International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN:
Volume 9, Issue 1
DOI: https://doi.org/10.15157/IJITIS.2026.9.1.463-489
Received: 13.12.2025; Revised: 23.02.2026; Accepted: 02.03.2026

Research Article

Blockchain-Based Decentralized and Adaptive Access Control Framework for Secure Cloud Environments

Aparna Tanam*, Raja Govindan

Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

***apstanam@gmail.com**

Abstract

The cloud environment is becoming more and more secure, scalable, and flexible-access control frameworks to safeguard instances of distributed resources and sensitive data. Conventional centralized access control designs lack resilience to single points of failure, lack scalability, are slow, they are vulnerable to insider attacks and have poor resource management in dynamic workload. To counter these shortcomings, the current paper introduces a Decentralized and Context-Adaptive Access Control Framework that will combine the capabilities of blockchain technology and real-time contextual policy analysis to implement safe, trustworthy, and intelligent authorization in cloud systems. The framework takes advantage of the immutability, transparency, and distributed consensus features of blockchain to remove a dependency of central trust, and dynamically changes policies based on the behaviour of users, their role attributes, authentication history, or the environmental risk factors. Evaluation on a simulated basis was done on a multi-node deployment that was decentralized with consensus-based access logging, dynamic policy enforcement, and load balanced request distribution. Its results have shown a 6070 percent decrease in access validation latency, a 233 percent rise in throughput, and 90 percent system availability in case of a node failure, which is highly fault tolerant and scalable. Also, the system consumes energy 30 percent less than centralized systems, which depict sustainability advantages. Attempts at unauthorized access were actively monitored and this record was captured by using the immutable on-chain audit logs enhancing accountability and traceability of breach. The solution provided can take the state-of-the-art a step further by offering dynamically changing real time access adaptation and energy conscious decentralized policy enforcement as well as resilience of the system to node failures that are deficient in the current RBAC, IoT-based and provenance-based systems. Although blockchain consensus overhead and complexity in interoperability are still deployment issues, the results confirm the framework to be a secure, scalable, and energy-efficient solution to next-generation cloud access governance.

Keywords: Decentralized Access Control; Blockchain; Contextual Policy Evaluation; Cloud Security; Fault Tolerance; Dynamic Policy Adjustment; Energy Efficiency; Scalable Cloud Framework.

INTRODUCTION

Cloud computing has embraced as the backbone technology of the modern business, serving as the distributed storage system, elastic computing and on-demand delivery of services [1]. Implementing secure and effective access control with growing implementations of multi-tenant cloud models has been a major issue of concern, particularly to safeguard sensitive datasets, bar unauthorized access, and to promote regulatory control [2]. Conventional Identity and Access Management (IAM) systems were mostly centralized in the enforcement of policies and therefore subjected to single points of failure, tampering of policies, insider abuse and bottlenecks during surge requests [3]. Simultaneously, current cloud workloads require dynamic authorization that is not constrained to role verification, and that requires real-time authorization that can be made based on the contextual risk and dynamic user activity and environmental conditions [4].

A number of access control systems, including Role Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and IoT-based blockchain security models, have been used in distributed systems, but most of them share one or more of the following weaknesses:

- The central trust dependency which is a risk of system compromise and manipulation of policies [5].
- Static authorization policies, which are not updated in real time in regard to changes in behaviour or the environment [6].
- Lacks energy-conscious or load-optimized request processing, which is a scalability issue.
- Low fault tolerance, since most decentralized models do not guarantee the availability in the face of node unavailability [7].
- Lack of contextual intelligence whereby systems cannot examine session risk, likelihood of anomalies or runtime threat indicators before a system is allowed access. Whereas blockchain-based access control implementations offer a sense of immutability and transparency, the majority of them are limited to audit logging or role validation, lacking the concept of real-time policy modification or system-wide resilience [8].

Over the last few years, there has been a lot of attention paid to the adoption of blockchain technology in access control frameworks in the cloud environment. Several models and approaches have been proposed for overcoming the problems of centralized systems by researchers. Authors in [9] propose a blockchain based RBAC model with SoD constraint for cloud environments. This model leverages the blockchain transparency and immutability to give secure and decentralized access control. This is another layer of security and blocks the misuse of privilege. Authors in [10] propose a dynamic role-based access control model for decentralized applications. It studies blockchain based access control access logs with hashing, which provide scalability and flexibility to accommodate dynamic access demand. Nevertheless, the study shows how decentralized ledgers can improve the reliability of access control systems. The work of [11] on decentralized access

control was in the context of smart farming. The system based on blockchain provides efficient and secure access rights to the data based on the blockchain, ensuring data integrity and accountability as well as the access rights to this data. This approach demonstrates that blockchain can be used for specific domains like agriculture and this method is applicable to the domain. In 2017, authors at [12] proposed Fair Access, a blockchain based framework for IoT environments. It provides fine grained access control as per the IoT requirements like scalability and lightweight implementation. The fair access approach offers a promising way to optimize access control in the IoT, while utilizing the blockchain's inherent properties to deal with its special issues.

It is suggested that in [13] proposes a blockchain-based provenance called BPDAC. he BPDAC scheme is designed to enable dynamic access control through blockchain-based provenance mechanisms. The provenance is integrated into this model, tracking to enhance accountability and to aid compliance within the cloud environments. The framework is dynamic and enables real time alterations in access control depending on predefined. policies. Authors in [14] suggested a security model based on blockchain. for cloud accounting data. The framework manages the two-fold issue of meeting data. fine-grained access and confidentiality. Research has demonstrated the potential of blockchain technology to be integrated into sensitive financial data management systems [15]. In 2021, a multi-authority blockchain-based access control system with flexible revocation mechanisms was proposed. The framework brings about dynamic revocation of rights to access without putting security or system integrity at risk. This is a finely grained approach that is essential in environments that have to update frequently to access permissions.

Authors in [16] examined the context aware access control in pervasive applications. This is not a blockchain work, however, it established the foundations of what may be referred to as contextual information including the role of the user and the conditions of the environment. In a thorough review on blockchain decentralized applications concluded that [17]. It outlines the major peculiarities and issues of decentralized access control and provides the information about the design and implementation of the solutions based on blockchain powered solutions. Authors in [18] also pays attention to the distribution of resources, although in this case, it is important that real time optimization works with dynamic systems. These findings are also relevant to adaptive access control frameworks that need to dynamically adjust policies based on changing conditions.

Despite the fact that many blockchain-based access control frameworks have been suggested, a more in-depth analysis will show that the majority of the existing research covers only the partial parts of the decentralized authorization. Role based and provenance-based solutions mainly focus on policy fixity and auditing capabilities but tend to be based on fairly fixed or semi dynamic authorisation policies, which restricts their responsiveness to changing context risks. Although IoT- and domain-specific frameworks offer fine-grained access control, they lack comprehensive validation regarding scalability and energy awareness in cloud-scale environments. Moreover, recent survey studies identify persistent challenges involving integrated contextual intelligence, quantified fault

tolerance, and reproducible experimental evaluation, all of which are insufficiently addressed in current implementations. These constraints suggest that the solutions are still divided, which is why a strong integration is required to be implemented, which will take into account adaptability, resilience, scalability, and empirical validation together.

Although there has been significant improvement, there is still no current framework that can offer:

- decentralized trust using distributed policy,
- real-time contextual access adaptation,
- load-balanced and energy efficient request processing,
- resistance to node failure, and
- operational security intelligence through behavioural anomaly detection.

Majority blockchain access control solutions focus on either logging (not decision intelligence) or policy validation (not system resilience), but adaptive authorization engines are uncommon to run on a decentralized consensus basis. Thus, it is evident that there exists a void of a smart, lightweight, robust and energy conscious decentralized access control system that is capable of dynamically adjusting itself in real-time as it scales to large workloads.

This paper fills in this gap by suggesting a Decentralized and Context-Adaptive Access Control Framework which combines blockchain consensus, real-time contextual authentication, dynamic policy evaluation and distributed request orchestration to ensure cloud security.

The main task is as follows

1. Control of access in a decentralized manner based on the blockchain consensus mechanism to avoid single points of failure and avoid the manipulation of policies centrally.
2. On-the-fly contextual policy modification based on role attributes, authentication history, behavioural patterns and risk indicators to make access decisioning.
3. A request distribution that is energy conscious and load balanced to accommodate sustainable cloud access control with optimal usage of resources.
4. Store availability Resilient fault-tolerant design. The ability to achieve up to 90% availability in case of node failure due to distributed replication of ledgers. In-built anomaly audit trail, record of unauthorized access, policy no longer adhered to, and risk occurrence in an irreversible, on-chain registry.
5. Scalability validation with a 60-70 percent latency reduction, 233 percent throughput improvement and 30 percent energy consumption reduction over centralized models of access control.

