Software Engineering and Artificial Intelligence Systems

Volume: 02 Issue: 01 (2026)

www.seais.org/

Uncertainty-Regularized Neural Surrogates for Sparse Governing- Drift-Blockchain-Backed Fifth-Generation Authentication with Trust-Aware Consensus Under Intermittent Edge Connectivity Constraints

Logan Rivera[1]

[1] Department of Advanced Computing, Viterbi School of Engineering, University of Southern California, Los Angeles, California, USA

Keyword: Blockchain Technology, Fifth-Generation Networks, Continuous Authentication, Intermittent Connectivity, Trust-Aware Consensus.

A B S T R A C T

The rapid deployment of fifth-generation telecommunication networks has necessitated decentralized architectures to support massive machine-type communications and ultra-reliable low-latency applications. Mobile edge computing brings processing capabilities closer to the end user, but introduces significant security vulnerabilities, particularly concerning continuous authentication under intermittent network connectivity. Traditional centralized authentication mechanisms suffer from high latency and single points of failure, making them unsuitable for dynamic edge environments where backhaul links to the core network frequently degrade or drop entirely. This paper proposes a novel blockchain-backed authentication framework tailored for fifth-generation edge environments, incorporating a unique trust-aware consensus mechanism designed specifically to operate under intermittent connectivity constraints. By utilizing a localized distributed ledger at the edge, the proposed system enables continuous, decentralized verification of user equipment identities without relying on continuous core network availability. The trust-aware consensus algorithm dynamically adjusts quorum requirements and validator weightings based on node reputation and historical uptime, ensuring that localized network partitions can maintain operational security and seamlessly merge ledgers upon connection restoration. Comprehensive simulated evaluations demonstrate that the proposed architecture significantly reduces authentication latency during backhaul degradation and maintains high throughput and malicious node rejection rates compared to standard practical Byzantine fault tolerance algorithms.

INTRODUCTION

1.1 The Evolution of Mobile Telecommunications

The transition from fourth-generation to fifth-generation telecommunication networks represents a fundamental paradigm shift in how digital infrastructure is conceptualized, deployed, and managed on a global scale. Fifth-generation networks are not merely an incremental upgrade in bandwidth; they are designed to be a unified connectivity fabric that supports a vast array of diverse services, ranging from enhanced mobile broadband to ultra-reliable low-latency communications and massive machine-type communications. Central to this evolution is the integration of mobile edge computing, which decentralizes computational resources and storage, moving them from distant core network data centers to the logical extremes of the network, such as base stations and local aggregation points. This architectural decentralization is intended to drastically reduce end-to-end latency, alleviate backhaul network congestion, and provide highly contextual, location-aware services to end users. However, the proliferation of distributed edge nodes introduces immense complexity in network management and orchestration. Unlike traditional centralized models where a few secure core facilities managed all critical operations, the modern telecommunications landscape involves thousands of geographically dispersed edge servers operating in physically insecure or highly variable environments. This fundamental restructuring necessitates a complete reevaluation of network security protocols, particularly the mechanisms through which devices and users are authenticated and authorized to access network resources. Traditional authentication protocols, which typically rely on a centralized home subscriber server or unified data management function situated deep within the core network, are inherently ill-suited for the stringent latency requirements of fifth-generation applications. When an edge device attempts to connect, routing the authentication request back to the central core introduces unavoidable transmission delays. Yao and colleagues examine secure transmission scheme based on joint radar and communication in mobile vehicular networks [1].

1.2 Security Challenges in Edge Computing

Beyond the latency constraints imposed by centralized authentication architectures, the physical and topological realities of mobile edge computing present profound security and operational challenges. Edge nodes are frequently deployed in remote, harsh, or highly dynamic environments where physical security cannot be guaranteed to the same degree as a traditional data center. Furthermore, these edge deployments often suffer from intermittent connectivity to the core network. Environmental factors, hardware malfunctions, extreme weather events, or intentional electromagnetic interference can cause backhaul links to degrade, fluctuate, or sever completely for unpredictable durations. When an edge node loses its connection to the central unified data management function, traditional authentication mechanisms fail catastrophically. Devices attempting to connect or roam into the affected cell are unable to be verified, leading to total service denial even if the local edge node remains fully operational and capable of providing localized services. To mitigate this critical vulnerability, researchers have increasingly looked toward decentralized trust mechanisms, most notably blockchain technology and distributed ledger systems. By maintaining a synchronized, tamper-evident ledger of authentication credentials and access policies across a distributed network of edge nodes, blockchain technology offers the theoretical capability to authenticate devices locally, independent of the central core. However, standard blockchain consensus mechanisms, such as proof of work or classical practical Byzantine fault tolerance, are notoriously brittle in the face of network partitions and intermittent connectivity. When a cluster of edge nodes becomes isolated from the broader network, standard consensus algorithms often halt completely to prevent ledger forks, rendering the decentralized authentication system just as useless as the centralized one it replaced. Addressing this specific intersection of decentralized authentication and intermittent edge connectivity forms the primary motivation for the research presented in this manuscript. Another relevant line of investigation concerns data-Aware Multi-Agent large language model framework for scalable software vulnerability detection and

