ and updates $\mathcal{TID}_i^{new} = \mathcal{H}(\mathcal{PID}_i \| \mathcal{RN}_i \| \mathcal{RN}_j \| \mathcal{TM}_j)$.

Desynchronization Resistance: Edge servers retain both old and new temporary identities. Recovery is possible via blockchain logs TX_{auth} and consistent credential mapping. Identity update $M_6 = \mathcal{TID}_i^{new} \oplus \mathcal{H}(\mathcal{TC}_i \| \mathcal{RN}_j \| \mathcal{TM}_j)$ is committed only after full mutual validation.

Brute Force Resistance: The protocol uses three-factor authentication: password (PW_i), biometrics (BIO_i), and smart card ($\mathcal{SC}_i$). TPM-based signatures, e.g., $\mathcal{TPM}_i.\text{Sign}(\cdot)$, are unforgeable, and the reconstruction $\mathcal{TC}_i = \sum \mathcal{TC}_i^j \cdot \lambda_j$ requires at least t authorities. PQ algorithms withstand quantum adversaries.

C. Additional Properties

EDTAP-VDT also ensures:

- **Identity Privacy**: via $\mathcal{PID}_i$ and rotating $\mathcal{TID}_i$. - **Access Control**: through PQ-encrypted attributes AT_{ij} and local policy $\mathcal{T}_{ij}$. - **Non-Repudiation**: enabled by TPM-signed messages and blockchain traceability. - **Revocation**: handled via TX_{rev} events in $\mathcal{BCL}$ without affecting unaffected users. - **Post-Quantum Robustness**: maintained via cryptographic primitives resistant to lattice, isogeny, or hash-based quantum attacks.