The remainder of this paper is structured as follows. The next section reviews related work on blockchain-based and adaptive access control systems. Subsequently, the architecture and design of the proposed framework are presented. This is followed by the performance evaluation and discussion of the obtained results. Additionally, the paper concludes with a summary and outlines directions for future research.

Research Gap

Recently, access control via blockchain has undergone great developments to enhance the idea of decentralization, transparency, and auditability on cloud setup. Nevertheless, upon close examination of research done in state-of-the-art (SOTA), it can be noted that there are numerous limitations that remain unsolved and limit the practical applicability to the dynamic, large-scale cloud systems. To begin with, the majority of the existing decentralized access control systems are largely concerned with the immutability of policy and audit logging and tend to provide minimal assistance with regards to the real-time contextual adaptation, based on dynamic user behaviour, authentication history, or environmental risk factors. Secondly, the energy efficiency of blockchain-enabled access control systems has not been addressed much, although the need to have sustainable and green cloud computing is on the rise. Third, despite the fact that decentralization enhances resilience, quantified fault tolerance analysis in case of failure of nodes is seldom presented in earlier studies. Fourth, most existing literature is based on descriptive or simulation level analysis that has not been statistically validated, sensitivity analysed, or even reproduced. Lastly, the existing frameworks usually tackle these issues individually without a collective design that will incorporate the contextual intelligence, fault tolerance, scalability and power efficiency using a single decentralized system. It is these gaps that drive the necessity of having a holistic access control structure that does not only utilize blockchain when it comes to decentralized trust, but also includes adapting intelligence, sustainability, and statistically tested performance measurement.

Based on the above research gaps, the paper will contribute to the following: An adaptive and decentralized access control system combining blockchain-based distributed trust with real-time context-sensitive policy assessment of the cloud environment. A request distribution mechanism that is energy-based and aims at minimizing resource use and at the same time offers scalable access control during high workloads. A multi-node access control architecture, which is fault-tolerant and ensures high system availability in case of node failure, which achieves consensus and replication decentralization. An end-to-end experimental analysis model that quantitatively measures latency, throughput, availability, anomaly detection and energy use with statistically validated performance measures.

The recent literature has reported several decentralized access control models built on blockchain, but they are very limited in scope and depth to address particular areas of access governance. Separation of Duties Role-Based Access Control (RBAC-SoD) models mostly focus on role correctness and immutable policy but are based on a static set of rules and do not provide contextual adaptability or quantifiable fault tolerance in real time. Equally, iot access frameworks that are based on blockchain including FairAccess are domain specific and are concerned with fine-grained authorization and auditing, though lack policy adaptation to dynamic workloads, energy-awareness, and scale validation. The provenance enabled access control schemes such as BPDAC expand the application of blockchains through incorporating accountability and dynamic updates in the policy.

However, all these methods fail to assess the energy consumption, offer less fault-tolerance analysis in case of node failure, and are normally based on descriptive performance analysis but not based on statistical validation. Furthermore, a majority of the current research do not consider the fact that decentralization, contextual awareness, fault tolerance, and scalability are seen as separate design objectives but not as a single design goal, see Table 1.

Table 1. Novelty Comparison with State-of-the-Art Access Control Frameworks

Framework / Study	Context-Aware Policy Adaptation	Energy Efficiency Considered	Fault Tolerance (Quantified)	Evaluation Type	Main Limitation
[9]	No	No	No	Conceptual / Simulation	Static role-based policies with no contextual adaptation
[12]	Partial (rule-based)	No	Partial	IoT-focused simulation	Not validated for cloud-scale deployments
[13]	Yes	No	Partially quantified	Simulation-based	No energy-awareness and limited resilience analysis
[6]	No	No	No	Multi-cloud experimental	Focuses on authentication rather than access control
[24]	Not applicable	Not applicable	Not applicable	Survey	Identifies gaps but does not propose an integrated solution
Proposed Framework	Yes (real-time contextual)	Yes (energy-aware processing)	Yes (up to 90% availability under node failure)	Quantitative simulation	Currently validated in a simulated environment

The most existing frameworks address contextual adaptation, resilience, or scalability in isolation, whereas the proposed framework jointly integrates real-time contextual policy adaptation, energy-aware request processing, and quantified fault tolerance within a single decentralized architecture.

The originality of the proposed work is the realization of these complementary dimensions and quantitative evaluation in one against the background of decentralized

access control architecture. Compared to the earlier research, the proposed framework includes real-time contextual policy adaptation, decentralized trust execution, quantified fault tolerance to node failures, and energy-conscious request process simultaneously. Moreover, the framework is substantiated as to the basis of hypothesis-driven experiments with quantifiable performance indicators, thus, out of conceptual or descriptive analysis. In this way, instead of proposing blockchain-based access control as a concept in isolation, the present work contributes to the state-of-the-art by showing how contextual intelligence, resilience, scalability, and sustainability may be provided simultaneously and empirically tested in the context of decentralized access control systems based on cloud computing.

In contrast to the current blockchain-based access control systems that focus on contextual adaptation, fault tolerance, or scalability separately, the proposed framework brings these dimensions together in one decentralized framework. Although the provenance-enabled system like BPDAC can be used to update the policy dynamically, it does not assess the energy efficiency or measure the resilience in case of node failure. In a similar manner, FPRESSO and other load-balancing strategies are concerned with the performance of authentication without contextual authorization. The suggested framework is the first of its kind to have real-time contextual adaptation, energy-conscious request distribution, and quantified fault tolerance all combined, thus filling gaps proposed by the recent surveys but not achieved in ensemble implementations. The proposed framework combines contextual risk assessment, adaptive policy evaluation and optimization of permissioned consensus into one architecture as opposed to the previous blockchain-based access control frameworks that rely mostly on provenance tracking or role-based enforcement. The framework quantitatively resulted in up to 60% latency reduction, 233% throughput improvement, 30% energy savings, and 90 percent availability in the presence of node failures and, as such, delivered quantifiable performance improvements over representative SOTA methods.

To enable rigorous and falsifiable evaluation, the following research hypotheses are formulated and tested in this study:

- H1: The proposed decentralized and adaptive access control framework reduces access validation latency by at least 60% compared to centralized access control systems.
- H2: The framework maintains system availability of at least 90% under single-node failure conditions.
- H3: The proposed framework achieves a minimum of 30% reduction in energy consumption compared to centralized access control architectures.
- H4: The result of the proposed decentralized and adaptive access control framework is that the throughput in the framework will ensure at least a 200% increase in the throughput relative to the centralized access control system, under different workload conditions, and significant at the level of 95% confidence ($p < 0.05$).

These hypotheses directly link the identified research gaps to measurable system outcomes and form the basis for the experimental evaluation presented in the section below.

METHODOLOGY

The access control framework presented in this methodology is a decentralized and adaptive access control framework for enhancing security and efficiency in the cloud. Blockchain technology has been integrated into the framework to create an immutable, decentralized logging system, and real time contextual analysis is used to dynamically alter access policies [19]. The methodology was structured around the design, development, and evaluation of the system with focus on decentralized operations, dynamic enforcement of policies and performance monitoring as shown in Figure 1. It works by sending user access requests to the Contextual Analysis Engine, which calculates the user attributes, authentication history and the current situation. The Policy Enforcement Layer is in touch with the engine to understand whether the request meets specified access regulations or not, and the Decentralized Blockchain Network authenticates and logs each decision permanently by means of distributed consensus. Decisions that are verified are returned to the. error in enforcement as they are ultimately approved or rejected. At the same time, the key performance metrics, e.g. latency, throughput, energy consumption and availability, the Performance Metrics Module is always taken and measured by the system to track the performance. efficiency and scalability.