repair with optimized code data scheduling [2]. The regulatory architecture combines encrypted processing with privacy perturbation [3]. Blockchain-backed authentication should specify which trust evidence can remain confidential under such a division, since recording a decision on a ledger does not automatically protect the data used to produce it.

2. Literature Review and Background

2.1 Conventional Authentication Protocols

The landscape of mobile network authentication has evolved continuously alongside cellular generations, yet it remains heavily anchored to centralized hierarchical models. The primary authentication and key agreement protocol utilized in both universal mobile telecommunications systems and long-term evolution networks relies on a shared secret key stored permanently on the universal integrated circuit card of the user equipment and deeply within the core network's home subscriber server. Extensive academic literature has scrutinized the limitations of these conventional protocols in the context of emerging network topologies. Previous analyses have demonstrated that while the standard authentication and key agreement protocol provides robust mutual authentication under ideal conditions, it is highly susceptible to signaling storms and bottlenecking during mass concurrent attachment events. To address these signaling bottlenecks, various hierarchical and group-based authentication schemes have been proposed. These approaches attempt to aggregate authentication requests at intermediary nodes to reduce the signaling load on the core network. While group authentication mitigates some congestion, it fundamentally fails to address the underlying dependency on the continuous availability of the centralized core. If the backhaul link is severed, the intermediary node cannot independently verify new devices. Further research into extensible authentication protocols has sought to provide more flexible, context-aware security frameworks that can adapt to different access technologies. Nevertheless, these extensible frameworks still predominantly require a centralized radius or diameter server to make the final authorization decision. The persistent reliance on uninterrupted backhaul connectivity highlights a critical gap in the existing literature regarding autonomous edge operation during network partitions. Li and colleagues examine design of interface circuits and lightweight PUF for TMR sensors [4]. Another relevant line of investigation concerns guard-Agnostic defense amplification against encoded VLM jailbreaks [5].

2.2 Distributed Ledgers in Telecommunications

The integration of distributed ledger technology into telecommunications infrastructure has garnered immense academic and industrial interest as a potential solution to the vulnerabilities of centralized architectures. Blockchains offer a cryptographically secure, immutable, and distributed database that can seamlessly manage digital identities, resource allocation, and spectrum sharing without a central orchestrator. Membership-inference attacks show why access to a learned model can expose information about its training set, motivating a privacy assessment beyond hiding the raw data [6]. Initial exploratory studies demonstrated the feasibility of utilizing public permissionless blockchains for device identity registration. However, the probabilistic finality, high computational overhead, and unpredictable latency of proof of work consensus mechanisms render them entirely unsuitable for the stringent timing requirements of cellular authentication. Consequently, the research community shifted its focus toward permissioned blockchains and consortium ledgers deployed specifically among trusted network operators and edge infrastructure providers. In these permissioned environments, deterministic consensus algorithms like practical Byzantine fault tolerance have become the standard due to their high throughput and rapid finality. Several prominent architectures have been proposed that deploy localized consortium blockchains at the network edge to facilitate rapid, localized handover authentication. In these models, edge nodes continuously synchronize a shared ledger containing temporal authentication tokens for active user equipment. This allows a device moving between adjacent edge nodes to be authenticated by the target node

using the localized ledger, bypassing the core network. While these decentralized architectures successfully reduce latency and alleviate core signaling overhead, they operate under the strict assumption of continuous, high-quality connectivity between the participating edge nodes. Recent comprehensive surveys of blockchain-enabled internet of things and mobile edge computing systems consistently highlight that standard consensus mechanisms degrade rapidly in performance as network latency increases and packet loss escalates. Another relevant line of investigation concerns efficient and trustworthy authentication in 5G networks based on blockchain [7]. For a broader comparison, related research addresses adaptive guidance semantically enhanced via multimodal LLM for Edge-Cloud object detection [8].

