Volume: 14 Issue: III Month of publication: March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78030

A Multi-Tiered Decentralized Framework for Context-Aware Access Control and Trusted Authentication in Scalable IoT Ecosystems

Srivalli Ch[1], Dr. Vinay Chavan[2]
[1]Assistant Professor, Institute of Insurance and Risk Management, Gachibowli, Hyderabad
[2]Professor, Nagpur

Abstract: The scalability, adaptability, and security of traditional centralized access control mechanisms are severely limited as Internet of Things (IoT) ecosystems grow to billions of linked devices. In order to enable adaptive and fine-grained authorization, this work suggests a decentralized multi-layer architecture that combines Context-Aware Access Control (CAAC), Attribute-Based Access Control (ABAC), and a semantic Long Short-Term Memory (LSTM) prediction model. The system integrates contextual intelligence processing, consortium blockchain-based policy validation via the Raft consensus protocol, and edge-level preliminary authentication. The framework maintains distributed trust and minimal verification delay while enabling high transaction throughput. Semantic prediction of environmental circumstances reduces computational overhead and improves resilience to replay and interception assaults, according to experimental data. For large-scale IoT environments, the suggested method effectively strikes a balance between scalability, security, and adaptability.

Keywords: IoT Security; Context-Aware Access Control; ABAC; Consortium Blockchain; Hyperledger Fabric; Raft Consensus; Semantic LSTM; Decentralized Authentication.

I. INTRODUCTION

The amount of sensitive data shared by diverse and resource-constrained IoT devices has dramatically expanded due to the quick development of Smart Cities and Industry 4.0 infrastructures. These settings require access control systems that are safe, scalable, and flexible enough to function in changing contexts.

However, conventional methods like Role-Based Access Control (RBAC) lack the adaptability needed to take into account constantly shifting environmental characteristics like device location, time limitations, and behavioral patterns. Static role assignments are insufficient to capture fine-grained contextual modifications that directly affect authorization choices in massively distributed IoT ecosystems. [1][2].

Additionally, centralized access control architectures create a crucial Single Point of Failure (SPF), leaving systems open to insider threats, denial-of-service assaults, and widespread compromise. Centralized identity management and policy enforcement systems find it difficult to maintain both security resilience and performance efficiency as IoT networks grow. [3][4]. These drawbacks emphasize the necessity of predictive, context-aware, decentralized security frameworks that can provide dynamic authorization in distributed settings.

The suggested approach has three fundamental elements to address these issues:

1) Decentralized Identity Administration: In order to provide distributed trust, unchangeable audit trails, and tamper-resistant policy enforcement, a consortium Blockchain architecture is used to do away with the need for centralized authorities. [5].

2) Contextual Intelligence via CAAC Based on Smart Contracts: In order to make fine-grained authorization decisions that are in line with operational context, a Smart Contract-enabled Context-Aware Access Control (SC-CAAC) mechanism assesses subject qualities, object features, and environmental conditions in real time [6].

3) Semantic LSTM Modeling for Predictive Security: To predict anomalous events, describe temporal environmental behavior patterns, and dynamically enforce least-privilege access regulations, a semantic Long Short-Term Memory (LSTM) network is employed [7].

The approach seeks to improve adaptive security enforcement in large-scale IoT ecosystems while overcoming scalability obstacles by fusing decentralized trust management with contextual intelligence and predictive analytics. [8].