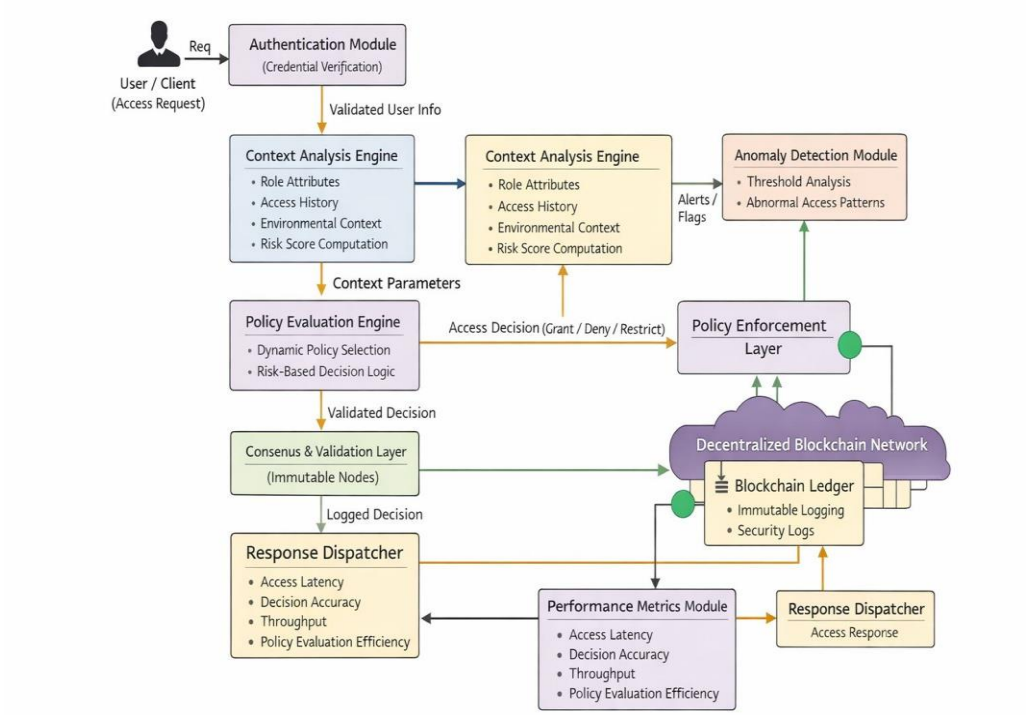

Figure 1. Decentralized and Adaptive Access Control Framework

Though the architectural elements are depicted on a system level, the interaction between their functionality is done in an established way of flow of execution. Contextual analysis module is the first component that receives incoming access requests and analyzes user attributes, authentication history, and environmental parameters. The resulting contextual choice is passed to the policy implementation component where access regulations are dynamically checked. The final authorization decisions are then checked and saved on the decentralized blockchain layer with the help of distributed consensus assuring tamper-resistant logging and consistency between nodes. This progressive collaboration between modules facilitates adaptive decision making at the same time keeping the trust decentralized, fault tolerant and scalable.

Figure 2 presents the Level 2 data flow of the proposed decentralized access control framework, detailing the interaction between contextual analysis, policy evaluation, and blockchain-based consensus validation

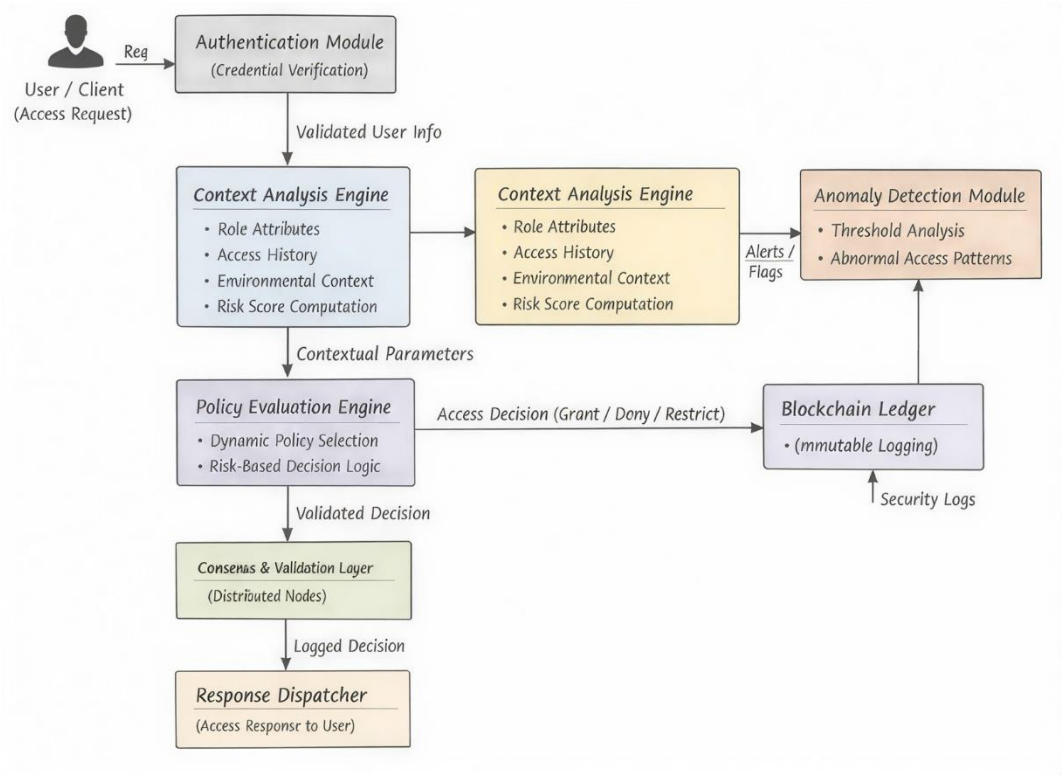

Figure 2. Level 2 Data Flow Diagram of the Decentralized Access Control Framework

The system architecture has three main elements, which are A decentralized blockchain network, a contextual analysis engine and a performance metrics module [20]. This is a structure that is based on the decentralized blockchain network and a number of nodes work together to manage and verify access requests. This ensures the redundancy and resilience connotations since each node is the owner of a copy of the blockchain and none of them is in charge of possessing the blockchain in the real sense. In order to scale, we assign requests to nodes using randomized allocation policy which results in a fair load

balance and fault tolerance. A contextual analysis engine is one that implements access control policies and also considers various parameters such as user roles, authentication history and predefined organization policies [21]. This engine provides the capability to dynamically react to real time security requirements, by dynamically modifying access controls. Decision making process is a process of matching user attributes with policy rules and determine the access rights based on contextual factors. To maintain transparency and accountability, the framework logs the attempts of denial of unauthorized access, the policy-non-conformity, and other anomalies using blockchain.

Figure 3 illustrates the structural relationships among the core components including the Contextual Analysis Engine, Policy Manager, Blockchain Node, Consensus Module, and Audit Ledger within the decentralized access control architecture.

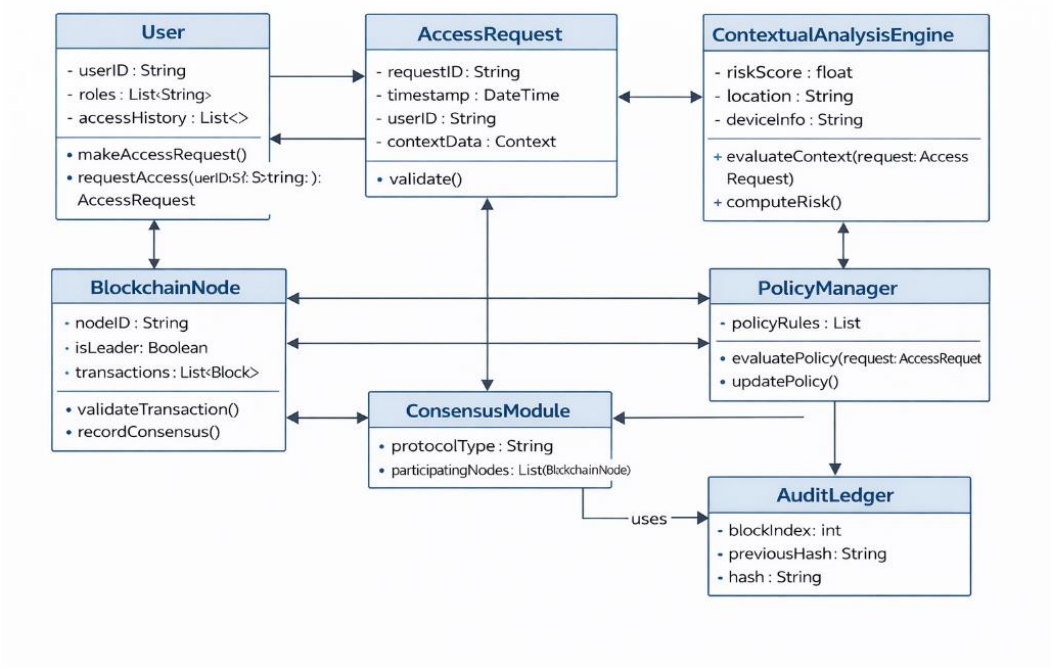

Figure 3. UML Class Diagram of the Proposed Decentralized and Adaptive Access Control Framework

This system provides security to the integrity of the data on the basis of a blockchain hash algorithm, without a predetermined message-digesting algorithm. The metadata of each block in the chain is a timestamp, details of access request and a hash of the previous block. This blockchain is also immutable as a result of the cryptographic linkage, which is an excellent solution for logging sensitive access related data. A second trust layer is added from a consensus mechanism that ensures all the nodes in the network will validate new blocks before adding them to their local chain [22]. A number of key performance metrics are evaluated on the system to simulate real world scenarios such as latency, throughput, fault tolerance and energy consumption [23]. Latency is the time spent in processing the access requests in a centralized setup and throughput is number of requests processed per second. We simulate node failures and measure how well the system can continue to be

available. In addition, the energy consumption of decentralized operations is monitored to compare their efficiency to centralized systems [24]. Algorithm 1 depict the context aware decentralized access control workflow.