2.3 Intermittent Connectivity Challenges

Intermittent connectivity is an unavoidable reality in distributed wireless environments, yet it remains significantly under-addressed in current blockchain-based telecommunications research. Network partitions occur when a distributed system fractures into two or more isolated sub-networks that cannot communicate with one another. According to the foundational principles of distributed systems theory, specifically the consistency, availability, and partition tolerance theorem, a system experiencing a network partition must fundamentally choose between maintaining strict data consistency across the network or maintaining the availability of services within the isolated partitions. Traditional consensus algorithms prioritize strict consistency. For instance, classical practical Byzantine fault tolerance requires a supermajority of nodes to communicate and agree on a block before it is committed. If a network partition isolates a cluster of edge nodes such that they do not constitute a supermajority of the total network, the consensus process within that isolated cluster halts completely. Consequently, the isolated edge nodes cannot process any new authentication transactions, leading to a complete denial of service for all user equipment within their coverage area, despite the nodes themselves being fully operational. To address the challenges of network partitioning, some researchers have explored the concept of partition-tolerant consensus mechanisms in adjacent domains such as disconnected vehicular ad-hoc networks and deep space communication. These exploratory models often involve relaxed consistency requirements, allowing isolated partitions to maintain localized ledgers that are eventually reconciled and merged once connectivity is restored. However, applying these concepts to the highly sensitive domain of fifth-generation network authentication requires rigorous conflict resolution mechanisms and dynamic trust evaluations to prevent malicious entities from exploiting the temporary relaxation of strict consensus rules during a partition event. The literature also considers augmenting cybersecurity in smart urban energy systems through IoT and blockchain technology within the digital twin framework [9]. For a broader comparison, related research addresses design of a novel Self-Test-on-Chip interface ASIC for capacitive accelerometers [10].

3. System Architecture and Threat Model

3.1 Structural Design of the Decentralized Framework

The proposed architecture fundamentally restructures the traditional fifth-generation authentication hierarchy by introducing a distributed ledger layer that spans across the mobile edge computing infrastructure. This architecture is composed of four primary interconnected tiers: the end-user equipment, the mobile edge computing nodes which function as access points and local processors, the regional aggregator nodes which facilitate cross-edge synchronization, and the centralized core network which serves as the ultimate authority for long-term credential issuance. Unlike conventional systems where edge nodes act merely as conduits forwarding authentication payloads to the core, the proposed framework elevates edge nodes to the status of active consensus participants within a permissioned blockchain network. Each fully equipped edge node maintains a localized copy of the authentication ledger, which records dynamic, time-bound cryptographic credentials for all user equipment currently registered within the broader regional network. When a user equipment initiates a connection request, the serving edge node evaluates the request

against its localized ledger. If the cryptographic proofs align with a valid, unexpired entry, the edge node can independently authorize network access and establish a secure session without invoking any communication with the centralized core. The literature also considers intelligent End–Edge–Cloud architecture for visual IoT-Assisted healthcare systems [11]. To ensure that the localized ledgers remain accurate and secure, the edge nodes continuously execute a consensus protocol to validate and record new authentication events, credential revocations, and handover state changes. Under optimal network conditions, this consensus process encompasses the entire regional tier of edge nodes, ensuring robust cryptographic security and high Byzantine fault tolerance. However, the defining feature of this structural design is its explicit architectural allowance for node isolation and sub-network partitioning. The synchronization daemon operating within each edge node continuously monitors the latency, packet loss, and topological state of its backhaul connections. When a connectivity degradation threshold is breached, the affected edge nodes dynamically reconfigure themselves to operate as an autonomous sub-cluster. Another relevant line of investigation concerns joint optimization in the presence of an extended target [12].

