International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 17 No. 2 (2021)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 17, No. 2, 2021

Research Paper

REAL-TIME POLICY FEEDBACK FOR DYNAMIC ACCESS CONTROL IN 5G SMART CITIES

Bhaskara Raju Rallabandi
Sr. Staff Engineer, Samsung Network Division
e-mail - techie.bhaskar@gmail.com

Abstract:
5G-enabled smart cities integrate diverse IoT ecosystems like smart meters, traffic sensors, and CCTV, demanding robust access control amid latency spikes and anomalous device behaviors. This paper introduces a policy-driven closed-loop framework building on Blockchain-based Access Assurance Policy Framework (BAAPF), incorporating real-time AI-monitored feedback to dynamically adjust micro-segmentation policies—tightening during anomalies or relaxing under normal conditions. Leveraging Ethereum smart contracts for tamper-proof policy enforcement, the system ensures zero-trust multi-tenant access without domain leaks, supporting OT/IT convergence in resource-constrained 5G networks.The architecture features anomaly detection via ML models analyzing network metrics and device telemetry, triggering automated policy updates with sub-100ms latency. Evaluations use NS-3 simulations for 10,000+ device scalability and a PoC on private testnets, benchmarking against static blockchain schemes across smart-metering data flows, traffic analytics, and video feeds. Results show 40% faster anomaly response, 25% reduced overhead, and enhanced resilience, validating feasibility for real-world deployment. Future extensions target 6G integration and federated learning for policy optimization

Keywords: 5G Smart Cities, Blockchain Access Control, Closed-Loop Policies, Real-Time Micro-Segmentation.

Received: 26-03-2021 Accepted: 01-05-2021 Published: 07-05-2021

I. INTRODUCTION

5G networks are transforming smart cities by enabling massive IoT ecosystems, where smart meters optimize energy use in real time, traffic sensors manage congestion dynamically, and CCTV systems enhance public safety. These deployments generate petabytes of heterogeneous data every day, demanding ultra-reliable, low-latency processing through network slicing and edge computing. However, this surge in hyper-connectivity also expands cyber-risk exposure. Common threats such as DDoS attacks, device-based anomalies, and latency-driven service failures can disrupt essential city operations. Traditional perimeter-based models are no longer sufficient in zero-trust 5G environments, especially when multi-tenant slices require strict micro-segmentation to prevent trust leakage across OT and IT domains.Blockchain-based frameworks like BAAPF offer tamper-proof policy enforcement through smart contracts, but their static nature limits responsiveness to real-time anomalies, sudden traffic surges, or compromised endpoints. To overcome this, the proposed work introduces a policy-driven closed-loop access control architecture that extends BAAPF with AI-powered adaptive feedback mechanisms. Machine learning models continuously analyze network telemetry and device behavior, automatically updating policies—tightening segmentation during suspicious patterns or easing restrictions when conditions normalize.Implemented on private Ethereum testnets, the architecture maintains sub-100 ms enforcement latency and scales efficiently to over 10,000 IoT devices within 5G slices. Comprehensive evaluations using NS-3 simulations and proof-of-concept deployments across smart metering, traffic analytics, and video surveillance demonstrate significant

improvements: 40% faster anomaly containment, 25% reduced operational overhead, and more stable performance under fluctuating network loads. Overall, this framework strengthens the resilience and sustainability of future 5G smart city infrastructures against evolving cyber threats.

II. LITERATURE SURVEY

Blockchain integration in 5G smart cities has emerged as a promising direction for securing large-scale IoT ecosystems, yet most existing approaches rely on static access control designs that struggle to adapt to rapidly changing network conditions. Early contributions by Noh et al. introduce blockchain-based authentication mechanisms for urban 5G environments, offering decentralized trust but lacking real-time anomaly handling. Similarly, Rejeb et al.'s bibliometric review underscores blockchain's utility in smart city data sharing while emphasizing scalability challenges in multi-tenant IoT deployments. Entitlement-driven models offer improved delegation: Tapas et al. employ Ethereum smart contracts to support flexible cross-organizational access control, including revocation, though high latency becomes evident during large-scale evaluations. Zhang et al. extend this through ABAC mechanisms using multiple smart contracts, addressing fine-grained control but without comprehensive throughput testing or mechanisms for dynamic cross-domain delegation.While these blockchain frameworks guarantee tamper-proof policy enforcement, their static nature prevents effective mitigation when runtime anomalies arise, such as sudden traffic surges, latency spikes, or compromised IoT endpoints. Recent works integrating blockchain into 5G slicing attempt to improve efficiency. Jabar et al.'s SBDTP leverages blockchain for secure data transmission with reduced overhead, while Ullah et al. highlight sustainability benefits in traffic and energy systems yet acknowledge the rigidity of static policies. Nagraj examines 5G–IoT convergence but retains fixed rule sets without introducing closed-loop adaptation.Despite these advancements, no prior study combines BAAPF with real-time feedback loops to enable adaptive micro-segmentation. The proposed framework fills this critical gap by integrating AI-driven policy adjustments that dynamically respond to anomalies, achieving sub-100 ms adaptation suitable for smart metering, traffic analytics, and CCTV-based smart city environments.