A. Technical Input

The following is a summary of this work's main technical contributions:

1) Decentralized Architecture with Multiple Tiers: Blockchain-based trust management, policy governance, contextual intelligence processing, and edge-level authentication are all divided into a hierarchical four-tier framework. Single points of failure are removed, system-wide attack surfaces are decreased, and scalability is enhanced by this architectural breakdown.
2) Context-Aware Dynamic Access Control (CAAC): To include predicted semantic insights and real-time environmental characteristics in authorization choices, an integrated ABAC–CAAC model is created. Beyond static role-based procedures, this technique allows for adaptive, fine-grained access control [9][10].
3) Risk Prediction Using Semantic LSTM: To simulate environmental behaviors and temporal access patterns, a lightweight LSTM-based prediction module is presented. Under changing operational conditions, the model dynamically applies least-privilege principles and enables proactive risk assessment. [11].
4) Framework for Tokenized Permission Management: Access rights are managed as verifiable digital assets through a token mechanism powered by smart contracts. In a decentralized trust context, this approach guarantees traceability, revocability, and tamper-resistant audit recording [12][13].
5) Raft-Based Consensus Integration Optimization: To enable deterministic transaction validation, high throughput, and low latency appropriate for large-scale IoT implementations, a consortium Blockchain network adopts an improved clustered Raft consensus configuration [14][15][16].

When taken as a whole, these contributions create a framework for secure, scalable, and adaptive access control that can handle the security and performance issues that arise in decentralized IoT ecosystems**.**

II. SYSTEM ARCHITECTURE SUGGESTION

A. Principles of Architectural Design

Large-scale IoT ecosystems provide inherent scalability, adaptability, and trust concerns that are intended to be addressed by the suggested system architecture. Four basic design principles—zero-trust enforcement, separation of operational planes, least-privilege authorization, and distributed trust management—direct the framework's tiered decomposition approach, as shown in Fig. 2.2.

First, no entity—device, user, or node—is implicitly trusted in this architecture, which adheres to a Zero-Trust security concept. Every access request is continuously assessed using dynamic risk assessment and contextual characteristics. Therefore, rather than relying on static identification assumptions, authorization decisions are based on real-time verification of subject, object, and environmental conditions. This strategy is especially important in heterogeneous IoT environments where behavioral unpredictability and device mobility are prevalent**.**

Second, the architecture makes sure that the control and data planes are kept apart. In order to lower latency and filter harmful traffic early in the pipeline, edge-layer components carry out contextual pre-processing and preliminary validation. Blockchain-based layers, on the other hand, are in charge of immutable record maintenance, consensus validation, and policy integrity. By avoiding pointless Blockchain transactions, this division improves scalability while maintaining global policy uniformity.

Third, the system uses predictive environmental modeling to operationalize the least privilege principle. Semantic LSTM-driven risk assessment is used to dynamically modify access privileges, guaranteeing that permissions are limited to the minimal extent necessary given the current context. The architecture shifts from reactive authorization to proactive risk reduction by integrating predictive intelligence.

Lastly, the system uses a consortium Blockchain architecture to implement distributed trust management. The architecture decreases vulnerability to centralized compromise and removes single points of failure by decentralizing identity verification, policy enforcement, and transaction validation. Establishing a safe, auditable, and tamper-resistant trust is made possible by the coordination of certificate issuance and policy governance among approved consortium members.

Together, these ideas serve as the structural cornerstone of the suggested multi-tier design, guaranteeing that security, scalability, and adaptability are attained without compromising performance in IoT situations with limited resources.

B. Decentralized Framework with Four Tiers

A structured four-tier architecture is proposed, as shown in Fig. 2-2, to address the issues of scalability, contextual flexibility, and decentralized trust in large-scale IoT networks. Blockchain-based trust enforcement, contextual intelligence processing, device-level operations, and governance control mechanisms are all methodically separated by the framework.

Efficient edge-level pre-authentication, dynamic risk-aware access decisions via semantic LSTM modeling, and immutable policy verification via consortium Blockchain infrastructure are all made possible by this layered decomposition. The suggested architecture ensures fine-grained, context-aware authorization and auditable permission management while removing single points of failure by dividing duties among logically distinct levels.