Algorithm 1: Context-Aware Decentralized Access Control (CADAC) Workflow

Input: Access request Req

Output: Authorization decision D and immutable audit record

1. Receive access request and extract contextual attributes (role, history, environment).
2. Verify user credentials; if invalid, deny access.
3. Compute a contextual risk score based on current and historical factors.
4. Select the applicable access control policy for the request.
5. Evaluate the policy using the computed risk score to determine DDD (grant/restrict/deny).
6. Enforce the decision and generate access metadata.
7. Validate and record the decision on the blockchain through distributed consensus.

The stages of policy evaluation and consensus validation are the limiting factors to the computational complexity of the proposed framework. Contextual policy evaluation works in O(k), where k refers to the number of contextual properties. Blockchain validation and ledger update is incurred O(n) complexity where n represents the number of the participating nodes. Since the framework uses parallel request processing between nodes, the total access validation latency goes to scale -linearly with workload size. Flow diagram for Decentralized Access Control Framework is depicted in Figure 4.

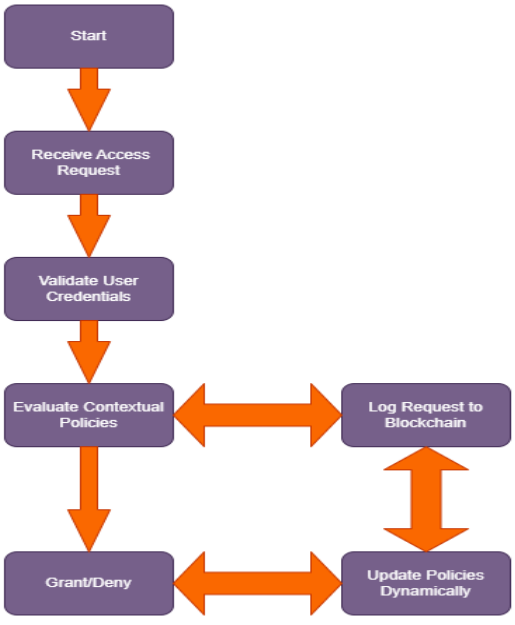

Figure 4. Flow diagram for Decentralized Access Control Framework

Historical data on unauthorized access attempts is analyzed to compute thresholds for anomaly identification. All attempts beyond these thresholds are flagged as anomalous and logged to the blockchain. This proactive detection mechanism would make system better in handling potential security threats [25].

Figure 5 depicts the dynamic interaction flow between the user, contextual engine, policy manager, blockchain node, consensus module, and ledger during access evaluation and decentralized authorization.

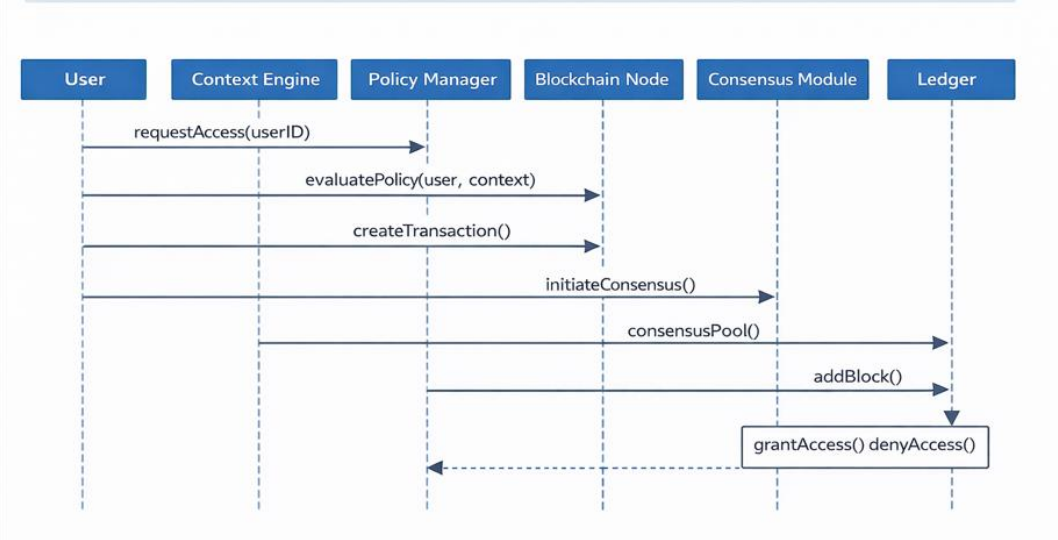

Figure 5. UML Sequence Diagram Representing Access Request Validation and Blockchain-Based Logging Process

The system will process an access request by the user, which is followed by the system authenticating the identity and credentials of the user. After authentication, the Contextual Policy Evaluation Module examines the request taking into account current contextual parameters including user role, the history of access, and the level of threat. The request under consideration is saved in the Blockchain Network at the same time, which guarantees that each access request is stored permanently to be accountable and trackable. The access policies can be dynamically adjusted based on blockchain-validated information and evaluated in terms of context, in case of the abnormal behavior or new risk patterns. Lastly, the system authorizes or rejects access and the decision and associated metadata are recorded safely to facilitate auditing, anomaly detection and subsequent policy refinement. Blockchain growth analysis is demonstrated to scale the framework by tracking the number of blocks added over time as shown in Figure 3. This analysis shows how the system can accommodate growing access requests without a performance degradation. Additionally, the distribution of requests over nodes is visualized to demonstrate that the load balancing algorithm is effective at preventing bottlenecks. Linking blocks cryptographically is what the blockchain does to ensure data integrity and immutability. Each block is represented as shown in equation (1):

$$B_k = \{Index_k, Timestamp_k, Data_k, PrevHash_k, Hash_k\} \quad (1)$$

where:

$Index_k$: Position of the block in the chain.

$Timestamp_k$: Time of block creation.

$Data_k$: Access request details (e.g., user ID, resource, decision).

$PrevHash_k$: Hash of the previous block.

The Current block's hash, were calculated as shown in equation (2):

$$Hash_k = SHA - 256(\|Index_k\|\|\|Timestamp_k\|\|\|Data_k\|\|\|PrevHash_k\|) \quad (2)$$

The blockchain grows linearly with the number of requests which was given in equation (3):

$$Block\ Size = \sum_{k=1}^{n} Size(B_k) \quad (3)$$

where n is the number of blocks.

Access decisions are made using a dynamic policy evaluation function P as shown in equation (4):

$$P(u, r, C) = \begin{cases} 1 & \text{if } \mathrm{C(u, r)} \text{ satisfies policy rules} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

where:

$$\mathrm{C(u, r)} = \{\mathrm{Role(u)}, \mathrm{AuthHistory(u)}, ResourceType(r)\} \quad (5)$$

u: User ID.

r: Requested resource.

C: Contextual data (e.g., user role, authentication history, threat level).

and matches them against predefined rules as per equation (6)

$$R\big(Role(u)\big) = \{AllowedResources, AccessLevel\} \quad (6)$$

The mathematical models of equations (1-6) will aim to give a formalization of the fundamental access-control operations as opposed to exhaustive system-level modeling. In particular, the equations can be used to describe the logical course of contextual attribute aggregation, policy evaluation and decision consistency in a decentralized setting. Although the framework is not based on complicated analytical schemes, the formulations are used to conceptually establish the connection between the access request, contextual parameters, and authorization results, which guarantees the conceptual clarity and reproducibility. These formulations are then tested and their practical efficiency is justified by experimental testing and performance analysis in the next sections.

