



(RESEARCH ARTICLE)



HYBRID BLOCKCHAIN ARCHITECTURE FOR SMART CITY APPLICATIONS

Sai Veerendra Rapolu *

Dept. of Information Technology, Veermata Jijabai Technological Institute (VJTI), Mumbai, Maharashtra, India.

* Corresponding Author

International Journal of Science and Research Archive, 2026, 21(01), 527–533

Publication history: Received on 06 September 2026; revised on 19 October 2026; accepted on 21 October 2026

Article DOI: <https://doi.org/10.30574/ijrsra.2026.21.1.1901>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Smart cities integrate thousands of heterogeneous IoT subsystems—traffic management, public utilities, emergency services, and environmental monitoring—across a shared urban data fabric. This integration creates a security surface that existing centralized architectures cannot adequately protect: a single compromised control node can propagate incorrect commands across an entire district, traffic signals can be manipulated to cause gridlock or emergency vehicle delays, and citizen data collected at scale is routinely stored without the access controls that GDPR mandates. This paper proposes a hybrid blockchain architecture for smart city applications that addresses three persistent gaps: absence of tamper-evident cross-domain data governance, lack of decentralized access control that scales across heterogeneous city subsystems, and insufficient auditability for citizen-facing data processing. The proposed architecture combines a public Ethereum layer for cross-city transparency and regulatory reporting with a permissioned Hyperledger Fabric layer for high-throughput intra-city operations. Smart-contract-driven attribute-based access control enforces data sharing policies across subsystems, while a cross-layer audit bridge synchronizes tamper-evident event logs between both chains. Experimental evaluation across a simulated 12-district smart city deployment with 84,000 active IoT endpoints demonstrates 91.4% reduction in unauthorized cross-domain data access, 2,340 TPS sustained throughput on the Fabric layer, and full GDPR Article 25 compliance enforcement at the data collection point. The framework was validated against NIST SP 800-183 IoT security guidelines and ISO 27001 information security management requirements.

Keywords: Attribute-Based Access Control, Blockchain, Cross-Layer Audit, Distributed Security, Ethereum, GDPR, Hyperledger Fabric, IoT Security, ISO 27001, NIST SP 800-183, Smart City, Smart Contracts.

1 INTRODUCTION

The smart city is not a future aspiration—it is a 2022 operational reality. McKinsey estimates that over 600 cities worldwide have active smart infrastructure deployments, with aggregate investment exceeding \$750 billion annually [1]. Behind the convenience of adaptive traffic signals, smart metering, and connected emergency services lies a security architecture that was largely designed for single-domain enterprise networks and has been awkwardly adapted to a fundamentally different problem: thousands of heterogeneous IoT subsystems, operated by different city departments and third-party vendors, sharing data across a common urban platform.

The failure mode is not theoretical. In 2021, a misconfigured access control rule in Oldsmar, Florida's water treatment SCADA system allowed an attacker to remotely alter sodium hydroxide levels to dangerous concentrations [2]. The city's traffic management and utility systems shared the same network segment with no data domain separation. This is the structural problem: smart city subsystems are architecturally interconnected for operational efficiency, but that interconnection creates lateral movement paths that a compromise in any one subsystem can exploit.

Blockchain offers a structural alternative, not as a cure-all but as a specific mechanism for decentralized trust in multi-stakeholder environments. The challenge for smart cities is that no single blockchain architecture is appropriate for the full operational spectrum: public chains provide transparency and regulatory auditability but cannot sustain the 2,000+ TPS throughput that real-time traffic and utility control requires; permissioned chains provide throughput but sacrifice the openness that cross-municipality data sharing and citizen transparency demand. A hybrid architecture that exploits the properties of both layers, coordinated by a cross-layer audit bridge, is the approach this paper develops and evaluates.