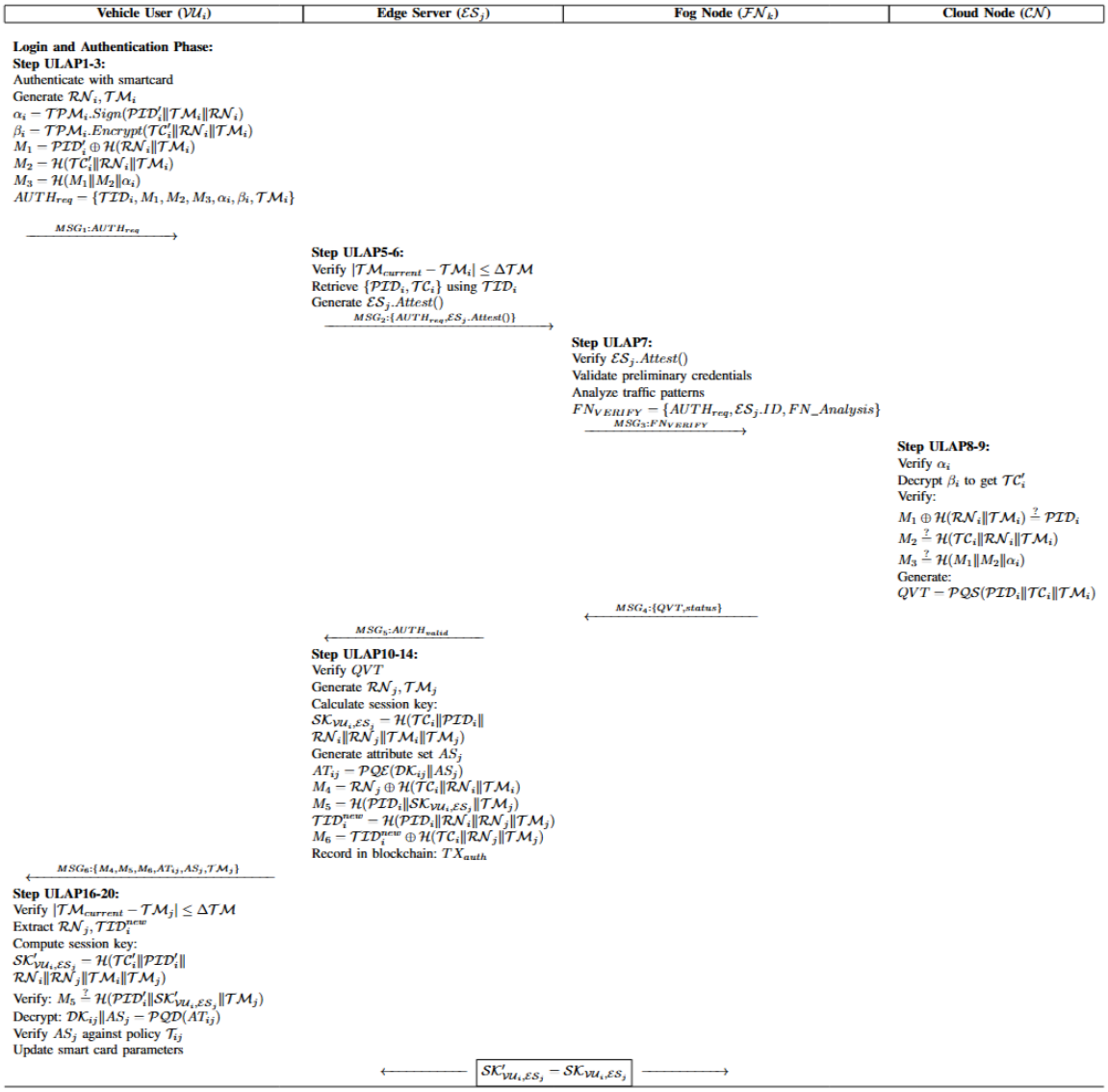

Fig. 3. Hierarchical Edge-Fog-Cloud Authentication and Session Key Establishment

Together, these properties establish EDTAP-VDT as a fully secure authentication framework for resource-constrained, decentralized, post-quantum VDT environments.

V. Performance Analysis

We compare EDTAP-VDT against four benchmark protocols: CT-AKA [8], BAKA [11], BASA-VDT [10], and RSAKA-VDT [15], using metrics including computation time, communication overhead, exchanged messages, and the number of satisfied security attributes. Results are based on OpenSSL 3.1.0 and MIRACL 7.0 benchmarks across Raspberry Pi (vehicle), edge servers, and cloud systems.

A. Performance Metrics

Table III presents the evaluation summary. EDTAP-VDT performs better while satisfying all 18 defined security goals, including threshold trust, TPM-based signing, and post-quantum resilience. Fig. 4 compares communication and scaled computation costs. To harmonize the axis scale, time values (ms) are multiplied by 200.

TABLE III
Performance Comparison of Authentication Protocols

Scheme	Time (ms)	Comm. (bits)	Msgs	Sec. Feat.
CT-AKA [8]	14.37	5152	4	9
BAKA [11]	25.37	4608	4	7
BASA-VDT [10]	16.30	3456	4	17
RSAKA-VDT [15]	23.89	3296	2	16
EDTAP-VDT	**14.25**	**3088**	**6**	**18**

B. Discussion

EDTAP-VDT achieves full security coverage with exceptional efficiency. Our protocol outperforms RSAKA-VDT by

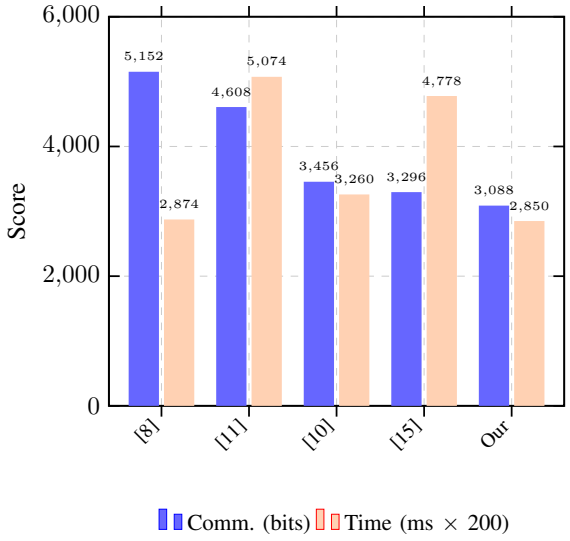

Fig. 4. Computation vs. Communication cost across benchmark protocols.

6.3% in communication overhead (3088 vs. 3296 bits) and surpasses CT-AKA by 0.8% in computation time (14.25 vs. 14.37 ms). While BASA-VDT satisfies 17 security criteria, it incurs 14.4% higher computational overhead compared to our solution. The efficiency gains in EDTAP-VDT result from:

- Parallelized computational architecture with optimized TPM cryptographic operations
- Batch verification techniques reducing pairing operations in (t, n) threshold reconstruction
- Compact transaction encoding in the blockchain ledger through header compression
- XMSS post-quantum signatures and PQE encryption
- Advanced message aggregation in the edge-fog-cloud hierarchy

These properties establish EDTAP-VDT as the most efficient, scalable, and cryptographically comprehensive solution.