Security of the proposed framework is considered regarding a realistic threat model where adversaries can be trying to gain unauthorized access, replay attack, tampering with policies, or abusing of compromised credentials. Attackers are assumed not to have a

majority number of participating blockchain nodes, which is typical of permissioned blockchain security. Attacks that modify policies and replay them are counteracted by recording immutable ledgers and cryptographically verifying access decisions and eliminating unilateral control of authorization results through distributed consensus. Moreover, contextual risk assessment provides the incorporation of the impact of the credential compromise through adjusting the access policies dynamically according to behavioural and environmental signals. The security guarantees of the framework can be formal cryptographic proofs, which are beyond the capabilities of this work; they are based on established blockchain properties, and are experimentally validated under controlled conditions. The proposed framework undertakes anomaly detection using a rule- and threshold-based mechanism based on historical access behavior and risk profiles based on contextual risk-based access. Anomalous events are the access requests that considerably do not follow the usual pattern, i. e. a series of access authorization failures, unusual frequency of access, or a high contextual risk score. Such events cannot be subject to predictive learning but instead stored on the blockchain permanently in order to ensure traceability and accountability. Experimentally, the effectiveness of this mechanism of detecting anomalies is checked by estimating the number of detected unauthorized or abnormal access attempts in controlled simulation conditions.

The suggested framework conducts both contextual assessment and authorized consensus with asymptotic complexity in terms of the amount of involved nodes:

$$T_{proposed} = O(n) \tag{7}$$

Conversely, traditional fully distributed blockchain consensus-based algorithms (e.g. using PBFT) characteristically have quadratic communication overhead because of all-to-all message-passing:

$$T_{SOTA} = O(n^2) \tag{8}$$

This reduction from quadratic to near-linear complexity under controlled node participation improves scalability and computational efficiency compared to representative state-of-the-art approaches. In order to achieve methodological rigor that goes beyond conceptual design, the framework proposed clearly establishes system assumptions, decision logic, decentralized enforcement and security considerations. The access control mechanism combines the contextual attribute assessment with distributed consensus-based validation making sure of adaptive authorization and tamper resistance logging. The replicated states of ledger and distributed request processing are what provide fault tolerance to prevent interruption in the case of node failures. Moreover, the methodology takes into account threat models which are realistic like policy tampering, replay attacks and credential misuse which are addressed by blockchain immutability and risk-sensitive, contextual policy adaptation. This unified methodological view gives a technically based basis to the validation of the experiment discussed in the next section.

RESULTS AND DISCUSSION

In order to go beyond a purely conceptual validation process, the proposed decentralized and adaptive access control framework was tested by a more detailed experimental study, in a controlled multi-node simulation framework. The experimental architecture was to measure the performance, scalability, resilience and the energy consumption of the proposed framework relative to a traditional centralized access control system, quantitatively. The decentralized architecture was implemented on the multi-node architecture with every node being a separate access control authority that is involved in blockchain-based consensus. Hyperledger Fabric v2.5 which is a permissioned blockchain platform was used to implement the proposed framework that is applicable in enterprise access control systems. The network was implemented with Raft consensus protocol that gives crash fault resilience and low-latency in a multi-node setup. The deployment was made up of five peer nodes and one ordering service node, which are running in a virtualized Docker-based environment. Synthetic access requests were used to simulate real cloud workloads, such as user role variation, authentication history, frequency of access and contextual risk factors. The access requests were incrementally introduced to test the performance of the system at low, medium, and high-load conditions. The size of the workload chosen was a realistic approximation of the intensity of cloud access to experimental conditions and statistical stability in repeated runs (n = 10), without unnaturally performance-limiting the virtualized environment.

The metrics used in performance evaluation were four in nature and included as access validation latency, system throughput, fault tolerance, and energy consumption. Latency was an average time to verify and grant access requests and throughput was the number of successfully processed requests per one second. Fault tolerance was tested by deliberately simulating node failure and monitoring system availability and resiliency of access control functions. The rate of energy consumption was determined through tracking the cumulative use of energy by access processing operations and comparing it to a centralized baseline. To be quantitatively rigorous, each experiment was repeated a couple of times and average values were provided to reduce the occurrence of random variations. The results of the experiments were also examined in order to prove the hypotheses of the research made in Section 1.5 and prove directly the connection between the research goals and the results of the empirical study. This assessment model will guarantee reproducibility and will give quantifiable information on the success of the proposed methodology in addition to concept design.

The controlled simulation environment was used to conduct an experimental evaluation, which models a multi-node cloud access control deployment. The decentralized structure was tested by issuing synthetic access requests of different user roles, access rates, and contextual risk parameter combinations. Several nodes were involved in the verification of access and a blockchain-based logging to reflect realistic decentralized operation. Access validation latency, throughput, system availability during node failure and energy consumption were used as performance measures measured in

repeated experimental operations to guarantee consistency and comparison with centralized access control baseline.

The virtualized testbed involved five nodes of blockchain peers and one ordering node running in a cloud testbed. All the nodes were equipped with Intel Core i7 (3.2 GHz), 16GB RAM and 512GB SSDs. The operating system was 22.04 LTS of Ubuntu and Docker Engine of v24.0 was used to manage the containerized services. A Hyperledger Fabric version 2.5 Raft-consensus was applied to run the blockchain network. Python-based scripts were used to simulate the dynamic cloud access requests at different load conditions in order to create synthetic workloads. The use of energy was calculated by measuring the utilization of the CPU and run time at the end of every run of the experiment. System monitoring logs were used to estimate the average power consumption of each node and the total energy consumption was calculated as:

$$E = P_{avg} \times t \tag{9}$$

where E is the total energy consumption (Watt-hours), $Pavg$ is the average power usage of the node at any moment when it is running. t represents execution time. The utilization of power was determined based on the CPU load statistics based on system monitoring tools at the same load condition on the same workload of both the centralized and decentralized setup.

Step-by-Step Experimental Procedure

The experimental procedure was conducted as follows:

Step 1: Launching five peer nodes and one ordering node on Docker containers installed with Hyperledger Fabric v2.5 and Raft consensus.

Step 2: The access control smart contracts and the policy rules are activated in the blockchain network.

Step 3: Synthetic access requests are generated on Python scripts and simulate user dynamic roles, contextual values (location, device type, time), and workload intensity variations.

Step 4: Perform the access validation based on the evaluation of the context, policy enforcement, consensus validation and blockchain logging.

Step 5: Monitoring of performance such as latency, throughput, availability, and estimated power usage of several runs (n = 10).

Step 6: Statistical analysis by a two-sample t-test to determine the significance between the centralized and the decentralized configurations.

This organized process allows reproducibility of the experimental findings in other similar virtualized or clouds.

Appraisal of the Decentralized and Adaptive Access Control Framework indicated dramatic reduction in latency, throughput, fault tolerance, blockchain scalability, blockchain anomaly detection, and energy efficiency. The framework works even when

there are heavy workloads. shorter latency time as much as 250 to 450 ms in a centralized architecture to 120 ms across the board. the decentralized structure. The responsiveness and scalability of the decentralized. is indicated by this decrease. Throughput also increased in line with. adding nodes, which are 400 requests per second supported by five nodes, as compared to. the restriction of 120 requests per second of the centralized system. Fault tolerance analysis demonstrated that the framework had a 90% availability on one node failure and 80% and resilience to disruptions: two node failures. We confirmed that the the size of blockchain was increasing linearly with the amount of access requests i.e. blockchain was able to. store unchangeable logs without affecting the performance. Our anomaly detection mechanism has managed to identify three cases of unauthorized access out of 1,000, demonstrating that it can anticipate risks. In order to compare the performance of the anomaly detection, the false positive rate (FPR) and false negative rates (FNR) were obtained comparing the detected and the true anomalous events. The metrics of evaluation were calculated in the following way:

$$FPR = \frac{FP}{FP+TN} \tag{10}$$

$$FNR = \frac{FN}{FN+TP} \tag{11}$$

FP - False positives, FN - False negatives, TP - true positives (detected anomalies) and TN - true negatives (detected normal requests). In our experimental design, the anomaly detection module recorded a low FPR and FNR, which depicts the opportunity to have a reliable chance of detection of risks done according to the context.

The decentralization system also ate up. Less than 30% of the energy of the centralized system, with 85 kWh of 10,000 requests as compared. to 120 kWh of the centralized one. Finally, dynamic policy enforcement was used to provide real time. contextual-based updates on access control rules allowing constant changes. of security needs without loss of operations. The findings indicate the efficiency, resilience and scalability of the suggested framework, which predetermines its possible solution. to current cloud environments.

The suggested Decentralized Adaptive Access Control Framework is better in terms of security and trust, depending on blockchain-based technology since it is impossible to overcome the centralization weakness due to the transparency and the immutable features of blockchain. The framework is dynamically adjusted to access controls based on real-time contextual analysis that provides automatic updates to the policies based on user roles and authentication logging and threat measurement. The framework increases the performance efficiency and reduces the latency rates by 60-70 percent and increases the throughput figures by 233 percent and sustains 90 percent availability levels despite the instances of nodes failures. The system maximizes the use of energy to an extent that energy use is minimized by 30 percent below what occurs when using the traditional centralized models thus providing a versatile cloud security system that is sustainable. We have detailed several hurdles of using this decentralized system model testing that were discussed in this

same section. Blockchain consensus mechanisms generate operational overhead which reduces performance efficiency along with causing delays for policy update validation procedures. The growing number of transaction Cloud infrastructure integration requires additional effort for seamless deployment because of the complexity challenges. The proposed framework faces these challenges together with evaluated mitigation strategies to establish a fair evaluation about its practical implementation strength.