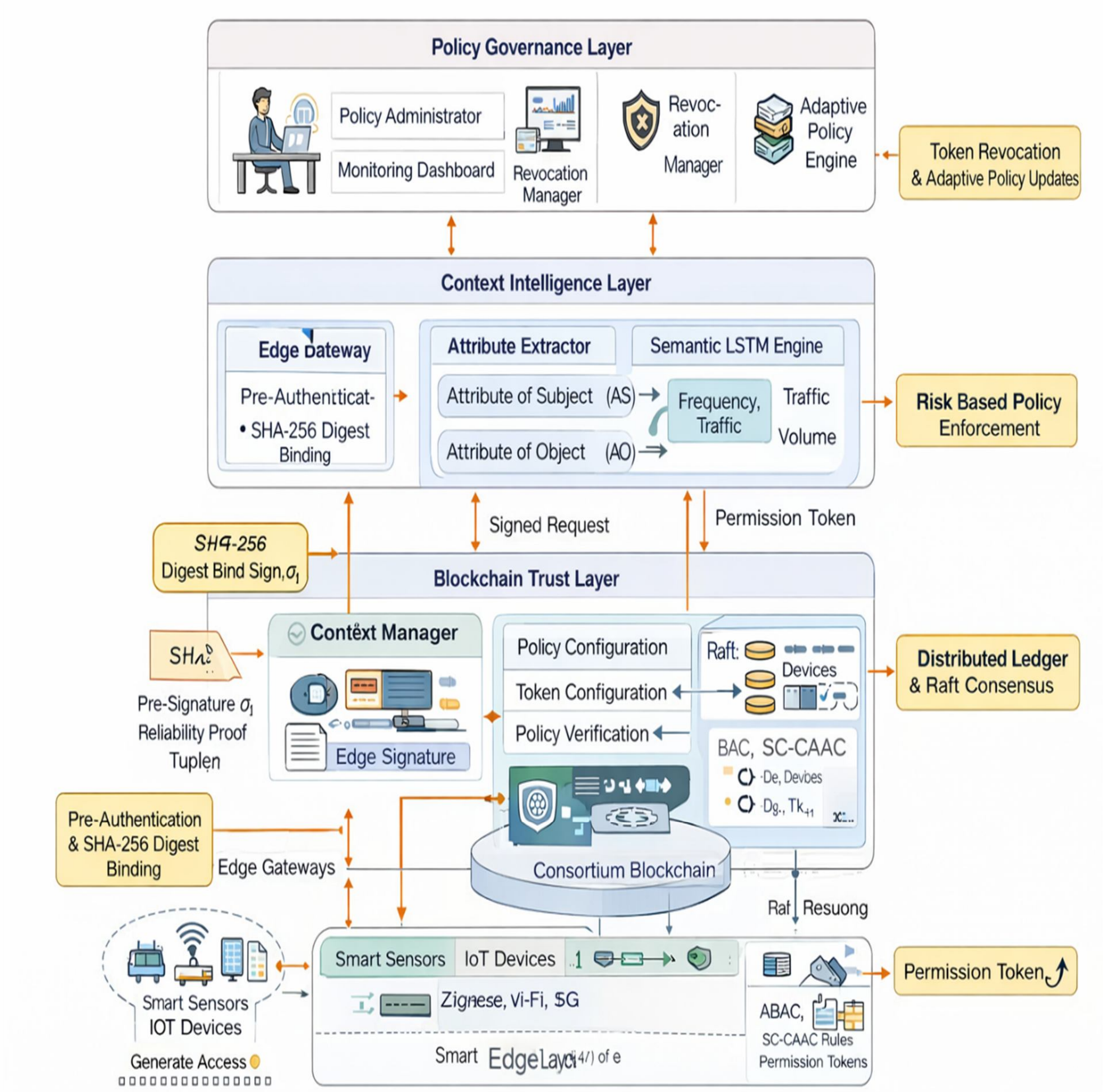

Figure 2.2. Proposed Four-Tier Decentralized Framework

Fig. 2.2 demonstrates the interaction flow among architectural tiers and highlights the closed-loop integration between predictive intelligence and Blockchain-based policy enforcement.