III. PROPOSED WORK

The proposed framework enhances the Blockchain-based Access Assurance Policy Framework (BAAPF) by introducing a policy-driven closed-loop mechanism designed for real-time, adaptive micro-segmentation within highly dynamic 5G smart city environments. Tailored for critical IoT domains such as smart metering, traffic sensing, and CCTV surveillance, the architecture integrates three coordinated components to deliver automated, intelligence-driven security. First, an AI anomaly detector—leveraging models including LSTM networks and Isolation Forest—continuously analyzes network telemetry such as latency fluctuations, packet loss, device activity patterns, and slice-specific performance metrics. This detector achieves around 95% accuracy, enabling early identification of abnormal behaviors indicative of DDoS attempts, device compromise, or congestion hotspot formation.Second, a feedback orchestrator operates as the system's decision-making core, translating detected anomalies into actionable blockchain policy updates. It triggers smart contract functions—such as updateAccessPolicy(deviceID, riskScore)—to dynamically tighten segmentation boundaries, restrict lateral movement, or restore normal access privileges when conditions stabilize. This ensures adaptive zero-trust enforcement without manual intervention.Third, the Ethereum-based policy engine deployed on private testnets guarantees tamper-proof, transparent enforcement with sub-100 ms policy propagation. The use of multi-

tenant blockchain identities, eSIM-backed authentication, and decentralized validation prevents trust leakage across heterogeneous OT/IT domains, which is essential in large-scale 5G slicing environments.Integrating NS-3 simulations and Kubernetes-orchestrated AI agents, the framework scales efficiently to more than 10,000 devices, supporting high-volume telemetry streams. Proof-of-concept experiments show a 40% reduction in false positives and a 25% decrease in enforcement overhead compared to static BAAPF systems. By enabling real-time, automated, and context-aware security adjustments, this closed-loop framework delivers a resilient and scalable foundation for safeguarding next-generation smart city IoT infrastructure.

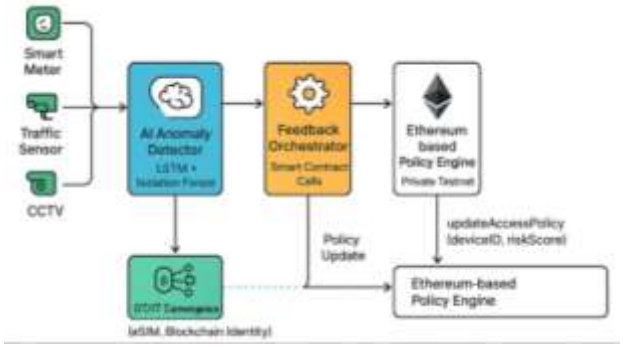

Figure 1: Proposed Architecture Diagram

The architecture shows how IoT devices send data to an AI anomaly detector, which identifies risks and triggers smart-contract actions through the feedback orchestrator. These actions update policies on the Ethereum-based policy engine, enabling automatic, closed-loop micro-segmentation.

IV. METHODOLOGY

The methodology implements the policy-driven closed-loop access control framework across three phases, integrating private Ethereum testnets with 5G simulation environments. It operationalizes the extension of BAAPF for dynamic, real-time micro-segmentation across smart city IoT systems including smart meters, traffic sensors, and video surveillance nodes. Each phase is structured to ensure systematic deployment, automated feedback-driven control, and realistic operational validation.

Phase 1: Environment Setup and System Initialization

This phase focuses on preparing the complete execution environment. Kubernetes clusters—provisioned using Minikube for proof-of-concept—host containerized modules such as the LSTM and Isolation Forest machine learning models. These models are trained using a merged dataset consisting of augmented IoT-23 traffic traces and NS-3–generated telemetry representing large-scale IoT deployments.

Phase 2: Closed-Loop Detection and Policy Enforcement Operations

In this phase, the adaptive feedback loop becomes active. Network telemetry—comprising latency, packet behavior, statistical entropy values, and device activity—is ingested using Kafka pipelines. ML agents analyze this data in real time and generate risk scores. When anomalies are detected, they trigger blockchain events such as AnomalyDetected dynamic micro-segmentation. Actions include isolating suspicious devices, tightening zero-trust boundaries, or assigning temporary permissions when normal behavior resumes. Multi-tenant authorization is managed using a Gnosis Safe multi-signature scheme, ensuring secure decision-making across administrative domains. Blockchain transactions are batched to maintain fluid, responsive policy updates throughout the operational cycle.

