

# A Review on Authentication and Key-Establishment Protocols in Internet of Vehicles

Amiya Kumar Sahu<sup>1</sup>

<sup>1</sup>Asst. Professor, Department of Computer Science and Applications,  
Sambalpur University, Odisha, India,

\*\*\*

**Abstract** - Secure authentication mechanism and efficient Key-Establishment protocols are fundamental requirements for the Internet of Vehicles (IoV). In addition, safety-critical messaging, high mobility, and device heterogeneity implies strict performance, privacy, and robustness constraints. This manuscript synthesizes the recent research contributions across five principal approaches, such as, hardware-rooted Physical Unclonable Function schemes, blockchain enabled decentralization and batch verification, anonymous or conditional-privacy protocols, edge/ UAV-assisted continuity and handover, and group/seamless handover schemes. We examine cryptographic primitives, protocol flows, claimed security properties, computational and communication costs, methodologies for evaluation, and practical deployment challenges. The review highlights recurring gaps—standardized adversary models, city-scale empirical evaluation, secure offload attestation, and transitional interoperability and proposes a concrete research agenda aimed at bridging the gap between theoretical proposals and real-world IoV deployments.

**Key Words:** Internet of Vehicles, Authentication, Key establishment, PUF, Blockchain, Edge computing, UAV, Privacy, Handover

## 1. INTRODUCTION

The Internet of Vehicles (IoV) augments vehicular ad-hoc networks (VANETs) with roadside infrastructure, fog/edge computing, cloud services, and often aerial elements such as unmanned aerial vehicles (UAVs)[1]. Real-time safety applications, such as, collision warnings, cooperative adaptive cruise control, impose stringent latency and reliability requirements. At the same time, privacy concerns, for example, driver anonymity with conditional accountability, are of serious concern. Device heterogeneity, such as, resource-constrained on-board units, or OBUs, and resource-rich RSUs/edge, and high mobility with frequent handovers create a constrained design space for authentication and session key establishment [2, 3]. High vehicular mobility generates frequent handovers, while heterogeneous computational capabilities across OBUs, RSUs, and UAVs complicate protocol design. As emphasized in the reviewed corpus, designing secure yet lightweight authentication and key-establishment mechanisms within these constraints remains a central challenge for IoV deployments [4, 5].

This review synthesizes the recent research works proposing authentication and key-establishment schemes for IoV. The objective is to provide a cohesive analysis that compares designs, identifies practical constraints, highlights empirical evaluation gaps, and lays out a research agenda that prioritizes deplorability.

## 1.1 Methodology and corpus selection

The selection criteria for the corpus were:

- Recent publications of last five years.
- Explicit proposal of an authentication and/or key-establishment protocol targeted at IoV or vehicular networks.
- Availability of technical details including protocol flows and sufficient analysis to extract claimed computational or communication costs and security properties.
- Representation across the major recent directions: hardware-rooted PUFs, blockchain-assisted ledger designs, anonymous conditional-privacy schemes, edge/UAV-assisted handover protocols, and group/handover optimizations.

The review works include PUF-based identity and multi-factor protocols, blockchain batch-authentication and hybrid ledger handover approaches, anonymous and conditional-privacy schemes, chaotic-map-based edge-assisted seamless handover protocols, and UAV-assisted authentication frameworks.

For each paper, we extracted the primitives used, the vehicle-side computational burden, communication overhead, claimed security properties, the type of formal analysis employed (if any), and the evaluation platform, simulator or testbed, or noted absence thereof. These extractions feed the comparative table and the cross-cutting analysis.

## 2. LITERATURE REVIEW

Authentication protocols are fundamental to securing the Internet of Things (IoT), ensuring that only authorized entities can access data and services in highly diverse and resource-constrained environments [8, 9, 10]. Recent research strongly emphasizes lightweight, scalable, and

robust authentication protocols that balance strong security guarantees with limited computational, memory, and energy resources typical of IoT devices.