1) IoT Edge Layer, Tier 1

Heterogeneous sensors, actuators, embedded controllers, and gateway nodes that communicate via Zigbee, Wi-Fi, or 5G networks make up the IoT Edge Layer, which is the framework's fundamental operating tier. Before interacting with higher-layer trust components, this layer is in charge of starting secure access requests and carrying out initial authentication.

Every device Di creates a signed access request with the following structure:

Reqi = { IDi, Timestamp, ASi, AOi, AEi, σi}, where ASi stands for subject attributes, AOi for object attributes, AEi for environmental attributes, and σi for the digital signature of **the device.** To guarantee message integrity and resistance to manipulation, the request is cryptographically bonded using a SHA-256 digest.

Signatures and timestamps are verified by edge-level pre-authentication methods before being sent to the blockchain. This initial filtering phase lessens the spread of pointless transactions, minimizes replay attempts, and eases network congestion in the distributed ledger. The approach enhances scalability while upholding security assurances by shifting initial validation to the edge.

2) *Context Intelligence Layer, Tier 2*

Adaptive security is introduced via the Context Intelligence Layer using predicted risk assessment and contextual modeling. This tier uses semantic machine learning approaches to bridge the gap between static attribute evaluation and dynamic environmental awareness.

A Context Manager, Attribute Extractor, Semantic LSTM Engine, and Risk Scoring Module make up this layer. Subject, object, and environmental attributes are processed to create a temporal feature vector once the edge layer validates a request.

Xt = [timestamp, frequency, device_id, traffic_volume, geo_location]

A semantic Long Short-Term Memory (LSTM) model that records temporal correlations and behavioral patterns across access events is fed this feature vector. A future environmental state $\hat{A}_E^{T+1}$, which represents expected contextual conditions, is predicted by the model.

After that, a dynamic risk score is calculated:

$$\text{Risk} = f\ (A_S, A_O, A_E)$$

Where a risk aggregation function set by policy is shown by f(·). In order to uphold the least-privilege concept, access permissions are automatically restricted if the calculated risk surpasses a predetermined threshold θ. The system is changed from reactive access validation to proactive security enforcement using this predictive evaluation.

3) *Blockchain Trust Layer, Tier 3*

Distributed consensus, unchangeable policy enforcement, and decentralized verification are all guaranteed by the Blockchain Trust Layer. This tier, which uses a consortium Blockchain architecture, does away with centralized trust authority without sacrificing performance. Three main smart contracts are integrated by the layer: (i) Policy Configuration Contracts for managing rules, (ii) Token Configuration Contracts for issuing and revoking permission tokens, and (iii) Policy Verification Contracts for making authorization choices in real time. The Hyperledger Fabric Certificate Authority (CA) and a CouchDB state database for attribute storage and sophisticated query functionality are examples of supporting elements.

The transaction lifecycle works like this: the Policy Verification Contract assesses the decision logic once an access request and related risk score are submitted.

Decision=Verify (A_S, A_O, A_E, Risk)

A permission token Tk is created and entered onto the distributed ledger if authorization requirements are met. The Raft consensus process, which offers predictable ordering, fault tolerance, and higher throughput than Proof-of-Work (PoW) methods, is used to validate every transaction. This setup maintains auditability and integrity while guaranteeing high transaction rates.

4) *Policy Governance Layer, Tier 4*

Throughout the whole system, the Policy Governance Layer offers compliance management, adaptive control, and supervisory supervision. This tier makes sure that Blockchain-enforced policies and contextual intelligence are always in sync.

A Policy Administrator, Audit Dashboard, Revocation Manager, and Adaptive Policy Engine are essential elements. The Context Intelligence Layer's risk forecasts and behavioral trends are tracked by the governance system. Policy settings are continually modified and coordinated with anomalous trends.

The framework supports a closed-loop adaptation cycle:

Predicted anomaly → Policy update → Smart contract synchronization → Ledger commit.

This feedback-driven architecture enables continuous security refinement while maintaining decentralized integrity. By integrating predictive analytics with Blockchain-based enforcement, the governance layer ensures long-term robustness against evolving threats.