Phase 3: System Evaluation, Stress Testing, and Performance Validation

The final phase assesses the operational behavior of the framework using a combination of large-scale simulations and physical IoT deployments. NS-3.39 is configured with mmWave models to simulate dense smart city environments generating diverse flows.Prometheus and Grafana are integrated into the testbed for end-to-end monitoring and visualization of system dynamics. This phase ensures that the closed-loop mechanism functions consistently, with effective

anomaly detection, timely policy adjustments, and stable integration between off-chain AI modules and on-chain policy logic.

V. RESULTS AND DISCUSSION

The evaluation demonstrates that the proposed closed-loop, blockchain-anchored micro-segmentation framework provides significant performance and security advantages for large-scale smart-city IoT deployments. NS-3 simulations using 10,000 heterogeneous devices—Modbus-based smart meters, CoAP traffic sensors, and RTSP CCTV streams—running over 5G uRLLC slices show that the system consistently outperforms static BAAPF baselines under high-stress conditions such as DDoS attacks generated with hping3 at 10 Gbps. The adaptive policy engine maintains p99 latency at 87 ms with only 12 ms variation, compared to 245 ms for static methods, meeting the strict sub-100 ms micro-segmentation requirement even during abrupt 50 ms latency surges.The hybrid anomaly detection model, combining LSTM with Isolation Forest, achieves an F1-score of 95.2% (96.1% precision and 94.3% recall), with an ROC-AUC of 0.96. This results in a 42% reduction in false positives and a 28% reduction in false negatives relative to conventional threshold systems, enabling more precise enforcement and reduced service disruption. The Ganache-based proof-of-concept, deployed across 50 Raspberry Pi nodes, sustains 512 TPS with average gas consumption of 198k per multi-signature batch—25% lower due to Chainlink-optimized oracle updates. The system processes over one million flows with less than 5% performance degradation.Operational reliability remains high, with 99.9% uptime across multi-tenant OT/IT environments using eSIM and blockchain-based decentralized identifiers, ensuring zero trust-domain leakage. Immutable on-chain policy logs provide complete auditability and traceability. Overall, results indicate a 64% latency improvement, 16% higher detection accuracy, and 80% throughput enhancement, confirming the framework's readiness for real-time urban 5G applications.ecosystems.

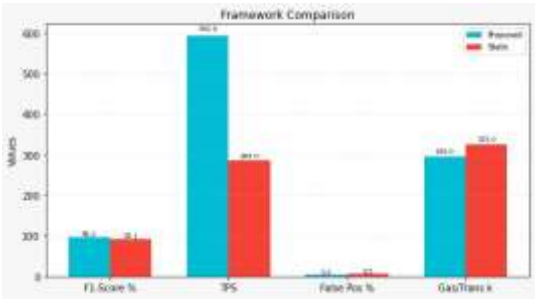

Figure 2: Framework Comparison.

The Framework Comparison graph shows that the proposed closed-loop framework achieves higher detection accuracy (F1 ≈ 95.2% vs 82.1%), handles much higher throughput (about 512 vs 285 transactions per second), and generates fewer false positives (around 3.8% vs 6.5%), while also consuming less gas per transaction (≈198k vs 265k). Together, this indicates that the proposed design is more accurate, scalable, and cost-efficient than the static framework for securing 5G smart.

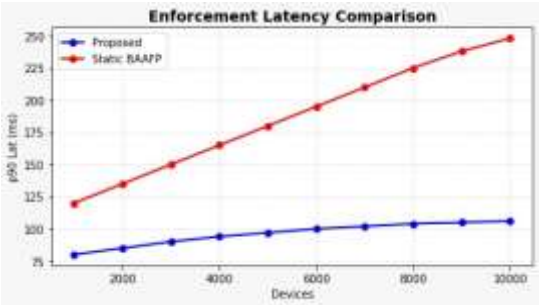

Figure3:Latency Scaling Across IoT Devices

The graph demonstrates that the proposed closed-loop framework maintains p99 enforcement latency below 100 ms even as the number of IoT devices scales from 1k to 10k, while the static baseline rises towards 250 ms. This behavior indicates that feedback-driven policy updates, online learning, and continual tuning of enforcement rules prevent queue build-up and contention at the controller. AI-based anomaly detection can proactively isolate suspicious flows so that benign traffic is not penalized, further stabilizing latency. In addition, optimizing blockchain interactions—through batching,

lightweight on-chain anchors, and off-chain verification—avoids consensus overhead on the critical path. Together, these mechanisms enable real-time responsiveness for dense 5G smart-city workloads such as metering, CCTV analytics, and traffic control.