The following section provides a literature review of recent research articles focusing on authentication protocols in the Internet of Vehicles (IoV), highlighting novel approaches such as PUF-based authentication, zero-knowledge- proof-enabled protocols, blockchain-oriented schemes, and adaptive lightweight mechanisms [6, 11]

The Internet of Vehicles (IoV) represents a critical paradigm in the evolution of intelligent transportation systems, integrating vehicles with ubiquitous communication infrastructure to support safety, traffic efficiency, and autonomous driving [12, 13]. Given the highly dynamic and open nature of IoV, secure and efficient authentication protocols are essential to ensure that only legitimate entities participate in vehicular communication, preventing impersonation, forgery, and unauthorized access [14, 6]. This review summarizes recent advancements in IoV authentication protocols published between 2023 and 2025, emphasizing innovations and emerging trends [4, 15].

Due to real-time constraints and the limited resources of vehicular devices, lightweight authentication schemes have gained prominence. Protocols employing XOR operations, hash-based constructions, and elliptic-curve cryptography (ECC) aim to reduce computational overhead while supporting mutual authentication between vehicles and roadside infrastructure [16, 17, 18]. These designs ensure resistance to replay, impersonation, and man-in-the-middle attacks, aligning with IoV's performance and scalability requirements.

To strengthen security beyond single-factor authentication, multi-factor mechanisms combining biometrics and Physical Unclonable Functions (PUFs) have been proposed [5, 19]. Some schemes introduce dual-layer verification using biometrics and cryptographic primitives such as homomorphic or fuzzy hash functions, safeguarding credentials against insider threats while maintaining anonymity through dynamic identity updates [20, 21].

Physical Unclonable Functions (PUFs) have emerged as strong hardware security primitives due to their inherent resistance to cloning and tampering [22, 23]. Recent IoV authentication protocols incorporate advanced PUF variants such as CUBE-PUFs to enable anonymous mutual authentication with high device uniqueness and secure session key establishment [4, 24].

UAV-assisted and edge-enabled authentication frameworks have also emerged. UAVs extend authentication coverage in

Infrastructure-limited areas, while edge servers perform real-time anomaly detection and behavioural analytics to

**Table -1:** Summary of Authentication Protocols for Internet of Vehicles

Protocol Type	Key Techniques	Security Features	Benefits
Lightweight Mutual Authentication	XOR, Hash Functions, Elliptic Curve Cryptography (ECC)	Mutual authentication, replay and impersonation resistance	Low computation and communication overhead, scalable
Two-Factor & Multi-Factor Authentication	Passwords, Biometrics, Homomorphic Hash, PUFs	Insider threat protection, privacy preservation	Strong authentication, anonymity, credential protection
PUF-Based Anonymous Mutual Authentication	CUBE-PUF, Hardware-rooted identity	Anti-cloning, tamper resistance, privacy preservation	Unique device identity, secure session key establishment
Zero-Knowledge Proof + ECC Authentication	Zero-Knowledge Proof (ZKP), ECC	Anonymous, unlinkable authentication	Privacy enhancement, lightweight, reduced overhead
Blockchain-Based Authentication Scheme	Blockchain, Distributed Ledger, ECC	Tamper-resistance, decentralized trust	Eliminates central points of failure, scalable
Group & Privacy-Preserving Authentication	Dynamic IDs, Batch Verification, Unlinkability	Privacy, group authentication	Scalable to dense vehicular networks, low latency
UAV and Edge-Assisted Authentication	UAV Coverage, Edge Deep Learning	Anomaly detection, behavioral biometric verification	Extended coverage, real-time intelligent security
Lightweight RFID-Based Authentication	ECC, Hash Functions, RFID Tags	Fast and secure vehicle identification	Low energy consumption, suitable for pervasive scenarios
Hybrid Post-Quantum Framework	Kyber-512, ASCON Lightweight Cipher	Post-quantum secure, lightweight	Future-proof security, optimized encryption performance
Adaptive Lightweight IoV Authentication	ECC, Hashing, Lightweight Cryptography	Adaptiveness, secure vehicle-to-infrastructure authentication	Efficient computation and communication

strengthen security [1]. These adaptive systems improve responsiveness and robustness in complex IoV scenarios.