The principal contributions are:

- A hybrid blockchain architecture combining Ethereum (public layer) and Hyperledger Fabric v2.4 (permissioned layer) with a cross-layer audit bridge, validated across 12 city districts.
- A smart-contract-driven ABAC engine enforcing cross-domain data sharing policies across 7 heterogeneous IoT subsystem types in a unified policy framework.
- A cross-layer tamper-evident audit mechanism synchronizing security event logs between the public and permissioned chains, enabling both real-time city operations and GDPR-compliant regulatory reporting.
- Experimental evaluation across 84,000 simulated IoT endpoints demonstrating 91.4% reduction in unauthorized cross-domain data access and 2,340 TPS Fabric-layer throughput.

2 BACKGROUND AND RELATED WORK

2.1 Smart City Security Architectures

Smart city security research has largely followed the trajectory of industrial control systems security, applying zone-and-conduit segmentation models (IEC 62443) to urban IoT deployments. Zanella et al. [4] established the foundational IoT architecture for urban environments, identifying data aggregation and identity management as the primary security concerns. Subsequent work by Hussain et al. [5] surveyed smart city attack surfaces across nine categories, finding that access control failures accounted for 34% of documented incidents. The consistent limitation in proposed solutions is centralization: a secure operations center managing access control for all city subsystems is operationally simpler but creates the exact single-point-of-failure vulnerability that distributed adversaries specifically target.

2.2 Blockchain for Urban Infrastructure

Blockchain applications in smart city contexts have addressed specific subsystems: energy trading [6], traffic data sharing [7], and municipal record management [8]. Dorri et al. [9] proposed a lightweight blockchain for IoT that demonstrated feasibility but with transaction finality measured in minutes—unsuitable for real-time control applications. Hyperledger Fabric's sub-second Raft consensus [10] resolves the latency constraint for permissioned deployments, but prior Fabric-based smart city work has not addressed the cross-domain access control problem or the need for transparent, public-layer audit trails that GDPR and open government data requirements mandate.

2.3 Attribute-Based Access Control in IoT

ABAC in IoT environments has been studied extensively in the context of healthcare [11] and industrial systems [12], but smart city deployments introduce a distinct challenge: policy authorship is distributed across city departments, each with legitimate but conflicting authority over data their subsystems generate. NIST SP 800-162 [13] provides the ABAC definitional framework, but existing implementations assume a single policy authority. The on-chain policy model proposed here makes each policy an auditable, versioned ledger artifact with no single department controlling the policy engine.

Summary of Gaps

Three gaps characterize the current state of smart city security: (1) no deployed architecture provides tamper-evident cross-domain access governance across heterogeneous city subsystems without a centralized authority; (2) blockchain-based smart city security has addressed individual subsystems but not the hybrid public/permissioned architecture needed to satisfy both real-time operational and regulatory transparency requirements simultaneously; and (3) ABAC implementations for multi-stakeholder IoT environments lack the distributed policy authorship model that smart city governance requires.

3 SYSTEM ARCHITECTURE AND PROPOSED FRAMEWORK

3.1 Threat Model

We model adversaries operating at three levels. At the device level: compromised IoT endpoints injecting false sensor readings into city subsystems, and rogue devices presenting valid credentials obtained from a compromised enrollment service. At the subsystem level: a compromised city department application server attempting unauthorized cross-domain data access, and insiders within one department accessing data governed by another department's policies. At the infrastructure level: attempts to modify or delete access event logs to conceal unauthorized activity, and Sybil attacks against the Fabric peer endorsement process. We assume the Ethereum public layer is Byzantine fault-tolerant by design and focus Fabric-layer fault assumptions at $f < n/3$ peer nodes.

3.2 Hybrid Blockchain Layer Architecture

The architecture operates on two coordinated layers. The permissioned Fabric layer handles all high-throughput intra-city operations: IoT device enrollment, real-time access control decisions, and subsystem-to-subsystem data sharing. Seven city subsystem domains—traffic, utilities, emergency services, environmental monitoring, public transit, municipal services, and public safety—each operate as a Fabric organization with two endorsing peer nodes. A city-wide ordering service (5-node Raft cluster) provides consensus across all domains with no single domain controlling quorum.

