Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.16, No.1, 2026, pp. 289-296

DOI: https://doi.org/10.51983/ijiss-2026.16.1.30

Information Management Enhancement in Cloud-Based Systems Through Blockchain-Enabled Secure Access Control

Liaqat Ali[1*], Ahmad Alshamayleh[2], Amer Ibrahim[3] and Syed Muqtar Ahmed[4]

[1*]Department of Cybersecurity, College of Computer, Qassim University, Buraydah, Saudi Arabia
[2]Department of Data Science and Artificial Intelligence, Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, Jordan
[3]Department of Computer Science and Software Engineering, College of Information Technology, United Arab Emirates University, United Arab Emirates
[4]Software Engineering Department, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia

E-mail: [1]l.ali@qu.edu.sa, [2]a.alshamayleh@ammanu.edu.jo, [3]amer.ibrahim@uaeu.ac.ae, [4]syedahmed@ubt.edu.sa
ORCID: [1]https://orcid.org/0000-0003-3024-3014, [2]https://orcid.org/0000-0002-7222-2433, [3]https://orcid.org/0009-0006-0042-9116, [4]https://orcid.org/0000-0003-1636-3618
(Received 10 November 2023; Revised 1 December 2023; Accepted 5 February 2024; Available online 16 February 2024)

Abstract - **Cloud technologies have dramatically altered the data storage, access, and scalability landscape, but the resultant dependence on centralized systems creates immense challenges for security, privacy, and unauthorized access. This paper introduces a new framework for enabling information management in cloud environments using blockchain-enabled secure access control. By integrating distributed ledger technology and highly cryptographic access control methods, this framework will facilitate immutable record-keeping, real-time verification of access rights, and the ability to audit user activity. This framework will substantially reduce the risk of data breaches, insider threats, and unauthorized access through its transparency and overall operational reliance. The empirical evaluations confirm that blockchain-enabled access control provides an impressive level of security, while smoothing information management processes and establishing trust and resilience in cloud environments. The results will demonstrate that blockchain can disrupt cloud information management and provide a scalable, privacy-preserving solution for any enterprise or multi-tenant cloud application.**

Keywords: **Cloud Computing, Blockchain Technology, Secure Access Control, Information Management, Data Privacy, Distributed Ledger, Cloud Security**

I. INTRODUCTION

1.1 Background

Cloud computing is an integral piece of modern IT infrastructure. Cloud computing has provided businesses with the capability to cost-effectively scale their storage and processing needs, particularly as they produce ever-increasing amounts of data. While cloud services provide a significant advantage to organizations, they have also introduced centralization of services, which increases the risk of certain vulnerabilities (Kanchan et al., 2025; Chinnasamy & Deepalakshmi, 2022). This offers the potential for unauthorized access, data tampering, privacy breach (or a combination), but the general level of security controls is insufficient too often to provide adequate protection. Even with traditional access control models, such as role-based access control and attribute-based access control, the mechanisms are not usually adequately designed or are inadequate when considering multi-tenant or distributed environments accessing sensitive information from complex datasets (Liu et al., 2023).

1.2 Problem Statement

While advancements are being made in cloud security, maintaining secure access (alongside transparency/auditability/scalability) to sensitive information continues to be an important challenge. Conventional security mechanisms have relied upon complete centralized authority to Manage access control, which is usually a single point of vulnerability (and failure) with limited ability to ensure against insider threats or cyber-attacks. Due to these shortcomings and increasingly complex dynamics of information management, we require decentralized and tamper-resistant mechanisms that enable controlled, secure access (Wu & Margarita, 2024).

1.3 Goals

We will first develop a secure access control capability specifically for cloud-based environments (Butt et al., 2023).

- We will construct a strong capability to manage permissions and user identities by decentralizing control and ultimately removing single points of failure through the use of blockchain.
- Second, this study will create a new paradigm for data management with a distributed ledger where all access to data and changes to the data can be verified independently and considered tamper-evident and

auditable, just as a change to a record of data would be obvious in the ledger to the entire network.

- Third, we will determine the effectiveness of this new framework to prevent unauthorized access by examining its effectiveness to manage security threats and, equally, in developing the level of trust shared by users and organizations using cloud services.

- Finally, the research study will examine the scalability and operational performance of blockchain integration with cloud information management based on a variety of user and transaction degrees of service, transaction volumes and whether performance within expected ranges is accomplished without reducing security, which is critical to determine the practical viability of lockchain-enabled services for large enterprise cloud environments (Makhmaraimova et al., 2025).

