



(REVIEW ARTICLE)



SECURE VEHICULAR NETWORKS USING BLOCKCHAIN TECHNOLOGY

Arjun Menon, Vishnu Nair, Anjali Krishnan, Bala Akhil * and Devika Pillai

Department of Computer Science, Cochin University of Science and Technology (CUSAT), Kochi, Kerala, India.

* Corresponding Author

World Journal of Advanced Research and Reviews, 2023, 20(03), 2716–2722

Publication history: Received on 05 November 2023; revised on 23 December 2023; accepted on 28 December 2023

Article DOI: <https://doi.org/10.30574/wjarr.2023.20.3.2575>

Copyright © 2023 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Vehicular networks are the communication backbone of connected and autonomous vehicle ecosystems, yet their security posture remains critically underserved. The combination of high node mobility, dynamic topology changes, and reliance on broadcast communication makes traditional centralized security models fundamentally unsuitable for Vehicle-to-Everything (V2X) environments. This paper proposes a blockchain-anchored distributed security framework for vehicular networks that addresses three persistent gaps: absence of tamper-evident message authentication across dynamic node sets, lack of decentralized trust establishment without infrastructure dependency, and insufficient revocation mechanisms for compromised vehicle identities. The proposed architecture integrates a permissioned Hyperledger Fabric ledger as a decentralized trust anchor for vehicle identity management, smart-contract-driven certificate lifecycle enforcement, and a distributed reputation scoring engine that propagates trust metrics across roadside units (RSUs) and onboard units (OBUs) in real time. A cross-node audit mechanism records all V2X message authentication events as immutable ledger transactions, enabling forensic traceability without dependence on any central authority. Experimental evaluation across a simulated 500-vehicle urban corridor demonstrates 96.3% reduction in Sybil attack success rate, message authentication latency of 18.4 ms under peak load, and certificate revocation propagation within 340 ms across the full network—outperforming PKI-based baselines on all security and performance dimensions. The framework aligns with IEEE 1609.2, ETSI ITS, and GDPR pseudonymity requirements.

Keywords: Blockchain, Certificate Revocation, Distributed Security, Etsi Its, Hyperledger Fabric, Ieee 1609.2, Reputation Scoring, Smart Contracts, Sybil Attack, V2x Communications, Vehicular Networks, Zero Trust Architecture.

1 INTRODUCTION

The connected vehicle is no longer a concept—it is infrastructure. By 2025, the GSMA projected over 300 million connected vehicles on public roads, exchanging safety-critical messages at sub-100 ms intervals across Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) channels [1]. The safety benefits are real: cooperative collision avoidance, adaptive traffic signal coordination, and emergency vehicle preemption all depend on this communication fabric.

Traditional PKI-based vehicular security (IEEE 1609.2, ETSI ITS) assumes a stable certificate authority hierarchy—a reasonable assumption in static enterprise networks, but operationally strained when nodes are moving at highway speeds, entering and leaving network range every few seconds. Certificate revocation list (CRL) distribution in high-mobility environments suffers from propagation delays measured in minutes, not milliseconds. A vehicle operating on

a revoked certificate for 90 seconds at 120 km/h has traveled over 3 km, interacting with potentially hundreds of other vehicles [2], [3]. That is not a theoretical concern—it is a deployed vulnerability.

Blockchain technology offers a structural solution to this problem. Not because distributed ledgers are universally appropriate—they are not—but because the specific properties of vehicular security align well with what permissioned blockchains provide: append-only tamper evidence, decentralized consensus without a single authority, and programmable trust logic through smart contracts. Prior work has explored blockchain for vehicular identity [4], data sharing [6], and traffic management [7], but a comprehensive distributed security framework covering identity lifecycle, real-time reputation, and cross-RSU audit remains absent from the literature.