Predicted anomaly → Policy update → Smart contract synchronization → Ledger commit.

C. End-to-End Operational Workflow

The suggested framework's operational workflow unifies governance oversight, blockchain-based authorization, edge validation, and contextual intelligence into a single execution pipeline. The following is a description of the order in which interactions occur across architectural layers.

An IoT device Di first creates an access request with its digital signature, contextual information, and identification. The edge node receives the request and completes first validation. This involves employing cryptographic digest binding to verify the message integrity, timestamp freshness, and digital signature. In order to avoid needless propagation to higher layers, requests that fail these checks are refused locally.

The request is sent to the Context Intelligence Layer when edge-level validation is completed successfully. The Context Manager creates a temporal feature vector for semantic analysis by extracting subject attributes (A_S), object attributes (A_O), and environmental attributes (A_E). The LSTM-based prediction module calculates the likelihood of an environmental anomaly or behavioral deviation by analyzing past access patterns. A dynamic risk score is calculated and appended to the request based on this forecast.

After that, the Blockchain Trust Layer receives the enriched request together with the computed risk value. The Policy Verification Smart Contract analyzes A_S, A_O, A_E, and the corresponding risk score in tandem to assess the decision logic. If the authorization criteria are satisfied, a permission token is issued to the requesting entity; otherwise, the request is denied. The final decision, along with relevant metadata, is recorded as an immutable transaction on the distributed ledger following Raft-based consensus validation.

The Policy Governance Layer then keeps an eye on token consumption patterns, risk variations, and transaction patterns. Adaptive policy changes are triggered and synchronized with smart contracts if anomalous patterns are found, guaranteeing that authorization rules stay in line with changing environmental circumstances.

The system maintains global consistency, auditability, and decentralized trust enforcement throughout the network while achieving low-latency processing at the edge through this distributed and multi-stage workflow.

This distributed pipeline maintains global policy consistency while lowering latency.

III. METHODOLOGY: TRUSTED AUTHENTICATION & DYNAMIC CAAC

This section describes the cryptographic authentication mechanism and the predictive context-aware access control model that collectively enable secure and adaptive authorization in the proposed framework.

A. Two-Way Identity Authentication

A mutual authentication approach is used to neutralize hostile or hacked edge nodes and prevent illegal participation in the network. The suggested method requires bidirectional trust establishment between IoT devices and edge nodes before transaction processing, in contrast to conventional one-way verification systems.

Let Bn be an edge node in the consortium network and Di be an Internet of Things device.

1) Phase of Reliability Certification

The edge node Bn creates a reliability proof tuple Tuplen, which contains its identification parameters and cryptographic credentials, and a pre-signature σi during the first handshake. Within the Blockchain consortium, this pre-signature acts as first proof of the node's authenticity.

Identity Certification Phase

Upon receiving the pre-signature, the device Di verifies the authenticity of the edge node using a bilinear pairing-based verification mechanism defined as:

$$e\ (\sigma_{i1},\ P_{un} + h_{i1}\ .\ PK) = e\ (G,\ G)$$

Where:

- e(·,·) denotes a bilinear map,
- Pun is the public key component of the edge node,
- PKepresents system public parameters,
- hi1 is a hash-derived scalar,
- G is the generator of the cryptographic group.

If the equality holds, the edge node is considered authentic. The device then transmits its primary signature σi^2 for final mutual authentication. Before access requests are sent to the Blockchain layer, this two-way verification method enhances distributed trust, reduces hostile edge participation, and stops impersonation assaults.

B. Learning Semantic Environmental Attributes

The suggested system incorporates a semantic Long Short-Term Memory (LSTM) network for environmental behavior modeling in order to facilitate proactive security enforcement. This predictive component allows for dynamic risk-aware permission based on temporal context evolution, in contrast to static access control systems.

The model's goal is to facilitate adaptive privilege control by estimating the likelihood of abnormal environmental activity linked to access requests.

1) Architecture of LSTM Model

An input layer that receives contextual feature vectors makes up the predictive module.