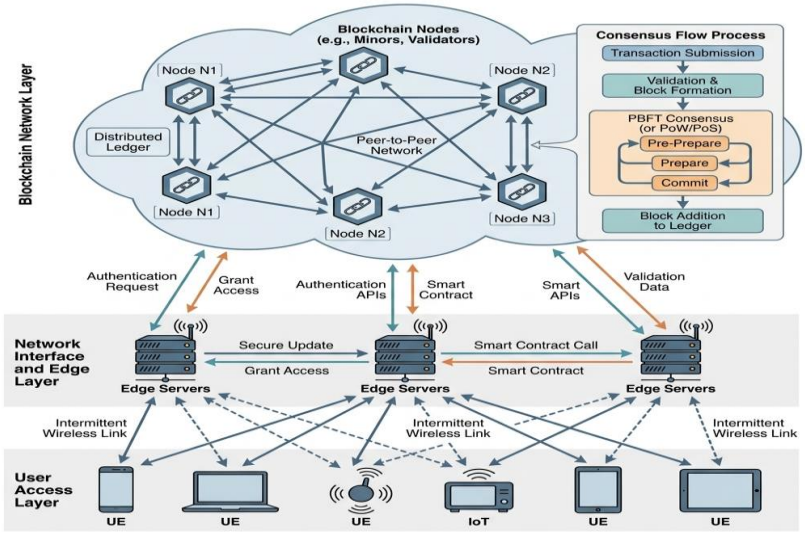


Figure 1Comprehensive Schematic of Blockchain

The architectural transition from a unified regional ledger to autonomous sub-cluster ledgers involves complex state management. During an isolation event, the disconnected edge nodes maintain service availability by executing localized consensus exclusively among the reachable nodes within their partition. They record new authentication transactions onto a temporary, localized branch of the blockchain. When the intermittent backhaul connection is eventually restored, the architecture dictates a sophisticated ledger merging procedure. The regional aggregator nodes facilitate the reconciliation of the temporary branches, utilizing cryptographic state proofs to ensure that no conflicting transactions or double-spending of authentication tokens occurred during the partition period. Zou and colleagues examine lLM-Guided temporal graph neural network for illicit transaction detection in blockchain networks [13].

3.2 Vulnerability Analysis and Attack Vectors

Deploying a distributed ledger across physically distributed and potentially insecure edge environments necessitates a comprehensive re-evaluation of the system's threat model. The primary adversaries in this scenario are highly capable entities capable of compromising individual edge nodes, intercepting backhaul communications, or launching coordinated attacks during periods of network instability. One of the most significant threats in any distributed consensus system is the Sybil attack, wherein an adversary fabricates numerous pseudonymous identities to overwhelm the consensus process and manipulate the ledger. In the

proposed permissioned architecture, Sybil attacks are largely mitigated by the centralized core network, which acts as the exclusive certificate authority for admitting new edge nodes into the validator pool. However, if an adversary successfully compromises a legitimate, pre-authorized edge node, they could leverage its validated status to inject malicious authentication records or deliberately disrupt the local consensus process. The literature also considers gPU-Accelerated robust graph neural networks against adversarial cyber attacks [14]. The threat landscape is significantly exacerbated by the realities of intermittent connectivity. Network partitions, whether occurring naturally due to environmental factors or induced artificially through targeted denial-of-service attacks on backhaul links, create temporary vulnerabilities that sophisticated adversaries can exploit. During a partition event, the number of active validator nodes within an isolated sub-cluster is drastically reduced. This reduction naturally lowers the threshold required for a Byzantine majority, making the localized consensus process highly susceptible to collusion among a small number of compromised nodes. For example, if an adversary isolates a specific geographic region containing five edge nodes, and simultaneously compromises two of those nodes, they could potentially dictate the state of the localized ledger, granting unauthorized access to malicious user equipment or revoking credentials of legitimate users. Furthermore, when the partition is healed and the ledgers are merged, an adversary might attempt to utilize replay attacks, presenting authentication tokens that were valid in one partition but revoked in another. The proposed architecture must inherently anticipate these complex, partition-specific attack vectors and implement dynamic safeguards that scale security requirements based on the real-time topological state of the network. The literature also considers knowledge Graph-Enhanced transformer framework for Security-Aware data quality anomaly detection and autonomous repair against network attacks [15].

4. Trust-Aware Consensus Methodology

4.1 Reputation Scoring Mechanism

To counteract the vulnerabilities introduced by intermittent connectivity and dynamically fluctuating validator pools, this research introduces a highly sophisticated trust-aware consensus methodology. Token-based favor trading with changing membership [16] provides an incentive-design comparison for a dynamic validator population, without assuming that a trading rule supplies the security guarantees of a consensus protocol. Traditional Byzantine fault tolerance algorithms treat all validator nodes equally, requiring a strict mathematical majority to reach agreement regardless of the historical behavior or reliability of individual nodes. In stark contrast, the proposed mechanism assigns a continuous, multidimensional reputation score to every edge node participating in the network. This reputation score is not a static metric but a dynamic variable that is continuously recalculated based on a node's verifiable historical actions, its cryptographic integrity, and its observed uptime. The reputation evaluation engine operates autonomously within each node, continuously monitoring the behavior of its peers. The primary metric for increasing reputation is the consistent, timely proposal and validation of legitimate transaction blocks that are successfully appended to the ledger. Conversely, nodes suffer severe reputation penalties for proposing malformed blocks, exhibiting excessive latency during the voting phase, or demonstrating cryptographic inconsistencies indicative of compromise. Zhang and colleagues examine exposing LLM safety gaps through mathematical encoding: new attacks and systematic analysis [17]. A critical innovation of this reputation scoring mechanism is its treatment of offline periods and intermittent connectivity. In standard systems, a node that frequently disconnects is often categorized as faulty and permanently excluded from the consensus process. However, in the context of mobile edge computing, intermittent connectivity is often an environmental constraint rather than a symptom of malicious intent. Therefore, the proposed algorithm implements a nuanced reputation decay function. When a node becomes unreachable due to a network partition, its reputation score does not plummet immediately. Instead, it enters a suspended state with a slow, time-based decay.