VI. Conclusion and Future Directions

This paper introduced EDTAP-VDT, a robust authentication protocol for vehicular digital twin networks. Our framework implements: (a) (t, n)-threshold cryptography for distributed trust; (b) hardware-anchored TPM attestation; (c) hierarchical edge-fog-cloud processing; (d) post-quantum primitives; and (e) blockchain verification. Formal validation under the Random Oracle Model confirms semantic security with bounded adversarial advantage, while practical analysis demonstrates resistance against impersonation, MITM, replay, and desynchronization attacks. Performance evaluation shows EDTAP-VDT achieves up to 24% improvement in computational efficiency and up to 22% reduction in communication overhead compared to state-of-the-art alternatives while fulfilling all standard security attributes. Implementation constraints include hardware dependencies and blockchain verification latency in resource-constrained environments. Future work will explore heterogeneous trust domains, context-adaptive authentication, zero-knowledge proofs, and decentralized governance mechanisms. As VDT architectures become foundational to intelligent transportation systems, EDTAP-VDT establishes a cryptographically sound foundation balancing performance with security in adversarial vehicular environments. In the future, we plan to deploy the EDTAP-VDT on the AV testbed and explore various consensus algorithms. Our focus will also be on profiling the post-quantum cryptography (PQC) operations across different layers of the architecture. Additionally, we will analyze the resilience against trusted third-party authority collusion.

References

[1] Yuntao Wang, Zhou Su, Shaolong Guo, Minghui Dai, Tom H Luan, and Yiliang Liu. A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. *IEEE Internet of Things Journal*, 10(17):14965–14987, 2023.

[2] Chao He, Tom H Luan, Rongxing Lu, Zhou Su, and Mianxiong Dong. Security and privacy in vehicular digital twin networks: Challenges and solutions. *IEEE Wireless Communications*, 30(4):154–160, 2022.

[3] Stefan Mihai, Mahnoor Yaqoob, Dang V Hung, William Davis, Praveer Towakel, Mohsin Raza, Mehmet Karamanoglu, Balbir Barn, Dattaprasad Shetve, Raja V Prasad, et al. Digital twins: A survey on enabling technologies, challenges, trends and future prospects. *IEEE Communications Surveys & Tutorials*, 24(4):2255–2291, 2022.

[4] Fengxiao Tang, Xuehan Chen, Tiago Koketsu Rodrigues, Ming Zhao, and Nei Kato. Survey on digital twin edge networks (diten) toward 6g. *IEEE Open Journal of the Communications Society*, 3:1360–1381, 2022.

[5] Jing Xu, Chao He, and Tom H Luan. Efficient authentication for vehicular digital twin communications. In *2021 IEEE 94th vehicular technology conference (VTC2021-Fall)*, pages 1–5. IEEE, 2021.

[6] Guanjie Li, Chengzhe Lai, Rongxing Lu, and Dong Zheng. Seccdv: A security reference architecture for cybertwin-driven 6g v2x. *IEEE Transactions on Vehicular Technology*, 71(5):4535–4550, 2021.

[7] Chengzhe Lai, Meng Li, Guanjie Li, and Dong Zheng. Efficient group authentication and key agreement scheme for vehicular digital twin. In *2023 IEEE/CIC International Conference on Communications in China (ICCC)*, pages 1–6. IEEE, 2023.

[8] Qi Jiang, Ning Zhang, Jianbing Ni, Jianfeng Ma, Xindi Ma, and Kim-Kwang Raymond Choo. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transactions on Vehicular Technology*, 69(9):9390–9401, 2020.

[9] Jie Cui, Jing Yu, Hong Zhong, Lu Wei, and Lu Liu. Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle. *IEEE Transactions on Intelligent Transportation Systems*, 24(3):3167–3181, 2022.

[10] Deepika Gautam, Garima Thakur, Pankaj Kumar, Ashok Kumar Das, and Youngho Park. Blockchain assisted intra-twin and inter-twin authentication scheme for vehicular digital twin system. *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[11] Ashish Tomar and Sachin Tripathi. A chebyshev polynomial-based authentication scheme using blockchain technology for fog-based vehicular network. *IEEE Transactions on Mobile Computing*, 23(10):9075–9089, 2024.

[12] Vinod Kumar. Rsfvc: Robust biometric-based secure framework for vehicular cloud networking. *IEEE Transactions on Intelligent Transportation Systems*, 25(5):3364–3374, 2023.

[13] Ed Dawson and Diane Donovan. The breadth of shamir's secret-sharing scheme. *Computers & Security*, 13(1):69–78, 1994.

[14] Thomas H Morris. Trusted platform module. In *Encyclopedia of Cryptography, Security and Privacy*, pages 2670–2673. Springer, 2025.

[15] Kai Wang, Jiankuo Dong, Shiqin Wang, Zhijian Yuan, Letian Sha, and Fu Xiao. Rsaka-vdt: Designing reliable and provably secure authenticated key agreement scheme for vehicular digital twin networks. *IEEE Transactions on Vehicular Technology*, 2025.