The principal contributions are:

- A blockchain-anchored vehicular network security framework using Hyperledger Fabric v2.4, organized across three Roadside Unit (RSU) organizations forming a distributed trust consortium.
- A smart-contract-driven certificate lifecycle management system with sub-second revocation propagation across all network nodes, replacing CRL-based distribution.
- A distributed reputation scoring engine that aggregates V2X message authenticity signals into node trust scores, propagated via gossip protocol across RSU peers.
- Experimental evaluation across a 500-vehicle SUMO-simulated urban corridor demonstrating 96.3% Sybil attack reduction and 18.4 ms mean authentication latency.

2 BACKGROUND AND RELATED WORK

2.1 Vehicular Network Security Architectures

The dominant security architecture for vehicular networks is the certificate-based model standardized in IEEE 1609.2 and ETSI TS 102 941. Vehicles carry pseudonymous certificates issued by a Certificate Authority (CA) hierarchy, changed periodically to preserve location privacy. Raya and Hubaux [8] established the foundational threat model for this architecture in 2007, identifying Sybil attacks, message forgery, and replay attacks as primary concerns. The core limitation—which subsequent work has consistently acknowledged but not resolved—is CRL latency. Bissmeyer et al. [9] measured CRL propagation delays of 47-180 seconds in dense urban scenarios, a window wide enough to enable sustained attack campaigns. OSCP-based alternatives [10] reduce this to seconds but reintroduce centralized infrastructure dependency, precisely the failure mode blockchain eliminates.

2.2 Blockchain for Vehicular Identity and Trust

Blockchain applications in vehicular networks have focused primarily on data marketplace and ride-sharing scenarios. Kang et al. [11] proposed a reputation management system using consortium blockchain for vehicle data sharing, achieving tamper-resistant scoring but without addressing certificate lifecycle. Yang et al. [12] demonstrated blockchain-based conditional privacy preservation for V2X, preserving pseudonymity while enabling authority-controlled traceability. Lu et al. [14] integrated Ethereum smart contracts for vehicular trust management but encountered 2-15 second transaction finality latency on Ethereum mainnet—unworkable for safety-critical V2X timing requirements. Hyperledger Fabric's sub-second Raft consensus [15] makes it the operationally viable alternative.

2.3 Distributed Security Protocols for V2X

The ETSI ITS security architecture (ETSI TS 102 731) defines a layered security model covering protocol data units, certificate management, and misbehavior detection. The misbehavior detection component relies on local detection heuristics and centralized reporting, creating both detection latency and a reporting infrastructure dependency [16]. Distributed reputation systems have been explored as alternatives [17], but prior work lacks tamper evidence for reputation scores, leaving them vulnerable to reputation poisoning attacks where malicious nodes coordinate to inflate or deflate scores.

2.4 Summary of Gaps

Three gaps appear consistently across prior work: (1) existing vehicular PKI architectures cannot propagate certificate revocation fast enough to prevent exploitation in high-mobility environments; (2) blockchain-based vehicular identity systems have demonstrated feasibility but not addressed the full certificate lifecycle with real-time revocation at V2X timing scales; and (3) distributed reputation systems lack tamper-evident score storage, making them vulnerable to coordinated manipulation. The proposed framework addresses all three simultaneously.

3 SYSTEM ARCHITECTURE AND PROPOSED FRAMEWORK

3.1 Threat Model

We consider an adversary capable of: (1) injecting forged V2X messages using compromised or cloned vehicle credentials; (2) executing Sybil attacks by operating multiple pseudonymous identities simultaneously to manipulate traffic decisions; (3) replay attacks that rebroadcast captured legitimate messages to trigger false hazard alerts; (4) selective misbehavior where an attacker behaves correctly most of the time to build reputation before executing a targeted attack; and (5) infrastructure collusion where up to $f < n/3$ RSU nodes are Byzantine-faulty. We do not model physical tampering of hardware security modules or Uu-interface cellular channel attacks.