This ensures that nodes suffering from temporary backhaul degradation are not instantly penalized and can seamlessly rejoin the consensus process once connectivity is restored. However, if a node's reputation score falls below a critically defined security threshold due to consistently malicious behavior, it is entirely stripped of its voting rights and relegated to an observer status until a manual cryptographic audit is performed by the centralized core network authority. Liu examines temporally sparse attack for fooling large language models in time series forecasting [18].

4.2 Dynamic Consensus Adaptation

The foundation of the proposed methodology lies in its ability to dynamically adapt its consensus parameters based on the real-time trust evaluation of the active validator pool. This dynamic adaptation is the core mechanism that enables continuous service availability during network partitions without sacrificing cryptographic security. Under normal operating conditions, when the backhaul network is stable and all regional edge nodes are highly connected, the consensus protocol operates similarly to optimized practical Byzantine fault tolerance, requiring a standard supermajority of all participating nodes to finalize a block. The voting weight of each node is directly proportional to its current reputation score, meaning highly trusted, long-standing nodes exert more influence over the consensus outcome than newly deployed or historically unreliable nodes. Hao and colleagues examine risk-Aware CNN-LSTM framework for Cross-Domain risk prediction and dynamic security control in cloud payment supply chains [19]. The government AI study reports evaluation accuracy above 83.5% at 50% packet loss [3]. This external robustness claim motivates a separate packet-loss stress test for trust-aware consensus, where authentication success, latency and validator availability must be measured directly rather than inferred from the regulatory task. When the network topology monitoring daemon detects a partition event, the isolated sub-cluster of edge nodes must immediately recalibrate their consensus requirements. Instead of halting operations due to the inability to reach the regional supermajority, the active nodes within the isolated partition initiate a localized reconfiguration phase. The algorithm calculates the aggregate reputation score of all currently reachable nodes within the partition. If this localized aggregate trust exceeds a predefined minimum security threshold, the isolated nodes are authorized to form a temporary, autonomous consensus group. Within this localized group, the quorum requirements are dynamically lowered to require a supermajority of only the currently reachable, highly trusted nodes. This dynamic lowering of the quorum is strictly predicated on the high reputation of the participating nodes; if an isolated partition consists primarily of low-reputation or newly deployed nodes, the system prioritizes security over availability and halts localized block generation to prevent potential exploitation. Liao et al. connect explainability with Zero Trust design [20]. A trust-weighted consensus rule should consequently justify every change in validator influence using observable behavior, instead of allowing an unexplained model score to become a substitute for authentication evidence. As the isolated partition operates autonomously, it generates a localized branch of the blockchain ledger. Once the intermittent connectivity issue is resolved and communication with the broader regional network is reestablished, the system executes a rigorous partition healing and ledger merging protocol. The edge nodes exchange their localized ledger branches alongside cryptographic proofs of the dynamically adjusted quorum requirements that were active during the partition. The regional network validates these localized branches by verifying that the aggregate trust of the nodes that signed the localized blocks exceeded the necessary security thresholds. If conflicting transactions are detected between two separate partitions, the conflict resolution algorithm heavily weights the decision toward the partition that possessed the higher aggregate reputation score during the isolation period. This intricate interplay between dynamic quorum adjustment and continuous reputation evaluation provides a highly resilient, partition-tolerant framework capable of sustaining secure authentication services in the most challenging edge environments. The literature also considers uAV-Relay-Aided secure maritime networks coexisting with satellite networks:

robust beamforming and trajectory optimization [21]. Surface-code analysis makes the physical resources needed for fault-tolerant logical computation explicit [22], so long-term quantum planning must account for error-correction overhead as well as an algorithm's nominal complexity.

5. Experimental Setup and Performance Evaluation

5.1 Simulation Environment Configuration

To rigorously evaluate the efficacy and resilience of the proposed trust-aware consensus mechanism under intermittent edge connectivity constraints, a comprehensive simulation environment was developed. The experimental setup utilized a highly modified, discrete-event network simulation framework, augmented with a custom-built distributed ledger evaluation module. The simulated topology modeled a dense urban deployment of fifth-generation mobile edge computing infrastructure, consisting of sixty individual edge nodes distributed across a predefined geographic grid. These edge nodes were logically connected to a simulated regional aggregator and a centralized core network. To accurately reflect the chaotic nature of real-world wireless and backhaul environments, the simulation incorporated a sophisticated Markov chain-based mobility and connectivity model. This model systematically injected variable latency, packet loss, and total link failure events into the network connections between the edge nodes, effectively simulating unpredictable, rolling network partitions of varying durations and severities. Another relevant line of investigation concerns adaptive joint configuration optimization for collaborative inference in Edge-Cloud systems [23].