Given the increasing deployment of RFID for vehicular identification and access control, lightweight RFID-enabled authentication schemes using ECC and hash functions have been proposed [35, 21]. These protocols aim to minimize

energy consumption while maintaining strong security, supporting widespread, rapid authentication in traffic management applications.

### 3. TAXONOMY AND TECHNICAL SUMMARIES

#### 3.1 Hardware-rooted PUF-based schemes

Physical Unclonable Functions (PUFs) use inherent, in response to quantum-computing threats, hybrid authentication frameworks combining post-quantum cryptographic algorithms such as Kyber-512 with lightweight symmetric primitives have been introduced [25]. Zero-knowledge proof (ZKP) techniques further enable anonymous legitimacy verification without disclosing secret information, improving privacy while reducing communication overhead [26, 27].

Blockchain-based mechanisms provide tamper-resistant, decentralized authentication frameworks for IoV. By maintaining immutable ledgers for authentication events, blockchain eliminates single points of failure and enhances trustworthiness across vehicular networks [28, 29, 30]. Blockchain-ECC hybrids support scalable and resilient authentication suitable for large-scale dynamic vehicular systems [31, 32].

To meet scalability requirements in dense traffic environments, group-based authentication protocols have been developed. These methods use batch verification, dynamic pseudonym updates, and unlinkability mechanisms to authenticate multiple vehicles simultaneously with reduced latency [33, 15, and 34].

Unpredictable manufacturing variations to provide device-unique responses to challenges. PUFs provide device-unique identifiers [4, 19, and 22]. Practical challenges, including environmental instability, have been noted [23]. PUF-based IoV proposals bind identity or cryptographic material to silicon fingerprints so that keys need not be stored persistently in OBUs. Typical flows include: challenge-response enrolment, PUF response mixing with nonces and hashes, symmetric key derivation functions, mutual authentication with RSUs or trusted authorities (TAs), and derivation of session keys. Advantages are low computational load on OBUs and strong anti-cloning guarantees. Practical challenges include secure enrolment provisioning, environmental sensitivity (temperature and aging effects on PUF response stability), and retrofit costs for legacy fleets.

#### 3.2 Blockchain-enabled and batch authentication

Blockchain-based designs decentralize credential and revocation management, offering tamper-evident audit trails. Blockchain decentralizes credential management [28,

30, 31]. Efficient revocation is supported by accumulator-based constructions [32, 33]. Given the latency sensitivity of safety messages, practical blockchain approaches in IoV use permissioned ledgers combined with off-chain verification or RSU caches to reduce on-chain latency. Batch authentication techniques (aggregate signatures, group MACs, batch verification) are used to handle high message volumes. Decentralization improves resilience to single-point trust failures but requires careful hybridization to maintain acceptable end-to-end latencies. Privacy and linkability concerns are addressed in some works by integrating pseudonymous credentials or group/ring signatures.

#### 3.3 Anonymous and conditional-privacy protocols

Lightweight anonymity and conditional traceability are explored in [15, 36, 34]. Many applications require unlinkability of sessions to protect driver privacy but also demand conditional accountability to deanonymize misbehaving nodes when legally required. Lightweight anonymous schemes use hash-based constructions, one-time pseudonyms, or short-lived credentials to avoid heavy asymmetric operations on OBUs. Conditional-traceability typically involves a trusted tracing authority that can revoke anonymity under defined procedures. Two-factor variants (for example, combining a PUF-derived secret with a password or biometric) increase assurance but require secure secret storage and recovery mechanisms on vehicles.