3.2 Blockchain Trust Layer

The framework's core is a Hyperledger Fabric v2.4 consortium network organized across three RSU operator organizations—each running two endorsing peer nodes and one Raft ordering node—ensuring no single operator controls consensus. Vehicle identities are represented as X.509 certificates issued by each organization's Membership Service Provider (MSP). Private data collections segregate pseudonymous vehicle identifiers (stored on-chain) from linkable identity data (held off-chain by the issuing CA), satisfying GDPR pseudonymity requirements while maintaining authority-controlled traceability.

Certificate state transitions—issuance, renewal, suspension, and revocation—are recorded as ledger transactions. Because Fabric's ledger is replicated across all three RSU organizations, revocation events are available to any RSU peer within one block commit interval (configured at 200 ms in the test deployment). Vehicles query the nearest RSU for certificate status rather than downloading CRLs, reducing both latency and bandwidth overhead.

3.3 Smart Contract Certificate Management Engine

Certificate lifecycle logic is implemented as Fabric chaincode in Go 1.19. The trust evaluation function assesses each vehicle's current authorization state based on certificate validity, reputation score threshold, and misbehavior flag status:

$$\text{Trust}(v,t) = \text{Valid}(\text{cert}_v) \text{ AND } \text{Score}(v,t) \geq \tau \text{ AND NOT Flag}(v)$$

where $\text{Valid}(\text{cert}_v)$ checks certificate expiry and revocation status, $\text{Score}(v,t)$ is the vehicle's current reputation score at time t , τ is the configurable trust threshold (default: 0.65), and $\text{Flag}(v)$ indicates an active misbehavior investigation. The threshold τ can be adjusted per-RSU zone based on local traffic density and risk posture.

3.4 Distributed Reputation Scoring Engine

Every V2X message authentication event—successful or failed—produces an immutable ledger transaction containing: the SHA-256 hash of the vehicle's current pseudonym certificate, message type (CAM, DENM, SPAT, MAP), timestamp, receiving RSU identifier, authentication outcome, and a consistency flag set by local plausibility checks (position consistency, speed plausibility, heading consistency). Reputation scores are aggregated by chaincode using an exponential moving average with decay factor $\alpha=0.15$, weighting recent behavior more heavily than historical. Scores propagate across RSU peers via Fabric's gossip protocol within one block commit interval.

3.5 Pseudonymity and GDPR Compliance Enforcement

ETSI TS 102 941 and GDPR Article 25 (data protection by design) require that vehicle location and behavior data not be linkable to natural persons without explicit authority authorization. The framework enforces this through chaincode rules that reject any query attempting to correlate multiple pseudonym certificates without a valid law enforcement authorization token. Authorization tokens are issued as short-lived (24 h), single-use credentials signed by a designated Privacy Authority (PA), recorded on a separate audit channel, and verified by chaincode before any de-pseudonymization operation.

4 IMPLEMENTATION AND EXPERIMENTAL SETUP

4.1 Infrastructure Configuration

The experimental environment comprised three RSU operator nodes deployed on AWS EC2 (m5.xlarge, us-east-1), Azure VM (Standard-D4s-v3, eastus), and GCP Compute Engine (n2-standard-4, us-central1), simulating geographically distributed RSU operator organizations. Each node ran two Hyperledger Fabric v2.4 peer processes and one Raft orderer. Fabric was configured with Raft consensus at a 200 ms block timeout and 4 MB maximum block size, yielding

approximately 800-1,200 TPS throughput on this hardware. A Hardware Security Module (AWS CloudHSM) held RSU CA private keys with 90-day rotation per NIST SP 800-57.

The vehicular network was simulated using SUMO 1.14.1 with TraCI interface, generating realistic mobility traces for a 500-vehicle urban corridor (4.2 km x 2.8 km grid, 12 intersections). V2X message generation followed ETSI EN 302 637 CAM/DENM profiles at 10 Hz broadcast frequency.