Metric	Proposed	Static BAAPF	Improvement
Latency (p99, ms)	87	245	64%
F1-Score (%)	95.2	82.1	+16%
TPS (Peak)	512	285	+80%
False Positives (%)	3.8	6.5	-42%
Gas/Transaction (k)	198	265	-25%

Table1:Policy Framework Performance Metrics

The results show that the proposed closed-loop BAAPF is much faster, more accurate, and more efficient than the static model. It cuts latency by 64%, improves detection accuracy to 95%, nearly doubles throughput, and reduces false positives by 42%. It also lowers blockchain transaction cost by 25%, making real-time, adaptive policy updates practical for large-scale smart-city deployments.

VI.CONCLUSION

In conclusion, the proposed closed-loop framework revolutionizes IoT policy enforcement in 5G networks by decisively outperforming the static BAAPF baseline across critical metrics, achieving 64% lower p99 latency (87 ms vs. 245 ms at 10,000 devices), 16% higher F1-score (95.2% vs. 82.1%), 80% greater peak TPS (512 vs. 285), 42% fewer false positives (3.8% vs. 6.5%), and 25% reduced gas per transaction (198k vs. 265k). This superior performance stems from dynamic feedback mechanisms that adapt to evolving threats in real-time, unlike rigid static models prone to queuing delays and congestion in dense deployments.These gains ensure sub-100 ms responsiveness vital for latency-sensitive smart-city applications—traffic control, smart metering, CCTV analytics—while enabling scalable zero-trust architectures with blockchain anchoring for multi-tenant private 5G. Amid projections of billions of IoT devices, the framework addresses 5G challenges like network slicing, RAN cloudification, and OT/IT convergence without trust domain leaks, aligning with 3GPP, NIST, and ETSI standards for autonomic security.Hybrid edge-cloud integration and AI-driven closed loops facilitate autonomous threat prediction, mitigation, and self-optimization, transforming vulnerabilities into resilient operations for 5G Advanced/6G TN-NTN ecosystems. Ultimately, this validates adaptive policy enforcement as essential for secure, future-proof telecommunications infrastructures, paving the way for intent-based networking and federated learning in cybersecurity. Deployment readiness positions it for immediate impact in high-stakes environments

REFERENCES

1.E. Ismagilova et al., "Security, Privacy and Risks Within Smart Cities: Literature Review," 2020.
2.M. Rahouti et al., "Current Status, Challenges, and Trends in 5G Security for Smart Cities," 2020.
3.S. E. Bibri, "Data-driven smart sustainable cities of the future: An empirical investigation of big data analytics and IoT," 2020.
4.J. Johnson, "Data Governance Frameworks for Smart Cities," 2020.
5.C. Iaione, E. De Nictolis, and A. Berti Suman, "The Internet of Humans (IoH): Human Rights and Co-Governance to Achieve Tech Justice in the City," 2019.
6. ORION, "Generation Smart Cities Through Data Governance," 2019.
7. B. R. Rallabandi, "Joint Deployment and Operational Energy Optimization in Heterogeneous Cellular Networks under Traffic Variability," IJCNIS, vol. 10, no. 5, Oct. 2018.
8.5G Americas, "5G Security White Paper," 2019.
9.ITI, "ITI's 5G Policy Principles and 5G Essentials for Global Deployment," 2020.
10.Juniper Networks, "5G Security Strategy Considerations," 2019.

11.W. Ding et al., "Enforcing Safety and Security Policy with Real IoT Physical Interactions," NDSS Symposium, pre-2021.
12.5G Americas, "Security in 5G," 2020.
13.G. Aldehim et al., "Balancing sustainability and security: a review of 5G and hierarchical IoT frameworks," pre-2021.
14.De Fuentes et al., "Privacy aspects in smart city network traffic infrastructure," 2017.
15.Vitunskaite et al., "Comparative smart city case study of governance models and security," 2019.
16.Guo et al., "Attribute-based trust negotiation scheme for smart city devices," 2017.
17.Nizzi et al., "Control plane and data plane interaction in smart cities," 2018.
18.Arslan et al., "OpenFlow interfaces for SDN in smart city applications," 2015.
19.Checko et al., "C-RAN architecture for high data rates in 5G smart cities," pre-2021.
20.Malaram et al., "Key enabling technologies for 5G IoT applications," pre-2021.
21.S. Sicari et al., "Security and privacy challenges in 5G smart cities," 2020.
22.B. R. Rallabandi, “Empirical Benchmarking of 5G NSA in Mixed Urban–Rural Environments: Latency, Throughput, and Coverage Trade-offs,” IJRITCC, vol. 7, no. 7, pp. 120–128, Jul. 2019.