Temporal dependence modeling with two layered LSTM hidden layers

An output layer that is totally connected

A sigmoid activation function that generates the probability of anomalies

The hidden state is calculated as follows at time step *t*: The computation of the hidden state is:

$$h_t = \sigma\ (W_x x_t + W_h h_{t-1} + b)$$

where:

- X_t is the feature vector at time t.
- h_t is the hidden state,
- Wx and Wh are weight matrices,
- b is the bias term,
- $\sigma(\cdot)$ denotes the nonlinear activation function.

The predicted anomaly probability is then calculated as:

$$y_t = \sigma\ (W_o h_t + b_o)$$

Where:

- X_t: Feature vector at time t
- h_t : Hidden state
- y_t : Probability of anomalous environment

If:

$$y_t > \theta$$

Then access privilege is dynamically reduced.

2) Dynamic Privilege Adjustment

A predefined threshold θ governs adaptive policy enforcement. If:

$$\mathrm{Y}\mathbf{t>\theta}$$

By tightening policy limitations at the smart contract layer, the system dynamically lowers access rights. This guarantees that the least-privilege principle is upheld in situations with increased risk.

The system improves resilience against replay attacks, aberrant access frequency, and behavioral aberrations by switching from reactive anomaly detection to predictive risk mitigation through the use of semantic temporal modeling.

IV. EVALUATION OF EXPERIMENTS

This section assesses the suggested decentralized access control framework's computational efficiency, scalability, and performance. Under actual IoT workload conditions, the experiments were carried out to examine consensus throughput, validation latency, and prediction model overhead.

A. Performance of Consensus

The suggested design uses a Hyperledger Fabric consortium Blockchain network with the Raft consensus protocol. Raft offers crash fault tolerance and predictable leader-based ordering without the computational complexity of Proof-of-Work (PoW) techniques.

Throughput and transaction validation time were assessed under various transaction loads in order to evaluate consensus performance.

Depending on network capacity and transaction complexity, the system can achieve a throughput of 3,000 to 20,000 transactions per second (TPS), according to the testing results. Compared to mainstream Blockchain platforms like Ethereum, which usually show confirmation delays of 15–20 seconds, and Bitcoin, where block confirmation may take up to 10 minutes, this speed is noticeably better.

The following factors are responsible for the suggested architecture's shorter validation time:

- Log replication based on leaders
- The lack of computational mining
- Fabric's effective endorsement policies

These findings show that the consortium-based Raft setup is appropriate for high-frequency IoT authorization requests that need to be processed almost instantly.

B. Overhead in Computation

Experiments with situations containing 60 active digital certificates were carried out to assess computing efficiency. Baseline static access control approaches and the Semantic LSTM-based context evaluation's performance were contrasted.

When compared to traditional non-predictive methods, the suggested predictive model showed a total processing overhead of 203 seconds for the entire evaluation cycle, which is around a 30% decrease in computing cost.

The main reasons for the decrease in overhead are:

- Contextual filtering of unusual requests in the early stages
- Fewer executions of redundant smart contract
- • Contextual preprocessing off-chain before ledger submission

Additionally, the Hyperledger Fabric Certificate Authority (CA), which decentralized certificate issuance, greatly decreased the amount of storage and processing needed for each IoT devices. Devices rely on Blockchain-verified identity validation rather than local certificate repositories, which increases scalability in contexts with limited resources.

V. EXAMINATION OF SECURITY

This section examines how the suggested procedures meet the specified security goals in light of the established threat model.

A. Model of Threat

The suggested framework's security is assessed using a predetermined adversarial model that is compatible with consortium Blockchain-based IoT setups.

1) Adversarial Premises

It is believed that the adversary has the following abilities:

a) Interception at the Network Level : Man-in-the-Middle attacks allow an attacker to monitor, intercept, and alter communication channels between IoT devices and edge nodes.

b) The capacity to replay transactions: It is possible to obtain unauthorized privileges by replaying previously recorded access requests.

c) Attempts to Escalate Privilege: To gain higher permission levels, the attacker could try to alter subject, object, or environmental characteristics.

d) Participation in Partial Networks: A small portion of edge nodes or client devices may be under the attacker's control.