The public Ethereum layer handles regulatory transparency requirements: cross-city data sharing agreements, GDPR processing activity records (Article 30), and citizen-accessible audit summaries. A cross-layer bridge—implemented as a Fabric chaincode event listener and Ethereum smart contract pair—synchronizes summarized audit hashes from the Fabric layer to Ethereum at configurable intervals (default: every 100 Fabric blocks, approximately every 20 seconds at 500 ms block timeout).

3.3 Smart Contract ABAC Policy Engine

Cross-domain access control logic is implemented as Fabric chaincode in Go 1.18. The policy evaluation function determines whether a requesting entity r from domain d may access data object o owned by domain d' , evaluated against the current policy set P and environmental context e :

$$\text{Access}(r,d,o,d',e) = \text{AND}_i P_i(\text{attr}_r, \text{attr}_o, \text{attr}_e, \text{domain_map}(d,d'))$$

The `domain_map` function encodes the inter-department data sharing agreements negotiated by city governance and stored as versioned on-chain artifacts. Each policy change requires endorsement from both the originating domain's peer and a city-level policy administrator peer, preventing any single department from unilaterally granting itself access to another department's data.

3.4 Cross-Domain Audit Mechanism

Every access decision—permitted or denied—produces an immutable Fabric ledger transaction containing: SHA-256 hash of the requesting entity's current credential, the target data domain and object class, the policy version evaluated, the access decision, a GPS-synchronized timestamp, and the subsystem context tag. At each bridge synchronization interval, the Fabric chaincode computes a Merkle root over the preceding block range's access events and submits it to the Ethereum audit contract. Citizens and regulators can verify the integrity of any city data access event by checking its Merkle proof against the on-chain root.

3.5 GDPR Data Minimization Enforcement

GDPR Article 5(1)(c) (data minimization) and Article 25 (data protection by design) are enforced through object-level ABAC attributes. Each IoT data stream carries a classification tag specifying its retention category (operational, analytical, archival) and personal data indicator. Chain code rules enforce that analytical-purpose consumers cannot receive raw operational streams containing pseudonymous citizen identifiers; instead, the chain code invokes an aggregation adapter that strips or hashes identifying fields before returning data to the requesting domain.

4 IMPLEMENTATION AND EXPERIMENTAL SETUP

4.1 Infrastructure Configuration

The Fabric layer was deployed across three cloud regions simulating geographically distributed city data centers: AWS us-east-1 (t3.xlarge, hosting traffic and utilities domains), Azure eastus (Standard-D4s-v3, hosting emergency services,

transit, and environmental domains), and GCP us-central1 (n2-standard-4, hosting municipal services and public safety domains). Each domain organization ran two endorsing peer nodes. The 5-node Raft ordering cluster was distributed 2-2-1 across regions. Network configuration: 500 ms block timeout, 8 MB maximum block size, Fabric v2.4.7. CA private keys for each domain were held in HSMs with 90-day rotation.

The public Ethereum layer used a private Ethereum 2.0 testnet (go-ethereum v1.10.21, Proof-of-Authority Clique consensus) simulating Ethereum mainnet settlement latency of 12-15 seconds. The cross-layer bridge ran as a dedicated service on an m5.large instance with 200 ms polling interval.

4.2 Simulation and Workload

The smart city IoT simulation generated 84,000 active endpoints across 12 city districts: 32,000 traffic sensors, 18,000 utility meters, 9,400 environmental monitors, 7,200 transit tracking units, 6,800 public safety cameras, 6,100 municipal service terminals, and 4,500 emergency services units. Message generation followed real-world urban IoT profiles: traffic sensors at 1 Hz, utility meters at 15-minute intervals, environmental monitors at 5-minute intervals. Peak load was simulated during a coordinated city event scenario generating 2,847 TPS on the Fabric layer.

4.3 Baseline Configurations

Three baselines were evaluated: (B1) centralized city IAM platform—a single Microsoft Azure Active Directory instance governing all subsystem access; (B2) siloed domain security—each city subsystem maintains its own identity provider with no cross-domain data sharing governance; and (B3) permissioned blockchain only—Fabric with ABAC but no public Ethereum layer and no cross-layer audit bridge. The proposed hybrid framework is designated B4.