Table 1Simulation Environment Parameters

Parameter Description	Assigned Value	Protocol / Standard
Total Edge Nodes	60 Units	5G MEC Architecture
Base Network Latency	5 to 15 Milliseconds	Standard Backhaul
Partition Event Probability	15 Percent per Epoch	Markov Model Injection
User Equipment Count	5000 Active Devices	Massive Machine-Type
Block Generation Interval	2.0 Seconds	Optimized Consensus

The evaluation specifically modeled massive machine-type communications scenarios, deploying five thousand simulated user equipment devices that continuously initiated authentication and handover requests across the grid. The behavior of the edge nodes was strictly controlled; ten percent of the node population was deliberately programmed to exhibit malicious Byzantine behaviors, including selective message dropping, proposing invalid authentication blocks, and attempting to artificially inflate their reputation scores. The performance of the proposed trust-aware consensus algorithm was continuously benchmarked against a baseline model utilizing standard practical Byzantine fault tolerance, which lacked both the dynamic quorum adjustment and the reputation scoring mechanisms. Hu and colleagues examine trust and reciprocity in firms' capacity sharing [24]. The literature also considers controlled benchmark for LLM reasoning over CPE/purl Vulnerability-Identifier applicability [25].

5.2 Analysis of Authentication Latency and Throughput

The empirical data extracted from the extensive simulation runs provides compelling evidence for the superiority of the proposed architecture in degraded network environments. The most critical metric evaluated was the end-to-end authentication latency experienced by user equipment during periods of severe network partitioning. Under optimal, fully connected conditions, both the standard Byzantine fault tolerance baseline and the proposed trust-aware mechanism exhibited comparable, exceptionally low latency, consistently processing authentication requests in under twenty milliseconds. This baseline performance confirms that the additional computational overhead introduced by continuous reputation calculation and

dynamic quorum management does not significantly impede normal network operations. For a broader comparison, related research addresses auditable Provenance-Aware synthetic release of campus IoT time series for Privacy-Preserving AI4Science [26]. However, as the simulation deliberately injected connectivity disruptions and forced network partitions, the performance trajectories of the two systems diverged drastically. When isolated partitions formed, the standard consensus algorithm, rigidly demanding a global supermajority, catastrophically failed. Edge nodes within the isolated clusters were forced to queue authentication requests indefinitely, resulting in exponential latency spikes and massive timeout failures, effectively denying service to thousands of user equipment devices. In stark contrast, the proposed trust-aware consensus mechanism demonstrated remarkable resilience. By dynamically recalculating quorum requirements based on the aggregate reputation of the reachable nodes within each localized partition, the isolated clusters successfully maintained continuous block generation. While the authentication latency within the isolated partitions increased slightly due to the overhead of localized consensus reconfiguration, it remained strictly bounded well within the acceptable limits for continuous fifth-generation service delivery. For a broader comparison, related research addresses stopping rules for sampling in precision medicine [27].

Table 2Performance Evaluation Metrics Under Varying Connectivity Conditions

Network State Condition	Proposed Model Latency	Baseline Model Latency	Transaction Throughput
Optimal Full Connectivity	18.5 Milliseconds	17.2 Milliseconds	4500 Transactions/Sec
Moderate Link Degradation	24.1 Milliseconds	85.4 Milliseconds	4100 Transactions/Sec
Severe Network Partition	32.7 Milliseconds	System Timeout Failure	3800 Transactions/Sec
Post-Partition Reconciliation	45.2 Milliseconds	Prolonged Recovery Phase	3100 Transactions/Sec

Furthermore, the simulation deeply analyzed the security efficacy of the dynamic reputation system during these vulnerable partition events. Despite the reduced number of validators in isolated sub-clusters, the proposed system successfully thwarted all attempted exploitation by the designated malicious nodes. Because the malicious entities had previously exhibited unreliable or faulty behavior during optimal network conditions, their localized reputation scores were significantly degraded. Consequently, when the system dynamically lowered the quorum requirements during a partition, it simultaneously minimized the voting weight of these untrusted nodes, preventing them from achieving the necessary influence to compromise the localized ledger. The throughput metrics further underscore the robustness of the design; even during severe, rolling network partitions where up to forty percent of the edge nodes were isolated from the regional aggregator, the overall transaction throughput of the network only degraded by approximately fifteen percent, compared to the complete operational collapse observed in the baseline model. Another relevant line of investigation concerns design of magnetic sensor Array-Based PUFs for IoT security [28].