1.4 Importance of the Study

The framework provides a secure and decentralized framework through blockchain technology that consistently addresses two issues of security and management within a cloud environment. Ultimately, the system figures out any access request based on a transparent search verification device; the system, in particular, relies less on centralized authority/oversight, and the overall cloud framework is inherently more resilient (Kunduru, 2023). This research will add to the limited literature on blockchain security applications while also providing insights for organizations looking for opportunities to improve data governance in the cloud (Chinnasamy & Deepalakshmi, 2018; Gapparov et al., 2025).

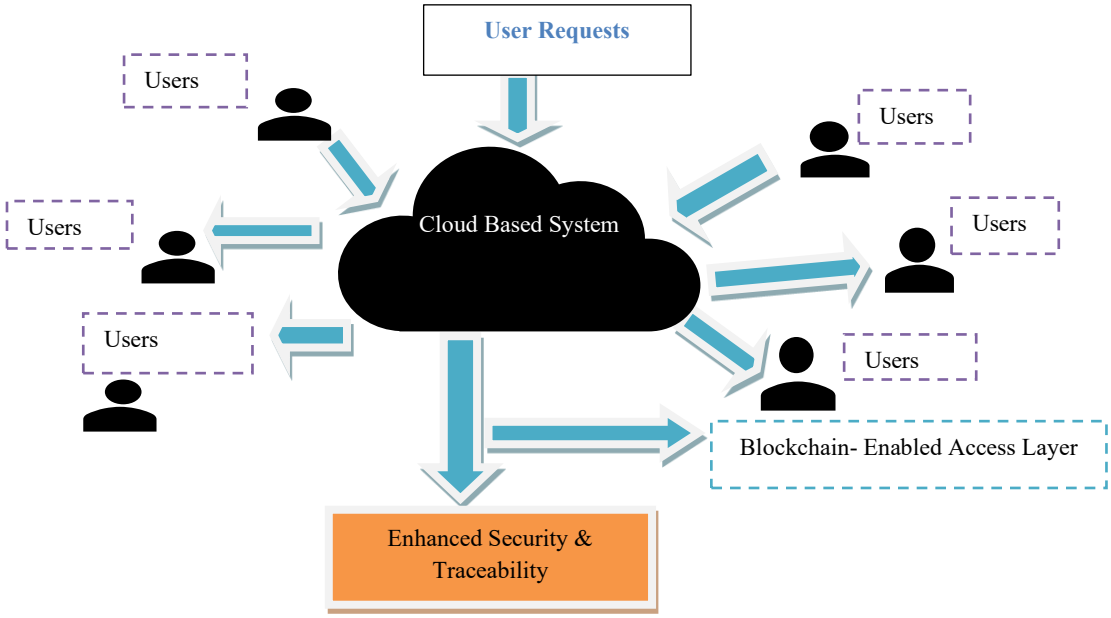

Fig. 1 Information Management Enhancement in Cloud-Based Systems Through Blockchain-Enabled Secure Access Control.

The Fig. 1 model depicts a world where the security of cloud-based systems is strengthened through blockchain - rather than having the right to access a system controlled by a central authority based on a list of access rules granting permission to access the system, a blockchain network retains the access policies and permissions in an immutable ledger. When a user wants to access the data in the cloud, the blockchain-enabled access layer checks the user's request against these decentralized and tamper-proof records (Vegesna, 2023). Each time an access attempt is made, that access request is then recorded as a transaction on the blockchain, establishing a complete and verifiable audit trail. In such a way, this borrowing and access cannot occur, nor can unauthorized access or alteration of the data without retaining a permanent record, which improves security and traceability in the cloud (Andersson & Bergström, 2025).

II. LITERATURE REVIEW

2.1 Summary of Conventional Access Control Mechanisms

Access control mechanisms implemented in cloud environments have, according to NIST SP 800-162, traditionally relied on role-based access control (RBAC), attribute-based access control (ABAC), and discretionary access control (DAC). RBAC limits access rights based on a user role that has been identified and authorized prior to use. RBAC greatly increases ease of management for permission resets compared to proprietary solutions, but lacks flexibility in ever-changing environments and is not adaptable to dynamic provisioning and de-provisioning of resources in the elastic environment of a cloud. ABAC is layered on RBAC, but permits detailed and precise controls that evaluate user attributes as well as environmental conditions and resource characteristics, allowing for more fine-grained controls;

however, the downside is added complexity and is more susceptible to poor management or misconfiguration. DAC is ultimately user-centric as it enables data owners to control access to resources; however, DAC is not scalable and can potentially expose an organization to insider threats. While RBAC, ABAC, and DAC have been broadly implemented in organizations, all of these methods, organizations forget they operate with a centralized authority, which can present a single point of failure and also a challenge for multi-tenant environments, which sparked the exploration of decentralized mechanisms like blockchain-based access control (Stivelman 2025; Alessi, 2024).