#### 3.4 Edge-assisted seamless and chaotic-map handover authentication

Edge-offloaded authentication reduces OBU computation [2, 3]. Chaotic-map approaches improve repeated handover efficiency [37]. High mobility induces frequent handovers between RSUs and edge nodes, posing availability risks if re-authentication is slow. Edge-assisted approaches offload heavy computations to proximal edge servers and use specialized primitives—such as chaotic-map-based constructs that claim computational advantages over ECC for repeated handovers—to minimize interruption. These schemes improve continuity but shift trust assumptions toward edge infrastructure and necessitate secure bootstrapping and attestation mechanisms for edge nodes.

#### 3.5 UAV-assisted and distributed reputation designs

UAV-based authentication frameworks enhance coverage in sparse regions [1, 38, 39]. Physical-layer risks remain a concern. UAVs can serve as temporary RSUs, aggregators, or relays in sparse or emergency scenarios, enabling authentication and message verification where terrestrial infrastructure is absent. UAV-assisted designs often use ECC for secure UAV-vehicle channels combined with distributed

reputation or aggregation mechanisms to strengthen misbehavior detection. Physical security risks for UAVs (hijacking, spoofing) and energy/endurance constraints are crucial deployment considerations.

#### 4. KEY-ESTABLISHMENT MECHANISMS

Key establishment mechanisms include symmetric derivation [4, 5], elliptic-curve methods [24, 14], and hybrid ledger-based exchanges [28, 40]. Key establishment across reviewed works falls into a few categories:

**Symmetric key derivation:** Using shared secrets, PUF outputs, or pre-shared material combined with nonces and hash-based KDFs to derive session keys. Preferred for low computational overhead and quick key agreement.

**Elliptic-curve Diffie-Hellman and ECC variants:** Employed when forward secrecy is required. ECC operations are often performed at infrastructure elements (RSUs, edge servers, UAVs) to minimize OBU load.

**Hybrid ledger-assisted key confirmation:** Permissioned ledgers record credentials and revocations, while key confirmation and ephemeral key exchanges occur off-chain to meet latency constraints

#### 5. COMPARATIVE ANALYSIS

The papers are been summarized using a concise technical comparison: primitives, vehicle-side compute, communication overhead, claimed security properties, formal proof methods, and evaluators (simulators/testbeds). Authors who prioritize low-latency vehicle-side processing consistently favor symmetric primitives, hashes, XORs, or PUF reads; asymmetric operations are pushed to infrastructure. Blockchain designs focus on hybrid on-chain/off-chain architectures to balance decentralization and latency. Edge and UAV assistance are effective for continuity but require trustworthy attestation.

Across the corpus, formal analyses include BAN logic, ROR-style arguments, AVISPA symbolic checks, and, in some hardware-rooted proposals, information-theoretic arguments. Evaluation methods mix analytical cost estimation, small/medium-scale simulations, and, rarely, testbed experiments

#### 6. EVALUATION PRACTICE TRENDS AND GAPS

Several recurring evaluation practices and shortcomings were identified:

1. Many works include formal proofs or symbolic checks but vary in adversary assumptions. This inconsistency complicates direct security comparisons.

2. Simulation-based performance claims are common but often limited to small/medium network sizes. City-scale, rush-hour message bursts—critical for realistic stress testing—are seldom emulated.
3. Few papers utilize physical testbeds to validate packet loss, processing delays, and handover latencies observed in real wireless environments; UAV-assisted designs are often simulation-only.

#### 7. CROSS-CUTTING OBSERVATIONS AND TRADE-OFFS

Key trends include, which are essential sections to along with the improvement of a security mechanism:

- **Security–Mobility Synchronization Trade-Off:** Faster mobility requires shorter authentication windows, which reduces cryptographic entropy unless compensated with stronger primitives.
- **Sustainability and Energy Constraints:** Emerging research addresses energy-efficient authentication, especially for UAV-based components, but most schemes still ignore thermal and power limitations in OBUs.
- **Vehicle-side light-weighting:** To satisfy latency constraints, OBUs avoid heavy asymmetric cryptography; trust and heavier operations are delegated to RSUs, edge, or UAVs.
- **Decentralization vs. latency:** Permissioned blockchains add auditability at the cost of potential latency and storage overhead; hybrid off-chain techniques mitigate this tension.
- **Trust-shifting:** Offloading to edge/UAVs reduces OBU load but requires remote attestation and robust trust bootstrapping.
- **PUF practicality:** PUFs provide unclonable identity but require dependable enrollment and handling of environmental variability.