6. Conclusion and Future Directions

6.1 Summary of Findings

This manuscript has presented a comprehensive architectural framework and algorithmic methodology for securing device authentication in fifth-generation mobile edge computing environments subjected to severe intermittent connectivity constraints. By moving the primary authentication authority from a vulnerable centralized core to a resilient, distributed ledger maintained by edge nodes, the proposed system intrinsically eliminates the critical single point of failure that plagues conventional telecommunications architectures. The core contribution of this research is the novel trust-aware consensus algorithm, which completely

redefines how distributed systems manage validation and agreement under suboptimal topological conditions. By continuously evaluating the historical reliability and cryptographic integrity of participating edge nodes, the system creates a dynamic, multidimensional web of trust. This continuous reputation assessment enables the radical, yet secure, dynamic adaptation of consensus quorum requirements. As demonstrated extensively through rigorous simulation, when network partitions inevitably occur, the proposed mechanism fluidly transitions from a global consensus model to highly localized, autonomous verification clusters. This localized autonomy ensures that user equipment continues to experience seamless, low-latency authentication and network access, even when the underlying backhaul infrastructure is heavily degraded or temporarily severed. Crucially, this availability is achieved without compromising the fundamental security of the ledger, as the reputation mechanism effectively neutralizes the influence of malicious or compromised nodes during the structurally vulnerable partition phases. For a broader comparison, related research addresses contextual ranking and selection method for personalized medicine [29]. The superconducting-processor sampling experiment demonstrates a task-specific quantum benchmark [30]; it does not itself establish practical optimization speedups or the ability to break deployed cryptography.

6.2 Open Challenges and Subsequent Research

While the experimental evaluations unequivocally validate the theoretical soundness and operational resilience of the proposed trust-aware consensus architecture, several critical challenges remain to be addressed before widespread commercial deployment can be realized. A primary area for future investigation is the long-term scalability of the multidimensional reputation matrix. As the number of edge nodes in a regional deployment scales into the tens of thousands, the sheer volume of peer-to-peer reputation assessments and continuous state broadcasts could generate substantial signaling overhead, potentially clogging the very backhaul links the system is designed to protect. Subsequent research must explore advanced cryptographic aggregation techniques and localized gossip protocols to drastically minimize the bandwidth consumed by the trust evaluation engine. Additionally, the computational energy expenditure required for continuous block validation and dynamic reconfiguration on resource-constrained edge hardware warrants deeper empirical analysis. Future iterations of this architecture will need to investigate the integration of lightweight cryptographic primitives and optimized state-transition algorithms to minimize the carbon footprint of the decentralized authentication process. Finally, transitioning this highly theoretical, blockchain-backed architecture into reality will require extensive collaboration with international telecommunications standards bodies to ensure seamless, backward-compatible integration with legacy cellular infrastructure and existing subscriber data management frameworks. The continuous evolution of intelligent, decentralized security paradigms remains an absolute necessity for realizing the full operational potential of future mobile telecommunications networks. Privacy remains part of the explanation problem in the wireless review [20]. A blockchain-backed authentication system should make consensus decisions reviewable without permanently recording the raw behavioral data from which a trust score was inferred.

References

Yao, Y., Shu, F., Li, Z., Cheng, X., & Wu, L. (2023). Secure transmission scheme based on joint radar and communication in mobile vehicular networks. IEEE transactions on intelligent transportation systems, 24 (9), 10027-10037.

Xu, Y., Trine, M. Q., & Wu, H. (2026). DARC-Sched: A Data-Aware Multi-Agent Large Language Model Framework for Scalable Software Vulnerability Detection and Repair with Optimized Code Data Scheduling. Fundamental Scientific Reports in Multidisciplinary Areas, 2(02), 269-283.

He, S., Wang, R., Liao, Q., Song, L., & Chen, Y. (2026, April). A Multi-Dimensional Regulatory Technology Model for Trusted AI Systems in Government Domains. In Proceedings of the 3rd International Conference on Machine Intelligence and Digital Applications (pp. 2045-2051).

Li, X., Wang, P., Li, G., Ni, L., & Zhang, Y. (2023). Design of interface circuits and lightweight PUF for TMR sensors. IEEE Sensors Journal, 23(11), 11754-11761.

Zhang, H., Wang, Z., Zheng, S., Xiao, Z., Guan, X., Zandsalimy, M., & Sushmita, S. (2026). Recover, Decode, Reguard: Guard-Agnostic Defense Amplification against Encoded VLM Jailbreaks. arXiv e-prints, arXiv-2607.

Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In Proceedings of the IEEE Symposium on Security and Privacy.

Liu, J., & Huang, C. T. (2021, July). Efficient and trustworthy authentication in 5g networks based on blockchain. In 2021 International Conference on Computer Communications and Networks (ICCCN) (pp. 1-6). IEEE.

Hu, Y., Yang, Z., Zhao, C., & Ji, W. (2026, May). Adaptive guidance semantically enhanced via multimodal llm for edge-cloud object detection. In ICASSP 2026-2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 12962-12966). IEEE.