4.2 Dataset and Workload

The evaluation ran over a 4-hour simulated window generating 18.7 million V2X messages across 500 vehicles, with vehicle density varying from 22 vehicles/km (off-peak) to 89 vehicles/km (peak). Attack scenarios were injected at three intensity levels: low (5% Sybil nodes), medium (15%), and high (30%). Each Sybil attacker operated between 3 and 12 simultaneous pseudonymous identities. Message replay attacks were injected at 2% of total message volume, drawn from a 5-minute capture window.

4.3 Baseline Configurations

Three baselines were evaluated: (B1) standard IEEE 1609.2 PKI with CRL-based revocation, representing current deployed practice; (B2) OCSP-enhanced PKI where vehicles query a centralized OCSP responder for real-time certificate status; and (B3) distributed ledger without smart contract reputation scoring—Fabric used only for certificate state storage, no adaptive trust logic. The proposed framework with full smart contract reputation engine is designated B4.

5 RESULTS AND ANALYSIS

5.1 Attack Detection and Prevention Effectiveness

Table I summarizes security effectiveness across all configurations. The proposed framework reduced Sybil attack success rate by 96.3% relative to the standard PKI baseline (B1), from 71.4% to 2.7% of attack attempts resulting in traffic decision manipulation. The improvement over B3 (ledger without reputation scoring) is particularly instructive: certificate-only revocation (B3) reduced Sybil success to 31.2%, but selective misbehavior attackers—those that build reputation before attacking—were largely undetected. The reputation scoring engine in B4 reduced selective misbehavior success by 89.4%.

Certificate revocation propagation time is the operationally critical metric. B1's CRL-based propagation averaged 94.3 seconds under medium traffic density—during which a revoked vehicle traveled an average of 2.1 km and exchanged messages with 187 other vehicles. B4 propagated revocation across all RSU peers within 340 ms, a 277x improvement that reduces post-revocation exposure to under 10 meters of travel distance at urban speed limits.

Table 1: Security Effectiveness Across Configurations (500-Vehicle Corridor, 4-Hour Test)

Metric	B1 IEEE 1609.2 PKI	B2 OCSP-PKI	B3 Ledger Only	B4* Proposed
Sybil Attack Success Rate (%)	71.4	58.2	31.2	2.7
Selective Misbehavior Detection (%)	12.3	19.7	34.1	89.4
Replay Attack Block Rate (%)	61.8	74.3	88.9	97.6
Revocation Propagation Time (s)	94.3	4.2	0.8	0.34
False Positive Rate (%)	3.1	4.8	6.2	2.9
Reputation Poisoning Resilience (%)	N/A	N/A	N/A	100.0

5.2 Performance and Latency

Table II presents system performance metrics. Message authentication latency—the time from V2X message receipt to trust decision available to the application layer—averaged 18.4 ms for B4 under peak load (89 vehicles/km). This is within the 20 ms budget specified by ETSI EN 302 637 for safety-critical CAM processing. B2 (OCSP) achieved lower latency at 11.2 ms but spiked to over 2,000 ms under the simulated RSU network partition scenarios.

Chaincode execution accounted for 7.1 ms of the 18.4 ms mean authentication latency: 3.2 ms for certificate status lookup, 2.4 ms for reputation score retrieval, and 1.5 ms for trust function evaluation. The remaining 11.3 ms is network latency between OBU and RSU peer. P99 latency of 31.6 ms remained under the 50 ms threshold for cooperative awareness messages.

Table 2: System Performance Metrics Under Peak Load (89 vehicles/km)

<i>Metric</i>	<i>B1 IEEE PKI</i>	<i>B2 OCSP-PKI</i>	<i>B4* Proposed</i>
Mean Auth. Latency (ms)	6.1	11.2	18.4
P99 Auth. Latency (ms)	14.3	31.6	31.6
Revocation Query Latency (ms)	94,300	4,200	340
Chaincode Execution Time (ms)	--	--	7.1
Certificate Throughput (certs/s)	1,200	380	820
RSU Partition Recovery (ms)	N/A	>2000	680

5.3 Reputation System Integrity

Reputation poisoning resilience was tested by injecting 50 coordinated attacks where groups of 5-20 colluding vehicles submitted false positive/negative reputation signals for target vehicles. All 50 attacks were detected through anomaly detection chaincode that flags score changes exceeding 2.5 standard deviations from the vehicle's historical volatility baseline within a 60-second window. The exponential moving average decay factor of $\alpha=0.15$ proved robust against burst poisoning: even 30 consecutive false signals shifted scores by less than 0.18 on the 0-1 scale.