#### 8. OPEN CHALLENGES

Despite significant progress, IoV authentication protocols face enduring challenges such as balancing security with latency and resource constraints, preserving vehicle privacy amid growing data exchange, and accommodating the heterogeneity and scalability of vehicular networks. The convergence of hardware-rooted security, privacy-enhancing cryptographic techniques, decentralized trust architectures, and intelligent, edge-assisted solutions represents the promising frontier for IoV authentication research.

This review synthesizes insights from recent research contributions to delineate the state-of-the-art in IoV authentication protocols. The trends suggest a move toward multi-faceted security approaches combining lightweight. Cryptography, hardware-assisted mechanisms, privacy

preservation, and de-centralized frameworks to meet the complex demands of modern vehicular networks. Continued innovation along these lines is vital to realize secure, scalable, and trustworthy IoV ecosystems.

Many proposing authentications protocol for the Internet of Vehicles (IoV) using Zero-Knowledge Proof (ZKP) and Elliptic Curve Cryptography (ECC) demonstrates an efficient, anonymous, and unlinkable authentication scheme. However, a key limitation identified in this and similar works is the dependency on relatively bulky cryptographic operations even though ECC is lightweight compared to classical cryptography. This makes them still somewhat heavy for very resource-constrained vehicular devices or scenarios involving frequent authentication, such as highly dynamic IoV networks. The computational overhead and communication delay could potentially impact real-time safety-critical applications where latency is crucial.

Additionally, the paper relies on a static network model and does not address authentication scalability in large-scale, multi-domain IoV environments with frequent vehicle mobility and handovers. Privacy preservation is focused on unlinkability and anonymity but does not extend to comprehensive location privacy or protection against advanced tracking attacks over time. Furthermore, dynamic trust management and adaptive authentication based on varying network conditions and vehicle behaviors are not sufficiently studied.

#### These limitations open avenues for new proposals involving:

- Development of ultra-lightweight authentication protocols leveraging physical-layer security, PUFs, or lightweight symmetric key primitives combined with post-quantum tools, optimized specifically for resource-constrained IoV devices.
- Design of scalable and cross-domain authentication frameworks supporting seamless mobility and handoffs, possibly employing blockchain or distributed ledger technologies for decentralized trust management.
- Enhanced privacy-preserving schemes integrating location obfuscation, dynamic pseudonym management, and resistance against correlation and long-term observation attacks.
- Adaptive authentication mechanisms using machine learning at the edge to dynamically adjust protocol parameters based on trust levels, network congestion, and detected anomalies, ensuring timely and secure communication.
- Focusing on these aspects can address current protocol shortcomings and significantly improve security, efficiency, scalability, and privacy in IoV authentication systems.

#### Primary challenges to real-world applicability are:

1. City-scale scalability: Proofs and simulations need to incorporate realistic urban traffic traces and congestion-based radio contention to evaluate authentication throughput and handover churn.
2. Standardization of adversary models: The community requires a shared set of adversary capabilities (partial compromise, RSU capture, side-channel linkability) for comparable formal analysis.
3. Transitional interoperability: Practical migration strategies to incorporate PUF-enabled vehicles alongside legacy OBUs are underdeveloped.
4. Secure offload attestation: Lightweight, low-latency remote attestation schemes for edge nodes and UAVs are essential to safely delegate authentication tasks.
5. Privacy-preserving revocation: Efficient revocation approaches (accumulators, short-lived pseudonyms, ledger-aided schemes) must preserve unlinkability while ensuring fast checks