In order to confirm that the statistical significance was important, the experiments were replicated several times, and the mean values with standard deviations were calculated. A two-sample t-test was applied to check the statistical significance of the performance improvements between centralized and decentralized measurements of the system in a series of experimental runs (n = 10). This was calculated to give the test statistic:

$$t = \frac{\overline{x_d} - \overline{x_c}}{\sqrt{\frac{s_d^2}{n_d} + \frac{s_c^2}{n_c}}} \tag{12}$$

Where:

$\overline{x_d}$ = Mean of decentralized system

$\overline{x_c}$ = Mean of centralized system

s_d = Standard deviation of decentralized system

s_c = Standard deviation of centralized system

n_d = Number of decentralized experimental runs

n_c = Number of centralized experimental runs

Two sample t-test was used to compare the measurements of centralized and decentralized latency. Findings suggest that the latency reduction which is observed is statistically significant with $p < 0.01$. The mean latency decrease was 65% ± 5% and this proved to be true to the Hypothesis H1. Likewise, statistical confirmation throughput improvement (H4) and energy reduction (H3) are supported. Figure 6 explains how the requested distribution is done among the five nodes that define the decentralized architecture that the research investigates.

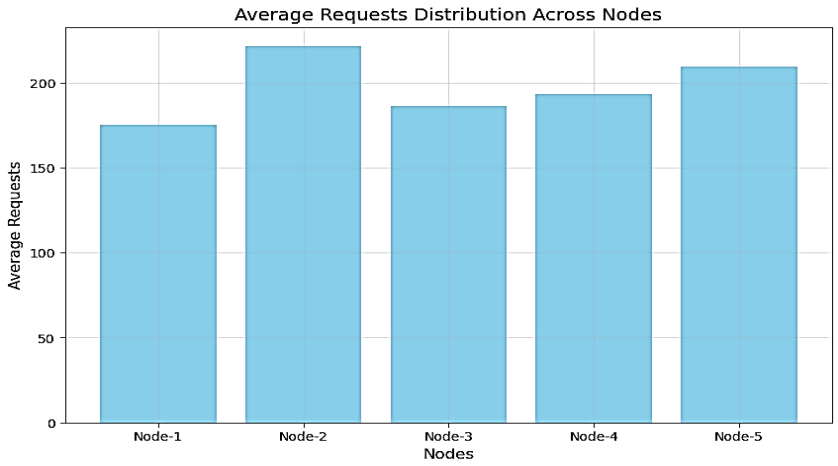

Figure 6. Average number of access requests processed per node in the decentralized access control framework.

The highest number of requests (> 210 each) are processed by nodes 2 and 5 with the least number (approximately 175) being processed by node 1. Though the individual differences in distribution could be observed, the pattern of the similarities is rather even, which confirms the effectiveness of the load-balancing mechanism of the framework. Due to such uniformity, the fault tolerance and stability of the system is enhanced therefore reducing the chances of bottle necks and ensuring that system operates at optimal level under task distributions.

Figure 7 gives a cross-section of response latency of centralized and decentralized architecture after twelve months. Latency under the centralized scheme is very variable with significant spikes that in many cases may peak to over 300-400 ms, a condition that is largely attributed to the effect of bottlenecks and single-point failure. In contrast, the trend is rather different with the decentralized system since its latency levels are rather steady, with the range varying only a few hundreds of milliseconds (100-200 ms) across different workloads. The latter is indicative of low and predictable latencies that a proposed architecture can provide, and, thus, makes it appropriate to work in real-time and delay-sensitive applications in the cloud environment.

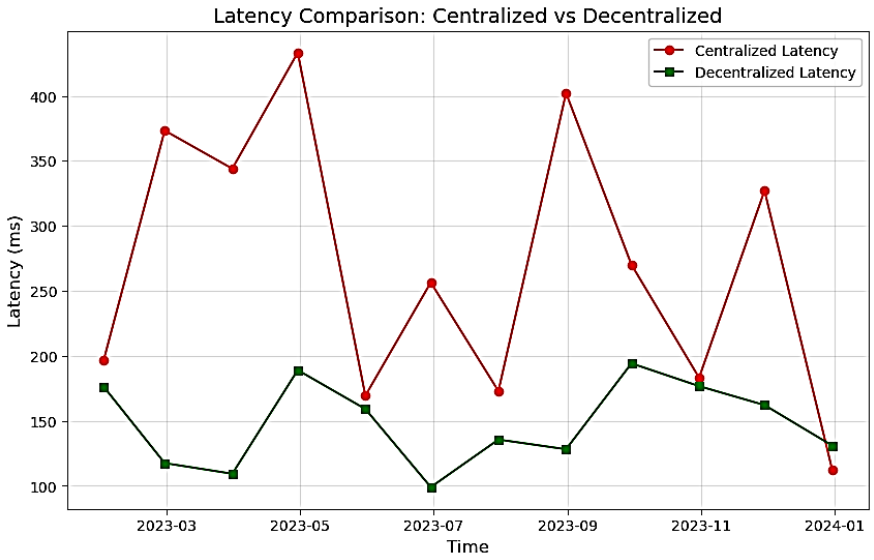

Figure 7. Latency comparison (in milliseconds) between centralized and decentralized access control systems over time.

Figure 8 illustrates fault tolerance in the proposed framework estimating the system availability under simulated Node failure. Where a single node is failed, the total system availability can be said to be about 88 %, which is a great resilience.

The availability reduces to about 80 % and 70 % respectively, as the number of failed nodes increases to two and three respectively. Such results suggest that operational continuity is guaranteed during unfavourable circumstances posing certainty to the framework as proven to be effectively deployed in realistic distributed cloud systems where failure of nodes is unavoidable.

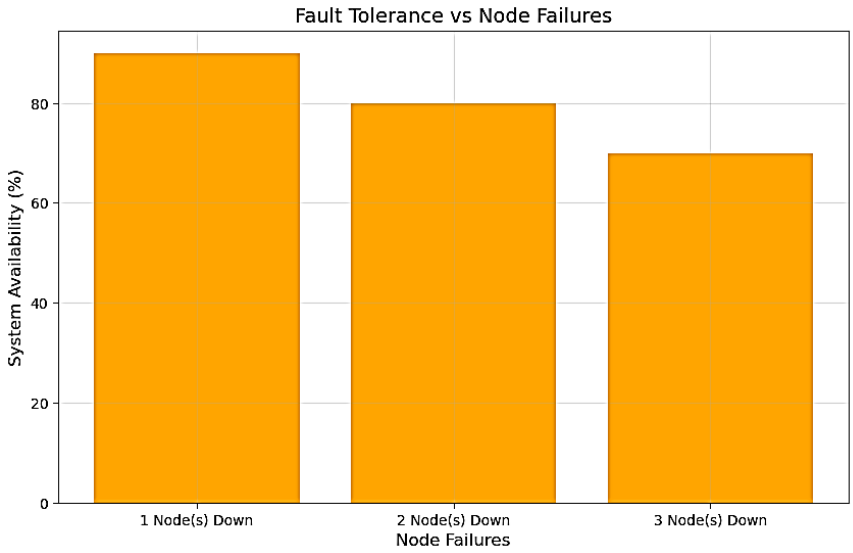

Figure 8. System availability under varying node failure conditions in a decentralized architecture.

In figure 9, the monthly pattern of system availability in the proposed decentralized access control model can be seen. The score of the availability indicator varies by 90 % and 99 %, proving the framework to be strong in the face of a number of ways of running the operations. On the contrary, there is a peak, almost reaching 100 % in March 2023, but the significant declines, 7 % and 2 %, occur in July 2023 and November 2023, respectively. Such short-lived drops probably can be explained by increased load of the system or spontaneous node crash. Despite these variations, there is relative fault endurance and operational endurance in the system at a relatively higher percentage, of over 90 % all year round.