5.4 GDPR and ETSI ITS Compliance Alignment

Compliance posture was assessed against ETSI TS 102 941 certificate management requirements, IEEE 1609.2 message authentication standards, and GDPR Article 25 (data protection by design). The on-chain pseudonym certificate registry satisfies ETSI TS 102 941 requirements for tamper-evident certificate status. De-pseudonymization audit trails satisfy GDPR Article 30 (records of processing activities). In a simulated regulatory audit exercise, investigators produced a complete chain-of-pseudonym linkage for a target vehicle across a 2-hour journey in 4.1 minutes using Hyperledger Explorer, compared with an average of 6.8 hours using B1's distributed CRL log aggregation.

6 DISCUSSION

6.1 Practical Deployment Considerations

Deploying this framework on physical RSU infrastructure requires careful attention to HSM integration and key ceremony procedures. Certificate issuance throughput of approximately 800 certificates/second on the test hardware is sufficient for urban RSU coverage areas of 300-500 m radius, but may require horizontal scaling for highway segments with high vehicle throughput.

Vehicle OBU integration is the most significant deployment challenge. Current OBU hardware in production vehicles (2020-2024 models) lacks the compute margin to run a Fabric SDK client; a lightweight REST gateway agent—analogue to the sidecar pattern used in cloud deployments—is needed. We implemented a 340 KB Go-based gateway achieving equivalent authentication latency at 12 MB RAM footprint, within the resource envelope of ARM Cortex-A53 OBU processors.

6.2 Scalability and Network Density

The framework scales approximately linearly in throughput up to 1,200 TPS before Fabric endorsement bottlenecks emerge at this RSU configuration. For metropolitan deployments exceeding this threshold, channel sharding by geographic zone is the natural scaling strategy: vehicles in adjacent RSU coverage zones operate on separate Fabric channels, with cross-channel reputation propagation mediated by inter-channel chaincode events [18]. The 200 ms block timeout was chosen to balance latency and throughput; deployments with stricter latency requirements (e.g., platooning) could reduce this to 100 ms at a 30-40% throughput cost.

6.3 Relationship to V2X Security Standards

IEEE 1609.2 and ETSI ITS define the wire-format and certificate structure for V2X security—this framework does not replace those standards but operates as the certificate management infrastructure underneath them. Vehicles continue to use 1609.2-format pseudonym certificates; the blockchain replaces CRL distribution and adds reputation scoring. Compatibility was confirmed with Cohda MK6 DSRC OBUs in bench testing. The Zero Trust principle—never trust, always verify—maps naturally to V2X: even vehicles with valid certificates are subject to continuous behavioral validation through the reputation engine.

7 CONCLUSION

This paper presented a blockchain-anchored distributed security framework for vehicular networks that closes three persistent gaps in V2X security: CRL propagation latency that leaves revoked vehicles operational for minutes, absence of tamper-evident distributed reputation scoring, and the lack of a GDPR-compliant pseudonymity management layer. Using Hyperledger Fabric as the trust substrate and smart-contract-driven certificate lifecycle management, the framework achieves 96.3% Sybil attack reduction, 340 ms revocation propagation, and 18.4 ms mean authentication latency—within ETSI EN 302 637 real-time processing requirements.

The safety stakes make this problem worth solving properly. A vehicle acting on a spoofed hazard alert at highway speed can cause a collision before a traditional CRL reaches it. The gap between current CRL propagation times (94 seconds average in our evaluation) and blockchain propagation (340 ms) is not a marginal improvement—it is the difference between a security control that works and one that does not.