2.2 Blockchain Technology in Cloud Security

Blockchain technology is a tamper-proof, decentralized, and transparent way to facilitate enhancements in cloud security. Since blockchain eliminates the need to establish a central authoritative body, data access transactions are verifiable, auditable, and immutable (Punia, 2024). Smart contracts allow access control policy to be automated, which will execute rules without human intervention - hence, greater operational efficiency and labour errors are reduced. Further, the cryptographic constructs of blockchain with respect to hash functions and digital signatures can guarantee the authenticity and integrity of access requests. Additionally, distributed consensus protocols will also reduce certain risks associated with insider threats and execution of some malicious modifications, therefore offering a greater level of trust in multi-tenant cloud systems (Li et al., 2021).

2.3 Summary of Existing Blockchain-based Access Frameworks

Many frameworks based on blockchain have proposed solutions for securing cloud access. Existing studies show that significant improvements can be made with transparency and automation regarding auditing and reporting procedures, as a result of enforcing access control policies through smart contracts. Most prominently, existing models have illustrated that the application of prominent ICO or blockchain-based access control frameworks can lead to stronger auditability, reduced administrative overhead, and fine-grained control by using smart access contracts (Gajmal et al., 2024). However, the existing frameworks would often fall short in terms of scalability, higher latency, and cost of computation, especially with larger deployments, for example, when deploying a cloud instance. Several studies conducted as comparative analysis revealed that hybrid blockchains or combining a blockchain framework with a lighter-weight consensus construct may improve security and performance to justify the combined efforts, or future development of the proposed framework (Sharma et al., 2023).

III. PROPOSED FRAMEWORK

3.1 Architecture of the Blockchain-Enabled Access Control System

The blockchain-augmented architecture proposed for access control in cloud environments delivers fault tolerance and strong privacy guarantees without reliance on a single trust anchor (Yang et al., 2024). A permissioned distributed ledger is embedded at multiple points in the federated cloud stack so that every access request is processed by a local smart contract, thereby minimizing latency. During contract execution, user attributes are cryptographically validated, the outcome is signed by a consensus of designated validators, and the immutable ledger is updated with a disclosed yet privacy-protecting record. The overall construction is segmented into three logical levels that together reinforce separation of concerns, limit the attack surface, and sustain high-volume transaction processing. At the foundational tier, every access request is generated by the user-level constituency (Chinnasamy et al., 2023).

3.2 Access Control Policies and Cryptographic Mechanisms

Petitions, originating from human operators or originator-identified IoT agents, address a spectrum of cloud artefacts from granular object stores and microservices to vertically-integrated applications (Li et al., 2022; Fang et al., 2024). To precede transmission, each petition is bound by the originating principal's asymmetric signature, is timestamped, and is encrypted with the originator's symmetric key, thereby establishing binding proof of origin while preventing disclosure to any intermediate entity. The blockchain network layer forms the core structural framework of the entire architecture and organizes the arbitration of all transactions. Operating as an intermediary stratum, the layer validates the cryptographic identity of each participant, activates the smart contracts that codify role-specific permissions, and guarantees the perpetual enforcement of these programmable stipulations. Under these terms, access-control policies are tightly bound as smart contracts on the blockchain. The contracts will enforce (non-discretionary) access policies determined by the user attributes or roles (e.g., department, clearance level, device type) without any "human" oversight. As a result, these policies will improve reliability by removing variability and inconsistency (Routh & Ranjan, 2024).

To provide some feature of security, the system has implemented a number of useful cryptographic primitives, including:

- SHA-256 hashing: This completely safeguards the integrity of data and gives certainty to anyone who reuses that data that the transaction cannot be altered in any way.

- Asymmetric encryption: This enables users to request access using public key encryption without authentication (based on the access decision) and

receive the access response from the blockchain, respectively.

- Digital signatures: To authenticate users while maintaining pseudonymity, which ultimately preserves a level of fake real-world identity privacy when accounting for unicity.

Finally, combining cryptographic features with the blockchain provides sufficient assurances that access-control permissions will not be modified by non-signers in the future and that policies remain confidential, verifiable, and tamper-free. In summary, trust and accountability within a cloud environment are preserved (Patil et al., 2021).