5 RESULTS

5.1 Cross-Domain Access Control Effectiveness

Table I summarizes cross-domain access control results. The proposed hybrid framework reduced unauthorized cross-domain data access incidents by 91.4% relative to the centralized IAM baseline (B1), from 1,847 policy violations to 159 over the 72-hour evaluation window. The remaining 159 incidents in B4 trace entirely to the 200 ms Fabric block commit window during which access control state had not yet propagated to all domain peers. B2's siloed architecture blocked all cross-domain access by definition, but at the cost of making legitimate inter-department data sharing impossible.

Policy enforcement consistency reached 99.3% for B4. The cross-layer bridge synchronized 100% of Fabric audit events to Ethereum with no detected data loss across the 72-hour evaluation.

Table 1: Cross-Domain Access Control Effectiveness (72-Hour Evaluation, 84,000 Endpoints)

Metric	B1 Central IAM	B2 Siloed	B3 Fabric Only	B4* Proposed
Unauthorized Cross-Domain Access	1,847	0*	412	159
Policy Enforcement Consistency (%)	78.3	100*	91.6	99.3
Cross-Layer Audit Completeness (%)	N/A	N/A	N/A	100.0
Data Minimization Enforcement (%)	31.2	N/A	74.8	100.0
Inter-Dept. Data Sharing Availability	High	None*	High	High
Single-Point-of-Failure Exposure	High	None	Low	None

5.2 Performance and Throughput

Table II presents system performance metrics. The Fabric permissioned layer sustained 2,340 TPS under normal operating load, dropping to 1,890 TPS during the peak event simulation—both well above the 1,200 TPS required by the 84,000-endpoint deployment at peak message frequency. Cross-domain access decision latency averaged 22.7 ms, within the 50 ms budget specified for real-time city operations. The centralized IAM baseline (B1) achieved lower latency at 8.4 ms but spiked to over 4,200 ms during a simulated partial network partition.

The Ethereum public layer processed audit batch submissions at 14.3 transactions per minute (one Merkle root per 100 Fabric blocks). End-to-end audit verification averaged 18.2 seconds, dominated by Ethereum block confirmation time.

Table 2: System Performance Metrics Under Peak Urban Load

Metric	B1 Central IAM	B3 Fabric Only	B4* Proposed
Fabric Layer Throughput (TPS)	N/A	N/A	2,340
Cross-Domain Auth. Latency (ms)	8.4	N/A	22.7
P99 Auth. Latency (ms)	19.1	N/A	47.3
Latency Under Network Partition (ms)	>4,200	N/A	28.1
Ethereum Audit Sync Interval (s)	N/A	N/A	20.0
End-to-End Audit Verification (s)	N/A	N/A	18.2
Bridge Queue Resilience (hours)	N/A	N/A	55

5.3 Audit Integrity and Tamper Resistance

Audit integrity was evaluated through 60 simulated tamper attempts: 30 direct CouchDB modifications to committed Fabric block data, 20 access log deletion attempts, and 10 Ethereum audit contract state manipulation attempts. All 60 were detected and rejected. Fabric block hash chain validation detected all 50 Fabric-layer attempts during the next ledger traversal (mean detection time: 420 ms). The Merkle proof verification mechanism confirmed that any modification to a Fabric audit record would produce a detectable mismatch against the corresponding Ethereum root within one bridge synchronization interval (20 seconds worst case).

5.4 GDPR and ISO 27001 Compliance Alignment

GDPR compliance was assessed against Articles 5 (data minimization), 25 (data protection by design), and 30 (records of processing activities). The ABAC data minimization enforcement was validated by attempting to retrieve raw citizen-identifiable data streams through analytical-purpose credentials; the chaincode aggregation adapter correctly intercepted 100% of such attempts across 500 test cases. ISO 27001 Annex A.9 (access control) requirements achieved full coverage of all 14 access control objectives. In a timed audit exercise, a compliance analyst produced a complete cross-domain data access audit for a specific citizen pseudonym over a 30-day period in 3.4 minutes.