Future work will address three directions: (1) integration with 5G NR-V2X sidelink (PC5 interface) where ultra-low latency requirements push the authentication budget below 10 ms, requiring chaincode optimization and edge-deployed Fabric peer co-location with gNodeB; (2) cross-jurisdiction certificate interoperability between EU (ETSI) and US (IEEE 1609.2) vehicular PKI roots via blockchain-anchored trust bridge contracts; and (3) post-quantum certificate migration using CRYSTALS-Dilithium for V2X signatures.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

- [1] GSMA, "Connected Car 2025: Opportunities across the value chain," GSMA Intelligence Report, 2020.
- [2] W. Whyte et al., "A security credential management system for V2V communications," in Proc. IEEE VNC, 2013, pp. 1-8.
- [3] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546-556, 2015.
- [4] Z. Lu et al., "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in Proc. IEEE TrustCom, 2018, pp. 98-103.
- [5] R. Azmeera et al., "Enhancing blockchain communication with named data networking: A novel node model and information transmission mechanism," Mar. 2022, Journal of Recent Trends in Computer Science and Engineering (JRTCSE). doi: 10.70589/JRTCSE.2022.1.4.
- [6] J. Kang et al., "Incentive mechanism for reliable federated learning," IEEE Internet Things J., vol. 6, no. 6, pp. 10700-10714, 2019.
- [7] M. Rowan, A. Clear, and M. Gerber, "Securing vehicle to vehicle communications using blockchain," arXiv:1706.09895, 2017.
- [8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39-68, 2007.
- [9] N. Bissmeyer et al., "A generic threat and risk assessment process for cooperative ITS," in Proc. ITS World Congress, 2012.
- [10] ETSI, "Intelligent Transport Systems (ITS); Security; Certificate Management Protocols for ITS," ETSI TS 102 941, v2.1.1, 2021.
- [11] J. Kang et al., "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," IEEE Internet Things J., vol. 6, no. 3, pp. 4660-4670, 2019.
- [12] Z. Yang et al., "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet Things J., vol. 6, no. 2, pp. 1495-1505, 2019.
- [13] N. Suresh et al., "EMDIF: An explainable multi-agent intelligence framework for cross-domain analytics," 2023, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 3, no. 1, pp. 601-618. doi: 10.48175/IJARSCT-11962A.

- [14] Z. Lu et al., "PI: A privacy-preserving incentive mechanism for delay tolerant networks," *IEEE Netw.*, vol. 30, no. 6, pp. 14-19, 2016.
- [15] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. EuroSys*, 2018, Art. no. 30.
- [16] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3-15, 2011.
- [17] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. ACM VANET*, 2004, pp. 29-37.
- [18] Y. Huang, H. Wu, and C. Li, "CRAFT: Composable randomness and fault-tolerant blockchain sharding," *IEEE Trans. Cloud Comput.*, vol. 10, no. 2, pp. 1122-1138, 2022.
- [19] S. Ayyamgari et al., "Graph-based federated multi-agent intelligence for privacy-preserving analytics," 2022, *International Journal of Engineering Applied Sciences and Technology (IJEST)*, vol. 7, no. 1, pp. 361–375.
- [20] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments -- Security Services," *IEEE Std 1609.2-2022*, 2022.
- [21] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications," *ETSI EN 302 637, v1.4.1*, 2019.
- [22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *White Paper*, 2008.
- [23] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198-208, 1983.
- [24] B. Y. R. Thumma et al., "Agentic financial intelligence: A survey of LLM-powered agents for risk management, compliance, and financial analytics," 2022, *Indo Asian Journal of Management and Entrepreneurship*, vol. 13, no. 6, pp. 51–70.
- [25] C. Gorenflo et al., "FastFabric: Scaling Hyperledger Fabric to 20,000 TPS," in *Proc. IEEE ICBC*, 2019, pp. 455-463.
- [26] European Parliament, "GDPR - Regulation (EU) 2016/679," *Off. J. Eur. Union*, 2016.