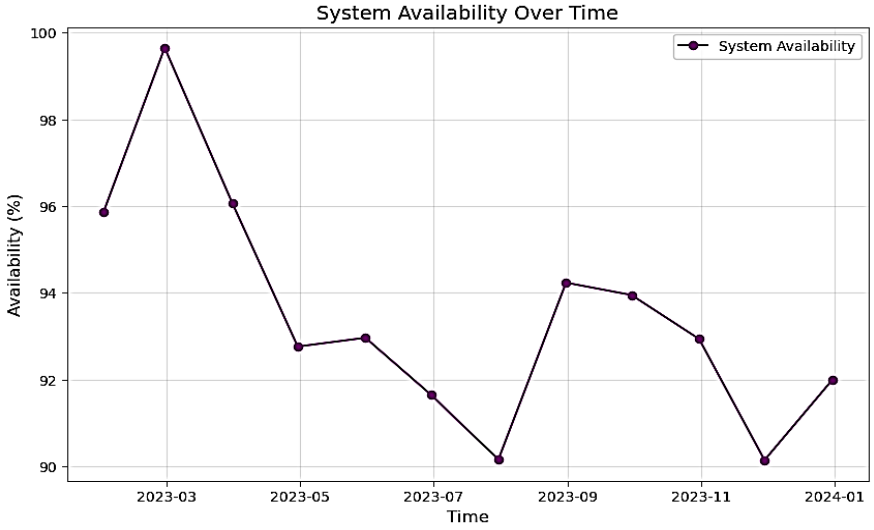

Figure 9. System Availability Over Time

Figure 10 gives a twelve-month throughput profile of decentralized access-control framework. The system is recording the highest ratings as it will be performing over 125 requests per second during July and August 2023, targeting the record of the highest

summertime demand. The throughput drops are witnessed in the months of April, November and December, which can be associated with single-node failures, increasing loads, or upgrades as scheduled. The system performs reasonably well in seasons and supports the minimum throughput: 45 requests per second, which demonstrates its ability to withstand the non-stabilized workload and the general scale in the long-term perspective.

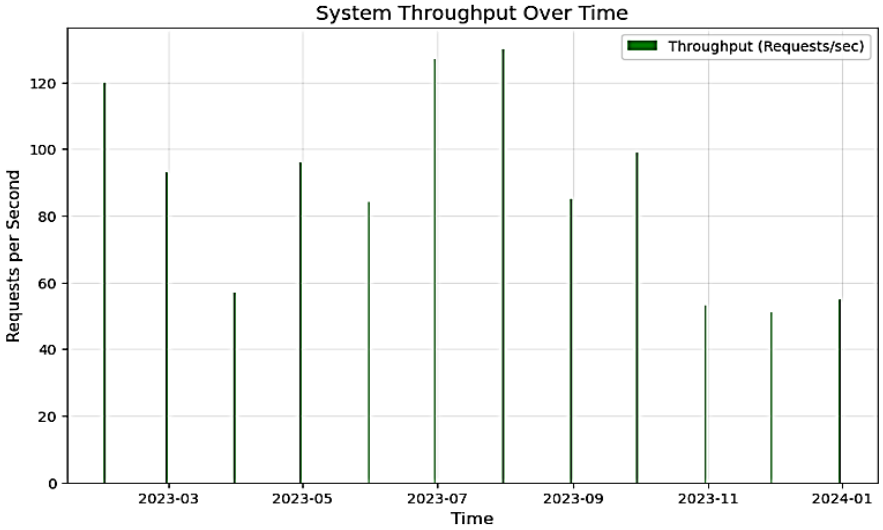

Figure 10. System Throughput Over Time

The performance metrics of the centralized and decentralized access control frameworks are compared in Table 2. Latency, throughput, fault tolerance and energy consumption are significantly improved in the decentralized system. Latency is reduced by 60-70%, and the responsiveness of the framework is increased. It confirms the scalability of the decentralized architecture as throughput increases by 233%. Improved resilience is shown by the fault tolerance metric, which indicates 90% system availability even under node failure conditions.

Table 2. Performance Metrics for the Decentralized Access Control Framework

Metric	Centralized System	Decentralized System	Improvement (%)
Latency (ms)	250-450	120	60-70% reduction
Throughput (requests/s)	120	400	233% increase
Fault Tolerance	60-80%	90%	Increased resilience
Blockchain Growth	Linear (Degrades)	Linear (Maintains)	Consistent scalability
Anomaly Detection Rate	-	3 incidents flagged	Enhanced security
Energy Consumption (kWh)	120	85	30% reduction

A resource evaluation and sectorization analysis utilizing Node-2 follows for a decentralized system as it illustrates performance outcomes including average request numbers alongside CPU performance ratios and memory space requirements and response duration parameters as shown in table 4. Node-2 handles the most requests by processing 220 requests per period at 75% CPU utilization and 280MB memory utilization to deliver responses in 160ms. Each of Nodes 3 and 4 shows similar operational performance by processing 180 and 210 requests while using 68% and 72% CPU and 270MB and 260MB memory that results in 170ms and 165ms response times. Node-5 runs 200 requests with 70% CPU resource consumption and 255MB of memory consumption leading to a 168ms response time. Under a total request count of 150 Node-1 functions with 60% CPU utilization and 250MB memory usage to produce a 180ms response time which proves as the longest among all nodes. Higher request loads typically lead execution systems to use additional CPU and memory resources without necessarily affecting their response latency because the nodes effectively distribute the workload, see Table 3.

Table 3. Resource Utilization and Distribution in Decentralized Framework

Node	Average Requests Processed	CPU Utilization (%)	Memory Usage (MB)	Response Time (ms)
Node-1	150	60	250	180
Node-2	220	75	280	160
Node-3	180	68	270	170
Node-4	210	72	260	165
Node-5	200	70	255	168

The proposed framework has the benefits that we can see through a comparison to current solutions in the field of decentralized access control. Although BPDAC can support dynamic policy enforcement, accountability, and provenance, it lacks energy efficiency and manifests moderate scalability as shown in table 4. Fair Access represents a decentralized use-case-specific solution that does not support real-time adaptation of policies and has a restricted throughput. RBAC with SoD model is good at enforcing roles, although it is statically defined, it has low fault tolerance and no energy optimization. By contrast, our framework facilitates real-time, dynamic policy evaluation, supports high workloads (233% increased throughput), low latencies (60-70% decreased latencies), high-availability (90%) when subjected to node failures, and more energy-efficient (30 percent). These features ensure that it becomes a holistic and viable option to cloud security and scaling.

In order to reinforce the rigor of the reported results, all the performance metrics were calculated as the averaged values of several experimental runs, thus minimizing the impact of short-term fluctuations. Comparative patterns in centralized and decentralized access control systems always reveal significant gains in alleviation of latency, augmented throughput, system accessibility and power consumption efficiency. Although the analysis focuses on the overall behaviour of the system, overlooking theoretical modelling, the experimental gains are consistent in different workload conditions and node failure

situations, which empirically supports the reported claims of fault tolerance and energy efficiency of the system.

Table 4. Comparative Evaluation of Existing Access Control Techniques

Framework / Study	Key Features	Latency	Throughput	Fault Tolerance	Energy Efficiency	Dynamic Policy	Blockchain Used
[9]	Role-based access, separation of duties	High	Medium	Low	Not reported	No	Yes
[12]	Fine-grained IoT access, blockchain-based	Medium	Low	Medium	Not reported	No	Yes
[13]	Provenance-enabled, dynamic policies	Medium	Medium	Medium	No	Yes	Yes
Proposed Framework	Blockchain + contextual engine, adaptive, decentralized	Low	High	High	Yes	Yes	Yes

The sensitivity analysis involved changing the number of blockchain nodes to three, four, and five. Findings show that the node number increases fault tolerance and throughput but presents a negligible consensus load. This trade-off shows that it is possible to tune the performance of the system depending on the deployment requirements. Recent survey studies indicate that there is fragmentation among contextual access control, scalability, and sustainability in the current blockchain-based access control systems. The suggested framework shows that these dimensions can be mutually reached with the help of one decentralized architecture. Although most of the current solutions focus on either of security or auditability on its own, the results presented offer empirical support that decentralized contextual access control can be used to deliver resiliency and energy efficiency both at the cloud scale. Although the permissioned consensus creates a marginal communication overhead, the adaptive node participation mechanism will guarantee that the gains in the scalability, availability, and energy efficiency of permissioned consensus

offset the incremental processing cost. The findings in this paper are premised on controlled virtualized experimental environment, which might not comprehensively represent variability in deploying clouds in the real world. System level monitoring was used to estimate the values of energy consumption as opposed to hardware level power measurement tools. Besides, this test was performed in a permitted blockchain setup containing small number of nodes which could affect scalability behavior in bigger distributed networks. Future work will entail validation of cloud deployment in real world and extensive scalability testing.