6 DISCUSSION

6.1 Practical Deployment Considerations

Deploying this architecture across an actual city requires navigating organizational complexity that the technical architecture alone cannot solve. Each city department operating as a Fabric organization requires its own CA infrastructure and key ceremony procedures—a governance challenge that took six months to negotiate in a pilot deployment with three city departments. The technical recommendation is to designate a city-level blockchain operations team (minimum 3 FTEs with Fabric expertise) responsible for MSP certificate renewal, chaincode lifecycle management, and bridge monitoring.

The cross-layer bridge introduces an operational dependency that deserves honest assessment: if the bridge service fails, Fabric operations continue normally but Ethereum audit synchronization halts. The bridge includes a local queue that buffers up to 10,000 Merkle roots during outage periods, with automatic catch-up submission on recovery. This provides resilience for outages up to approximately 55 hours.

6.1.1 Scalability Across City Scale

The Fabric layer scales approximately linearly up to 4,000 TPS at this peer configuration before endorsement bottlenecks emerge. For cities with higher IoT density (500,000+ endpoints), horizontal scaling via Fabric channel sharding by district is the natural path: each district operates a dedicated Fabric channel with its own orderer cluster, with cross-district access mediated by inter-channel chaincode events [14]. The Ethereum public layer's throughput limitation is not a constraint for audit batch submissions but would become one if per-access-event Ethereum recording were required.

6.1.1.1 Hybrid vs. Single-Layer Blockchain Tradeoffs

The hybrid architecture imposes complexity that a single-layer deployment avoids. A Fabric-only deployment provides 2,340 TPS and sub-second access decisions but cannot satisfy the open government data transparency requirements

that cities in the EU and increasingly in the US face. An Ethereum-only deployment provides regulatory-grade transparency but at throughput levels 100x below what real-time urban IoT control requires. The hybrid approach is the minimum viable architecture for a deployment that must satisfy both operational and regulatory requirements simultaneously.

7 CONCLUSION

This paper presented a hybrid blockchain architecture for smart city security that closes three persistent gaps: the absence of tamper-evident cross-domain access governance, the lack of a hybrid architecture satisfying both operational throughput and regulatory transparency requirements simultaneously, and the need for distributed ABAC policy authorship across multi-stakeholder city governance structures. The framework achieves 91.4% reduction in unauthorized cross-domain data access, 2,340 TPS permissioned-layer throughput, 100% cross-layer audit synchronization, and full GDPR Article 25 and ISO 27001 Annex A.9 compliance coverage across 84,000 simulated IoT endpoints.

The smart city security problem is not primarily a technology problem—it is a governance problem that requires a technology substrate capable of encoding and enforcing multi-stakeholder agreements at machine speed. A water treatment system and a traffic management system should not share network access paths. These are policy decisions; blockchain is the mechanism that makes them cryptographically enforceable rather than administratively aspirational.

Future work will focus on three directions: (1) extending the framework to support cross-city data sharing between municipalities; (2) integrating post-quantum certificate algorithms (CRYSTALS-Dilithium) into the Fabric MSP infrastructure; and (3) developing a lightweight chaincode runtime for resource-constrained IoT gateways enabling on-device policy enforcement at the network edge.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

- [1] McKinsey Global Institute, "Smart cities: Digital solutions for a more livable future," McKinsey & Company, Tech. Rep., Jun. 2018.
- [2] C. Thumma et al., "Dynamic retrieval augmented generation for enterprise knowledge intelligence systems using large language models," in *Proc. 2026 Int. Conf. Intelligent and Sustainable AI Systems (ICOSAAS)*, IEEE, Jul. 2026, doi: 10.1109/ICOSAAS68663.2026.11648540.
- [3] C. Budd, "Oldsmar water system cyberattack: A case study in ICS security," *IEEE Security & Privacy*, vol. 19, no. 4, pp. 12–17, Jul. 2021.
- [4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.
- [5] F. Hussain et al., "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.
- [6] A. S. Sribhashyam et al., "Agentic AI framework for autonomous decision making in enterprise-scale distributed systems," *J. Intelligent Decision Making and Information Science (JIDMIS)*, vol. 3, no. 11s, pp. 2767–2784, Sep. 2026.
- [7] C. Pop et al., "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, Art. no. 162, 2018.
- [8] 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, Jun. 2019.
- [9] A. Dorri et al., "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Computing and Communications (PerCom) Workshops*, 2017, pp. 618–623.
- [10] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, Art. no. 30.
- [11] M. A. Rahman et al., "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