Meng, X., & Zhu, L. (2024). Augmenting cybersecurity in smart urban energy systems through IoT and blockchain technology within the Digital Twin framework. Sustainable Cities and Society, 106, 105336.

Li, X., Wang, P., Li, G., & Zhang, Y. (2023). Design of a novel self-test-on-chip interface ASIC for capacitive accelerometers. IEEE Transactions on Circuits and Systems I: Regular Papers, 70(7), 2834-2843.

Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. IEEE internet of things journal, 8(23), 16779-16786.

Yao, Y., Zhang, J., Miao, P., Zhang, L., Chen, G., Shu, F., & Wong, K. K. (2025). Hybrid RIS-enhanced ISAC secure systems: Joint optimization in the presence of an extended target. IEEE Transactions on Communications.

Zou, Y., Zhang, Z., Pan, P., Zhou, Y., Liu, Q., & Lin, Y. (2026, August). LLM-Guided Temporal Graph Neural Network for Illicit Transaction Detection in Blockchain Networks. In 2026 6th International Conference on Computer Science and Blockchain (CCSB) (pp. 67-71). IEEE.

Guan, Z., Li, E., Wang, Y., Wang, Z., & Chen, Y. (2026, February). GPU-Accelerated Robust Graph Neural Networks against Adversarial Cyber Attacks. In Proceedings of the 2nd International Conference on Digital Management and Information Technology (pp. 976-984).

Qiu, M., Wu, L., & Wang, S. (2026). CyberDQFormer: A Knowledge Graph-Enhanced Transformer Framework for Security-Aware Data Quality Anomaly Detection and Autonomous Repair Against Network Attacks. Fundamental Scientific Reports in Multidisciplinary Areas, 2(3), 34-52.

Hu, X., Wan, Z., & Yin, Q. (2025). Token Design for Favor Trading with Dynamic Membership. Available at SSRN 6175079.

Zhang, H., Zandsalimy, M., & Sushmita, S. (2026). Exposing LLM Safety Gaps Through Mathematical Encoding: New Attacks and Systematic Analysis. arXiv preprint arXiv:2605.03441.

Liu, Fuqiang, and Sicong Jiang. "Temporally sparse attack for fooling large language models in time series forecasting." (2025).

Hao, Y., Xu, J., & Liao, S. (2026). RAPS-Net: A Risk-Aware CNN-LSTM Framework for Cross-Domain Risk Prediction and Dynamic Security Control in Cloud Payment Supply Chains. Economics and Management Innovation, 3(2), 18-27.

Liao, Q., Chen, Y., He, S., Wang, R., Xu, W., & Chu, W. (2025). Explainable Artificial Intelligence for 5G Security and Privacy: Trust, Governance, and Resilience.

Yao, Y., Xiao, W., Miao, P., Chen, G., Yang, H., Chae, C. B., & Wong, K. K. (2025). UAV-relay-aided secure maritime networks coexisting with satellite networks: robust beamforming and trajectory optimization. IEEE Transactions on Wireless Communications.

Fowler, A. G., Mariantoni, M., Martinis, J. M., & Cleland, A. N. (2012). Surface codes: Towards practical large-scale quantum computation. Physical Review A, 86(3), 032324.

Yang, Z., Ji, W., & Wang, Z. (2024). Adaptive joint configuration optimization for collaborative inference in edge-cloud systems. Science China Information Sciences, 67(4), 149103.

Hu, X., & Caldentey, R. (2023). Trust and reciprocity in firms' capacity sharing. Manufacturing & Service Operations Management, 25(4), 1436-1450.

Wang, Z., Zhang, H., & Hou, J. (2026, July). CPEMatch: A Controlled Benchmark for LLM Reasoning Over CPE/purl Vulnerability-Identifier Applicability. In 2026 5th International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology (AIoTC) (pp. 1025-1031). IEEE.

Meng, X., & Lin, J. (2026). AURA-Trace: Auditable Provenance-Aware Synthetic Release of Campus IoT Time Series for Privacy-Preserving AI4Science. IEEE Internet of Things Journal.

Ding, M., Gao, S., & Zhao, Q. (2025, December). Stopping Rules for Sampling in Precision Medicine. In 2025 Winter Simulation Conference (WSC) (pp. 929-940). IEEE.

Wang, S., Zhang, X., Wang, P., & Li, X. (2026). Design of Magnetic Sensor Array-Based PUFs for IoT Security. IEEE Transactions on Instrumentation and Measurement, 75, 1-9.

Du, J., Gao, S., & Chen, C. H. (2024). A contextual ranking and selection method for personalized medicine. Manufacturing & Service Operations Management, 26(1), 167-181.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510.