But it's anticipated that the enemy won't:

- Crack common cryptographic primitives like bilinear pairing schemes and SHA-256.
- Have most consortium Blockchain validator nodes compromised (i.e., no 51% attack circumstance).

These assumptions align with practical threat models in permissioned Blockchain environments, where participating nodes are authenticated entities under administrative governance.

2) Security Objectives

The framework seeks to accomplish the following under the specified adversarial model:

a) Access credentials' confidentiality

b) The integrity of requests for access

c) Participating entities' authenticity

d) Non-repudiation of decisions regarding authorization
e) Opposition against the expansion of privileges
f) Removing single points of failure

B. Attack Resistance Analysis

This section examines how the suggested procedures meet the specified security goals in light of the established threat model.

1) Defense Against Replay and Man-in-the-Middle Attacks

Cryptographic digest binding and timestamp verification help prevent man-in-the-middle attacks. Before any further processing, the integrity of the message is verified and each access request is hashed using SHA-256. Replayed transactions are identified and refused if temporal freshness restrictions are broken since every request has a timestamp and is verified at the edge level.

Furthermore, bilinear pairing-based two-way authentication guarantees reciprocal verification between edge nodes and IoT devices. This stops enemies from posing as authentic infrastructure elements.

2) Preventing Privilege Escalation

The joint enforcement of ABAC policies and the UnRedeemed Policy Output (URPO) mechanism included into smart contracts limits efforts at privilege escalation. Verified subject, object, and environmental characteristics are used to deterministically evaluate authorization decisions.

Unauthorized privilege modification is computationally impossible without jeopardizing consensus since access tokens are granted and recorded immutably on the Blockchain. The predictive risk score enforces dynamic least-privilege regulations by further limiting privilege extension in abnormal environmental conditions.5.2.3 Fault Tolerance and Single Points of Failure(SPF) Elimination

Conventional centralized access control systems are susceptible to administrative compromise and service interruptions. The suggested system uses the Raft consensus technique to spread ledger replication and transaction validation among several consortium nodes.

Because distributed leader election and log replication are used to create consensus, system availability is preserved even in the event that a portion of nodes go down. In large-scale IoT implementations, this architectural style improves fault tolerance and eliminates dependency on a centralized authority.

C. Security Implications

The platform offers multilayer security guarantees by combining decentralized ledger enforcement, predictive contextual modeling, and cryptographic authentication. Edge-level validation, context-aware risk assessment, and immutable smart contract execution work together to provide proactive mitigation of emergent behavioral anomalies as well as reactive protection against established risks. All things considered, the security measures maintain scalability and operational efficiency while satisfying the specified threat model assumptions.

VI. CONCLUSION

In order to overcome the shortcomings of conventional access control methods in extensive IoT ecosystems, this article introduced a scalable and context-aware security architecture that combines Blockchain-based trust management with predictive machine learning. The proposed system provides fine-grained, adaptive, and risk-aware authorization choices by merging Attribute-Based Access Control (ABAC) with Context-Aware Access Control (CAAC) and a semantic LSTM-based environmental prediction engine.

Blockchain-based policy verification, contextual intelligence processing, edge-level pre-authentication, and governance control are all divided by the multi-tier decentralized architecture. In contexts with limited resources, this structural deconstruction increases scalability, decreases single points of failure, and boosts operational effectiveness. Adopting a consortium blockchain with Raft consensus guarantees low-latency transaction processing and predictable validation while preserving access record immutability and auditability. Experimental evaluation demonstrates that the proposed framework achieves high throughput and reduced computational overhead compared to conventional centralized and non-contextual methods for controlling access. By dynamically enforcing minimum-permission principles, the integration of semantic environmental prediction strengthens resilience against replay attacks, impersonation attempts, and privilege escalation, hence contributing to proactive risk mitigation.