#### 9. CONCRETE RESEARCH AGENDA

The following immediate research direction has been proposed:

1. An IoV Benchmark Suite and Testbed: Define traffic traces, mobility models, adversary behaviors, and metrics (authentication latency, verification throughput, false positive/negative rates for misbehavior detection). Implement at least one federated, city-scale emulation/testbed.
2. Hybrid PUF-Legacy Bootstrapping Protocols: Design enrollment and token-based transitional mechanisms permitting gradual deployment of PUF-enabled identity without wholesale OBU replacement.
3. Lightweight Remote Attestation: Develop attestation protocols suitable for edge servers and UAVs integrated into handover flows, prioritizing low latency.
4. City-Scale Empirical Evaluations: Apply the benchmark suite to measure ledger/handover/authentication performance under realistic load and mobility.
5. Privacy-First Revocation Mechanisms: Study accumulators and verifiable revocation lists cached at RSUs to minimize on-path latency while preserving anonymity

#### 10. CONCLUSIONS

This review synthesized recent advancements in authentication and key-establishment protocols for the Internet of Vehicles (IoV), focusing on PUF-based hardware security, blockchain-assisted mechanisms, anonymous and conditional-privacy schemes, edge-enabled seamless authentication, and UAV-supported architectures. These approaches collectively demonstrate meaningful progress

toward meeting IoV requirements for low latency, high mobility, and privacy preservation.

However, the analysis indicates that several critical challenges remain unresolved. Many proposals rely on simplified adversary assumptions, limited-scale simulations, or infrastructure models that do not reflect the complexity of real deployment environments. Key issues, including city-scale scalability, secure offloading and remote attestation, interoperability with legacy vehicles, and privacy-preserving revocation, are still inadequately addressed.

Future research should prioritize standardized adversary models, realistic large-scale benchmarks, and testbeds that capture congestion, mobility dynamics, and cross-domain operations. Advancing lightweight attestation mechanisms and transitional deployment strategies will also be essential. Addressing these gaps will help translate promising designs into secure and deployable IoV authentication frameworks capable of supporting next-generation intelligent transportation systems