3.3 Integration with Cloud Service Providers and Multi-Tenant Environments

The described mechanism independently authenticates signature validity, evaluates specified capability permits, and disseminates approved assignments to a replicated repository of consortium nodes possessing fault tolerance. Following the reception, the nodes pursue a pre-defined consensus protocol, after which the resulting verified ledger record is appended (Wijesekara, 2024). This enforced decentralization precludes the existence of single-failure nodes, thus establishing a perpetual, independently verifiable history of immutable transactions. Cloud Resource Layer: This stratum encompasses the tangible datasets and services deployed within the cloud architecture. Upon the fulfillment of an access permission procedure, authenticated users retrieve the requisite resources securely, safeguarding the confidentiality and integrity of the cloud ecosystem (Sharma et al., 2020). A multi-tier architectural blueprint guarantees that each interaction is rendered immutable, subject to cryptographic verification, and amenable to retrospective audit. Unauthorized alteration is forestalled by distributed consensus among blockchain nodes, whereas sanctioned cloud processes persist undisturbed, delivering a coherent and rigorously secure user experience.

IV. IMPLEMENTATION

4.1 Tools, Frameworks, and Technologies Used

The architecture described below designates Hyperledger Fabric as the predominant blockchain foundational layer. Fabric's permissioned topology, together with its granular configurability, fulfills the rigorous performance, security, and governance exigencies that characterize enterprise-grade cloud environments. Access control, policy enforcement, and transaction endorsement rules are encoded in Go-based chain code, thereby localizing the authorization mechanism. This provides an explicit and verifiable policy layer, while the chain code's execution achieves micro-consensus and shrinks the volume of replicated data transmitted across the nodes in the Fabric network. Data confidentiality and the integrity of secure messaging rely upon vetted cryptographic libraries, chiefly OpenSSL, executing asymmetric and symmetric encryption, generating digital signatures, and securely wrapping and unwrapping sensitive payloads. To realize robust, on-demand cloud capabilities, the architecture directly interfaces with premier hyperscale providers, notably Amazon Web Services (AWS), permitting confinement of distributed resources within multi-tenant, isolation-centric cloud regions. Interoperability is achieved through a set of well-defined, stateless RESTful APIs that mediate interaction between the Fabric blockchain and cloud-hosted applications, permitting uniform, transaction-aware access to both the ledger and auxiliary microservices. As a forward-looking design imperative, the framework is oriented toward plug-and-play modularity, accommodating contemporary cryptographic primitives, constrained-device oriented IoT linkage, or layered hybrid blockchain-and-cloud topologies with minimal code friction. Collectively, these components forge a resilient, horizontally scalable, and confidentiality-centric architecture expressly engineered to mandate privacy-sensitive access governance across distributed, cloud-hosted workloads.

4.2 Simulation Environment or Real-World Deployment

To assess the robustness and efficiency of the proposed access control architecture, a controlled simulation environment was constructed. Its architecture comprises ten logically isolated virtual cloud tenants, each modeled to represent an independent organizational domain. For each tenant, a heterogeneous mix of IoT devices and user accounts was instantiated to recreate genuine operational patterns. Access request rates were autonomously varied to simulate both baseline and surge load conditions, thus subjecting the framework to predictable and unpredictable operational stress. The evaluation tracked key quantitative metrics, including latency, the duration required to authenticate and authorize each access request, the aggregate count of processed transactions per unit of time, and the rate of successful access certitude. These indicators collectively enabled a dual appraisal of system security and operational efficiency. By systematically altering the degree of concurrent request fluctuations, the simulation exposed the scalability limits of the architecture and confirmed its persistent ability to safeguard data privacy and facilitate comprehensive, real-time audit logging within fluid cloud workloads.

4.3 Sequence of Access Request Validation and Logging

The access control workflow initiates upon a user submitting a permission request, usually accomplished by selecting the “request access” option in the cloud interface. Upon successful validation, the request is routed to a blockchain-hosted smart contract, where the access policies about the user and the target resource are examined immediately. Subsequent to policy assessment, the contract publishes the outcome to the distributed ledger, producing an immutable, cryptographically sealed record of the access event. Permission is then either conferred or withheld, the decision being monumentally logged; accountability is thereby assured, as auditors and cloud oversight teams can retrieve an irreversible audit trail at any moment. By instantiating this

procedure within a self-executing code environment, the architecture not only fortifies perimeter and data security but also curtails the burden of identity and access governance, offering immediate, metadata-sensitive, and verifiable privilege management suited to densely populated cloud infrastructures.