Overall, the findings show that the suggested method successfully strikes a balance between scalability, security, and adaptability, making it appropriate for use in industrial IoT systems, smart city infrastructures, and other large-scale distributed contexts.

REFERENCES

[1] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, “Trust-based blockchain authorization for IoT,” arXiv preprint arXiv:2104.00832, Apr. 2021.

[2] M. M. Merlec and H. P. In, “SC-CAAC: A smart-contract-based context-aware access control scheme for blockchain-enabled IoT systems,” IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19866–19881, Jun. 2024, doi: 10.1109/JIOT.2024.3371504.

[3] I. Singh and B. Singh, “Access management of IoT devices using access control mechanism and decentralized authentication: A review,” Measurement: Sensors, vol. 25, Art. no. 100591, 2023, doi: 10.1016/j.measen.2022.100591.

[4] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, “SATI: Sidechain-based access control & trust mechanism for IoT networks,” IEEE Transactions on Network and Service Management, vol. 21, no. 5, pp. 5888–5903, Oct. 2024, doi: 10.1109/TNSM.2024.3438621.

[5] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trustchain: Trust management in blockchain and IoT supported supply chains,” in Proc. 2019 IEEE Int. Conf. Blockchain (Blockchain), Jul. 2019, pp. 184–193.

[6] M. Gupta, “Integration of IoT and blockchain for user authentication,” Scientific Journal of Metaverse and Blockchain Technologies, vol. 1, no. 1, pp. 72–81, 2023, doi: 10.36676/sjmbt.v1i1.10.

[7] P. Chinnasamy, B. Vinodhini, V. Praveena, C. Vinothini, and B. B. Sujitha, “Blockchain based access control and data sharing systems for smart devices,” Journal of Physics: Conference Series, vol. 1767, no. 1, Art. no. 012056, 2021, doi: 10.1088/1742-6596/1767/1/012056.

[8] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, “An attribute-based access control model for Internet of Things using Hyperledger Fabric blockchain,” Wireless communications and Mobile Computing, vol. 2022, Art. no. 6926408, 2022, doi: 10.1155/2022/6926408.

[9] A. Z. Ourad, B. Belgacem, and K. Salah, “Using blockchain for IoT access control and authentication management,” in Proc. ICIOT 2018, Lecture Notes in Computer Science, vol. 10972, pp. 150–164, 2018, doi: 10.1007/978-3-319-94370-1_11.

[10] D. Ongaro and J. Ousterhout, “In search of an understandable consensus algorithm (extended version),” Stanford University, Tech. Rep., May 2014.

[11] S. Joshi, S. Stalin, P. K. Shukla, P. K. Shukla, R. Bhatt, R. S. Bhadoria, and B. Tiwari, “Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain,” Wireless Communications and Mobile Computing, vol. 2021, Art. no. 8621230, 2021, doi: 10.1155/2021/8621230.

[12] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, “A blockchain-inspired attribute-based zero-trust access control model for IoT,” Information, vol. 14, no. 2, Art. no. 129, Feb. 2023, doi: 10.3390/info14020129.

[13] W. Jiang, E. Li, W. Zhou, Y. Yang, and T. Luo, “IoT access control model based on blockchain and trusted execution environment,” Processes, vol. 11, no. 3, Art. no. 723, Feb. 2023, doi: 10.3390/pr11030723.

[14] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, “Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices,” Applied Sciences, vol. 10, no. 2, Art. no. 488, Jan. 2020, doi: 10.3390/app10020488.

[15] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, “A novel attribute-based access control scheme using blockchain for IoT,” IEEE Access, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[16] A. Z. Ourad, B. Belgacem, and K. Salah, “Using blockchain for IoT access control and authentication management,” in Proc. Int. Conf. Internet of Things (ICIOT), LNCS 10972, 2018, pp. 150–164, doi: 10.1007/978-3-319-94370-1_11.