## REFERENCES

- [1] M. Y. Ararat, S. Moh, Secure UAV relay framework for sparse vehicular networks, *IEEE Internet of Things Magazine* (2021).
- [2] A. Banerjee, S. Roy, Edge-assisted continuous authentication for vehicular networks, *IEEE Transactions on Mobile Computing* (2024).
- [3] L. Guo, D. He, Fog-enabled v2i key agreement with reduced handover delay, *IEEE Access* (2022).
- [4] H. Men, A PUF-based lightweight identity authentication protocol for internet of vehicles, *Computers Electrical Engineering* (2025).
- [5] M. Yuan, Y. Xiao, PMAKA-IOV: A PUF-based multi-factor authentication and key agreement protocol for internet of vehicles, *Information* (2025).
- [6] P. K. S. et al., A comprehensive survey on authentication in v2x and iov systems, *IEEE Communications Surveys & Tutorials* (2023).
- [7] X. Li, L. Chen, Survey on blockchain-enabled IoV authentication, *Vehicular Communications* (2022).
- [8] S. Sicari, A. Rizzardi, L. Griepentrog, C. Cappelletto, B. Carminati, Security, privacy and trust in internet of things: The road ahead, *Computer Networks* (2015).
- [9] F. Alaba, et al., Internet of things security: A survey, *Journal of Network and Computer Applications* (2017).
- [10] Y. Zhang, et al., A survey on IoT authentication protocols: Challenges and future directions, *IEEE Communications Surveys & Tutorials* (2022).
- [11] X. Li, L. Chen, Survey on blockchain-enabled iov authentication, *Vehicular Communications* (2022).
- [12] R. Hussain, et al., Security and privacy in vehicular ad hoc networks: Challenges and solutions, *IEEE Communications Surveys & Tutorials* (2018).
- [13] N. Lu, et al., Connected vehicles: Solutions and challenges, *IEEE Internet of Things Journal* (2020).
- [14] R. Hussain, G. Kim, Efficient certificate-less key agreement for v2v and v2i, *IEEE Transactions on Dependable and Secure Computing* (2021).
- [15] C. K. et al., An anonymous and efficient authentication scheme with conditional privacy preservation in IoV, *Mathematics* (2024).
- [16] M. Wazid, et al., Secure lightweight authentication in IoV, *IEEE Transactions on Vehicular Technology* (2019).
- [17] B. Alzahrani, A lightweight ECC-based mutual authentication protocol for IoV, *Wireless Communications and Mobile Computing* (2021).
- [18] R. Amin, et al., Lightweight mutual authentication protocol for IoV, *Future Internet* (2022).
- [19] M. A. et al., A distributed lightweight puf-based mutual authentication protocol for IoV, *IoT (MDPI)* (2023).
- [20] R. Amin, et al., Multifactor biometric authentication for iot, *Journal of Network and Computer Applications* (2018).
- [21] S. Aghili, et al., A multi-factor lightweight authentication scheme for IoT, *IEEE Internet of Things Journal* (2023).
- [22] C. Li, W. Zhao, Improved fuzzy-extractor-based puf authentication for IoV, *Future Generation Computer Systems* (2024).
- [23] S. Lee, J. Park, Machine-learning-resistant puf constructions for secure v2x, *IEEE Transactions on Information Forensics and Security* (2022).
- [24] X. Li, SSL-PUF based group key agreement for vehicle-road coordination, *Scientific Reports* (2025).
- [25] W. Y. et al., Post-quantum secure authentication for IoV using lattice-based primitives, *IEEE Transactions on Quantum Engineering* (2024).
- [26] R. Zhang, et al., Zero-knowledge proof based lightweight authentication for IoT, *Computers & Security* (2022).
- [27] T. Lin, et al., Blockchain and zkp-based anonymous authentication for IoV, *IEEE Internet of Things Journal* (2023).
- [28] P. B. et al., Blockchain-based batch authentication protocol for internet of vehicles, *Computer Networks* (2021).
- [29] S. Abbas, Blockchain-based authentication in internet of vehicles (survey), *Sensors* (2021).
- [30] Q. Zhang, X. Lin, A hybrid blockchain architecture for scalable v2x authentication, *Computer Communications* (2022).

- [31] J. Huang, F. Zhou, Rsu-assisted blockchain sharding for low-latency IoV authentication, *IEEE Transactions on Vehicular Technology* (2023).
- [32] Y. C. et al., Efficient pseudonym revocation using accumulators in blockchain-enabled IoV, *Ad Hoc Networks* (2024).
- [33] L. Sun, Z. Han, Fast pseudonym revocation using merkle accumulators in vehicular networks, *IEEE Transactions on Intelligent Vehicles* (2023).
- [34] Y. Li, H. Chai, Lightweight privacy-preserving vehicle authentication using hash-based identities, *Security and Communication Networks* (2021).
- [35] M. Ammar, et al., Lightweight authentication for iot: Recent advances and open challenges, *Future Generation Computer Systems* (2022).
- [36] R. Patel, M. Sharma, One-time pseudonym-based privacy-enhanced authentication for v2x, *Wireless Networks* (2023).
- [37] S. S. et al., A seamless authentication scheme for edge-assisted IoV environments using chaotic maps, *Electronics* (2025).
- [38] M. Khalid, S. Ahmed, UAV-assisted secure v2x communication with ECC- based authentication, *Sensors* (2022).
- [39] H. L. et al., Aerial edge computing for trust-aware IoV authentication, *Journal of Network and Computer Applications* (2024).
- [40] S. W. et al., Improved blockchain-based lightweight vehicle-to- infrastructure handover authentication, *Mathematics* (2025)