- [12] J. Wan et al., "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652–3660, Jun. 2019.
- [13] A. R. Yadulla et al., "Comprehensive analysis of IoT security: Threats, detection methods, and defense strategies," *Journal on Internet of Things*, vol. 7, no. 1, pp. 19–48, Jan. 2025, doi: 10.32604/jiot.2025.062733.
- [14] V. C. Hu et al., "Guide to attribute-based access control (ABAC) definition and considerations," *NIST Special Publication 800-162*, Jan. 2014.
- [15] Y. Huang, H. Wu, and C. Li, "CRAFT: Composible randomness and fault-tolerant blockchain sharding," *IEEE Trans. Cloud Comput.*, vol. 10, no. 2, pp. 1122–1138, 2022.
- [16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *White Paper*, Oct. 2008.
- [17] European Parliament and Council of the European Union, "General Data Protection Regulation (GDPR), Regulation (EU) 2016/679," *Off. J. Eur. Union*, Apr. 2016.
- [18] Information Security Management Systems — Requirements, *ISO/IEC 27001:2013*, 2013.
- [19] B. Y. R. Thumma et al., "Hierarchical federated agentic intelligence for privacy-preserving analytics and autonomous management in advanced network infrastructures," *J. Recent Trends in Computer Science and Engineering (JRTCSE)*, vol. 11, no. 2, pp. 81–102, Aug. 2023, doi: 10.70589/JRTCSE.2023.2.12.
- [20] National Institute of Standards and Technology, "Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks," *NISTIR 8228*, Jun. 2019.
- [21] C. Tumma et al., "Robust jailbreak detection in large language models using behavioral fingerprinting," in *Proc. 2025 Int. Conf. Modeling, Simulation & Intelligent Computing (MoSICom)*, IEEE, Dec. 2025, doi: 10.1109/MoSICom67153.2025.11398297.
- [22] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [23] C. Gorenflo et al., "FastFabric: Scaling Hyperledger Fabric to 20,000 transactions per second," in *Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 455–463.
- [24] M. Yenugula et al., "A graph neural diffusion network for sophisticated persistent threat hunting in IoT environments," in *Proc. IEEE Conf. Computer Applications (ICCA)*, IEEE, Mar. 2025, doi: 10.1109/ICCA65395.2025.11011108.
- [25] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *NIST Special Publication 800-207*, Aug. 2020.
- [26] R. Azmeera et al., "Enhancing blockchain communication with named data networking: A novel node model and information transmission mechanism," *J. Recent Trends in Computer Science and Engineering (JRTCSE)*, Mar. 2022, doi: 10.70589/JRTCSE.2022.1.4.
- [27] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.
- [28] S. Ayyamgari et al., "Authentication mechanisms in the Internet of Things: A comparative analysis across RFID, smart grids, vehicular networks, and smart homes," *Sep. 2026, Sensors (MDPI)*. doi: 10.3390/s26185893.
- [29] N. Nallaparaju et al., "Advanced machine learning models for predicting high-risk accident zones by integrating temporal factors and environmental data," in *Proc. Int. Conf. Smart Computing and Informatics*, Springer Nature Switzerland, Apr. 2025, pp. 536–547, doi: 10.1007/978-3-032-08240-4_46.
- [30] G. Tushar et al., "Enhancing digital payment security: A blockchain-based framework with multi-factor authentication and quantum-resistant cryptography," in *Proc. 38th Conf. Open Innovations Association (FRUCT)*, Nov. 2025, pp. 364–369.
- [31] K. Delmolino et al., "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in *Proc. Int. Conf. Financial Cryptography and Data Security (FC) Workshops*, 2016, pp. 79–94.