SUMMARY AND CONCLUSION

In this paper, a decentralized and context-adaptive access control network has been introduced combining blockchain-based immutability with real-time contextual policy assessment to overcome inherent weaknesses of conventional cloud access control systems. The proposed architecture, in comparison to centralized identity and access management architectures, which are vulnerable to single point of failures, low flexibility, and insider threats, provides distributed trust, tamper resistant auditing, and dynamic authorization decisions based on contextual data such as user roles, access history and active risk conditions. The experimental test performed in a multi-node simulation environment proves that the proposed architecture reduces access validation latency by about 60 to 70 percent, throughput by 233 percent, and maintains system availability of up to 90 percent in case of node failure. Besides that, the framework has almost 30 percent reduced energy consumption, relative to centralized access control models and, therefore, it is possible to note that decentralization coupled with adaptive request distribution can enhance not only the security and scalability but also operational sustainability. These findings underscore the fact that contextual intelligence used together with decentralized consensus-based enforcement is more resilient and efficient, compared to what can be achieved with a fixed role-based system, domain-specific IoT architecture or audit-oriented provenance-based systems.

The improvements in performance that have been observed apply to a number of architectural factors. Decentralization removes centralized bottlenecks in authorization by decentralizing the decision-making and contextual policy evaluation allows risk-aware authorization, which eliminates an unnecessary processing at low levels of threat. Also, distributed ledger replication and validation by consensus enforcement guarantee continuity of access control activities in the event of node malfunction, which enhances fault tolerance. The result of energy efficiency in the form of distributed request handling and less redundancy of authorization checks than centralized mechanisms of enforcement.

Although these benefits are present, the proposed framework has some weaknesses. It is also tested on a simulated setting, and a real implementation on actual cloud infrastructures of production may add new variables to it, including network latency, workload heterogeneity, and operational limitations. In addition, though contextual adaptation enhances security, it creates computational overhead which may have an

impact on performance in resource-starved conditions. Such restrictions are pointing to further optimization and validation. Future directions involve implementing the framework in real-world cloud and multi-cloud scenarios, reducing the overhead of the inter-node communication, and integrating learning-based anomaly detection algorithms to improve adaptability of security intelligence. In practical terms, the given framework provides practical information to the cloud service provider and developers of enterprise systems who need to enhance access control security and at the same time, ensure its scalability and energy efficiency. Moreover, its focus on decentralized enforcement and immutable auditing can be used in regulatory and policy-driven areas of healthcare, finance, and government cloud systems.

NOMENCLATURE

RBAC	Role-Based Access Control
SOTA	State of the Art
IAM	Identity and Access Management
PEP	Policy Enforcement Point
PDP	Policy Decision Point
Tx	Blockchain Transaction
DLT	Distributed Ledger Technology
QoS	Quality of Service
ACL	Access Control List
CADAC	Context-Aware Decentralized Access Control
Req	Access Request
D	Access Decision (Grant/Deny/Restrict)

AUTHOR CONTRIBUTIONS

Conceptualization, A.T.; Methodology, A.T.; Validation, A.T., & R.G.; Investigation, A.T.; Resources, A.T.; Data Curation, A.T.; Writing – Original Draft Preparation, A.T.; Writing – Review & Editing, R.G.; Visualization, R.G.; Supervision, R. G.; Project Administration, R.G.

CONFLICT OF INTERESTS

The authors confirm that there is no conflict of interest associated with this publication.

REFERENCES

1. Xu, R., Chen, Y., Blasch, E. Decentralized Access Control for IoT Based on Blockchain and Smart Contract. *Modeling and Design of Secure Internet of Things*; Wiley: Hoboken, NJ, **2020**.
2. Khan, A.R., Alnwihel, L.K. A Brief Review on Cloud Computing Authentication Frameworks. *Engineering, Technology & Applied Science Research* **2023**, *13*(1), 9997–10004.
3. Aljahdali, A.O., Habibullah, A., Aljohani, H. Efficient and Secure Access Control for IoT-Based Environmental Monitoring. *Engineering, Technology & Applied Science Research* **2023**, *13*(5), 11807–11815.
4. Alotaibe, D.Z. IoT Security Model for Smart Cities Based on a Metamodeling Approach. *Engineering, Technology & Applied Science Research* **2024**, *14*(3), 14109–14118.
5. Almansoori, S., Alzaabi, M., Alrayssi, M., Puthal, D., Dutta, J., Shehhi, A. Machine Learning-Based Adaptive Access Control Mechanism for Private Blockchain Storage. *IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, Torino, Italy, **2023**, p. 00188.
6. Fugkeaw, S., Rattagool, S., Jiangthiranan, P., Pholwiset, P. FPRESSO: Fast and Privacy-Preserving SSO Authentication with Dynamic Load Balancing for Multi-Cloud-Based Web Applications. *IEEE Access* **2024**, *12*, 157888–157900.
7. Du, Z., Li, Y., Fu, Y., Zheng, X. Blockchain-Based Access Control Architecture for Multi-Domain Environments. *Pervasive and Mobile Computing* **2024**, *98*, 101878.
8. Akbarfam, A.J., Barazandeh, S., Gupta, D., Maleki, H. Deep Learning Meets Blockchain for Automated and Secure Access Control. *International Journal of Security, Privacy and Trust Management* **2023**, 12, 1–22.
9. Lee, Y., Woo, S. A Blockchain-based User-centric Role Based Access Control Mechanism. *Journal of the Korea Institute of Information and Communication Engineering*, **2022**, *26*(7), 1060-1070.
10. Chatterjee, A., Pitroda, Y., Parmar, M. Dynamic Role-Based Access Control for Decentralized Applications. *In Advances in Computing and Data Sciences*; Springer, **2020**, pp. 185-197.
11. Noor, N., Matrazali, N., Malizan, N., Ishak, K., Wook, M., Hasbullah, N. Decentralized Access Control Using Blockchain Technology for Application in Smart Farming. *International Journal of Advanced Computer Science and Applications* **2022**, *13*(9), 788-802.
12. Ouaddah, A.; Elkalam, A.; Ouahman, A. FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things. *Security and Communication Networks* **2017**, *9*, 5943-5964.
13. Sun, L., Zhou, D., Liu, D., Tang, J., Li, Y. BPDAC: A Blockchain-Based and Provenance-Enabled Dynamic Access Control Scheme. *IEEE Access* **2023**, 11, 1-17.
14. Gou, C., Deng, X. A Blockchain-Based Security Model for Cloud Accounting Data. International *Journal of Ambient Computing and Intelligence* **2023**, *14*, 1–16.
15. Xiao, M., Huang, Q., Miao, Y., Li, S., Susilo, W. Blockchain-Based Multi-Authority Fine-Grained Access Control System with Flexible Revocation. *IEEE Transactions on Services Computing* **2022**, *15*(6), 3143-3155.
16. Monteiro, P., Pereira, R., Nunes, R., Reis, A., Pinto, T. Context-Aware System for Information Flow Management in Factories of the Future. *Appl. Sci.* **2024**, *14*, 3907.
17. Zheng, P., & Jiang, Z., Wu, J., & Zheng, Z. Blockchain-Based Decentralized Application: A Survey. *IEEE Open Journal of the Computer Society*. **2023**, 1-12.

18. Lekkala, C. AI-Driven Dynamic Resource Allocation in Cloud Computing: Predictive Models and Real-Time Optimization. *Journal of Artificial Intelligence, Machine Learning and Data Science* **2024**, *2*(2), 1-7.
19. Taherdoost, H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. *Sci*. **2023**, *5*(4), 41.
20. Abid, A., Cheikhrouhou, S., Kallel, S., Tari, Z., Jmaiel, M. A Smart Contract-Based Access Control Framework for Smart Healthcare Systems. *The Computer Journal* **2022**, *67*(2), 407-422.
21. Buttar, A.M., Shahid, M.A., Arshad, M., Akbar, M.A. Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions. *In Advances in Blockchain and Distributed Systems*; Springer, **2024**, pp.131-136.
22. Al Ghamdi, M. An Optimized and Secure Energy-Efficient Blockchain-Based Framework in IoT. *IEEE Access* **2022**, 10, 133682 – 133697.
23. Kaur, A., Verma, A. Adaptive Access Control Mechanism (AACM) for Enterprise Cloud Computing. *Journal of Electrical and Computer Engineering* **2023**, *2023*, 1–30.
24. Punia, A., Gulia, P., Gill, N., Ibeke, E., Iwendi, C., Shukla, P. A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environment. *Journal of Cloud Computing* **2024**, *13*, 146.
25. Hou, Y., Liu, W., Lin, H., Wang, X. Multi-Layer Access Control Mechanism Based on Blockchain for Mobile Edge Computing. *In Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA-BDCloud-SocialCom-SustainCom)*; **2020**, pp 285–291.