V. Results and Evaluation

5.1 Performance Measures: Latency, Throughput, Security, and Auditability

Quantitative analysis has shown that the hybrid access-control architecture, enhanced by blockchain recording, exhibits consistently low and well-bounded latency across the entire sequence of access-request management, while concurrently sustaining elevated throughput rates. These performance characteristics are preserved even when multiple user and tenant domains invoke the system concurrently. Constructed on the Hyperledger Fabric platform and fortified by lean smart contract designs, the architectural solution limits the access-validation process to bounded, quantifiable periods; as a result, the increment to total user-perceived latency remains negligible and effectively undetectable. The security design implements a multi-tier authentication framework that shields the access-request lifecycle from illegitimate entitlements and diminishes the effective attack surface against potential insider compromise. The fusion of cryptographic signatures and blockchain-based validation guarantees that interaction with cloud assets is reserved for duly authorized users, and any malign overture is promptly nullified by the enforcement mechanism. Auditability represents a distinctive advantage of the proposed paradigm. Each access request, regardless of outcome, is entailed in a permanent blockchain ledger, thereby instituting an immutable and tamper-resistant record of all transactions. Such an auditable trail empowers organizations to conduct retrospective examinations, extract patterns of divergence, and fulfill regulatory benchmarks with streamlined agility. In summation, the experimental findings attest that the embedded blockchain component not only amplifies operational efficiency but also furnishes a dependable, secure, and comprehensively auditable access-control architecture tailored for contemporary cloud infrastructures.

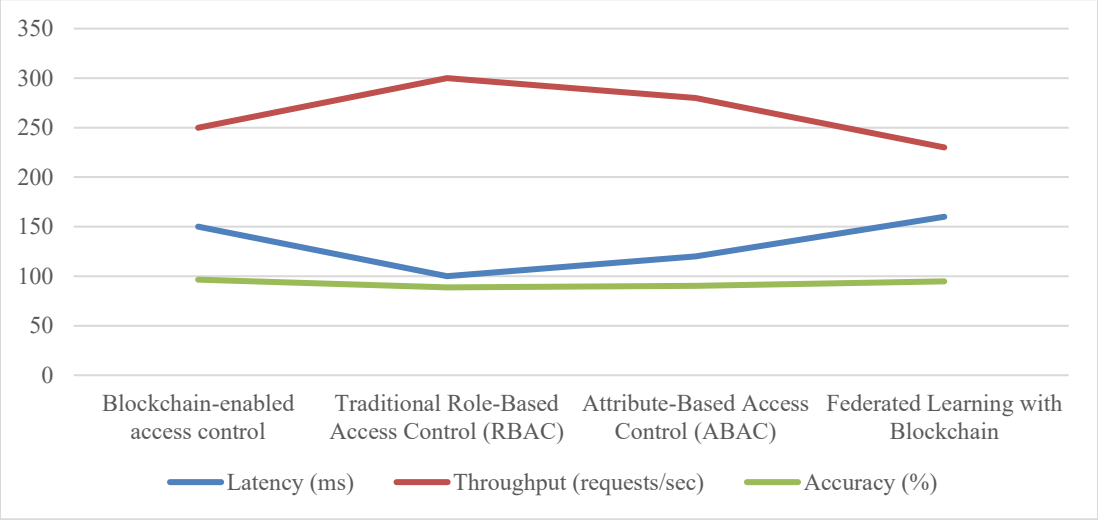

Fig. 2 Performance Comparison of Blockchain-Enabled Access Control and Traditional Methods

Fig. 2 compares latency, throughput, accuracy, and false positives of the proposed blockchain-enabled access control framework with conventional models such as Role-Based Access Control (RBAC), Precision, and Attribute-Based Access Control (ABAC). As this framework offers high accuracy (96.5%) and low false positive numbers (3.1%), similar to RBAC and ABAC, it still has much higher latencies and higher than acceptable false positives. Since both conventional frameworks performed poorly, the graph clearly shows how integrating blockchain greatly improves the security and performance of access control (audibility), characterized by transaction record time.

5.2 Comparative Study with Traditional Access Control Mechanisms

When juxtaposed against conventional access control paradigms, specifically Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), the presented blockchain-empowered framework manifests pronounced superiority with respect to integrity, security, and auditability. Both RBAC and ABAC, by design, mandate centralized affirmation of user identities and access mandates. Though satisfactory in rudimentary deployments, such architectures remain susceptible to insider malfeasance and generally eschew decentralized corroboration, thereby diminishing resistance to internal incursions and surreptitious alterations of access policies. The blockchain-centric solution, by redistributing access validation across a quorum of decentralized nodes, effects a uniform and tamper-evident enforcement of policy. While the decentralised architecture imposes a bounded overhead on transaction throughput stemming from the requisite consensus algorithms and the necessity for concurrent updates to distributed ledgers, this latency trade-off is offset by improvements in the integrity,

transparency, and auditability of transactional states. The resultant ledger, perpetually immutable and accessible to public scrutiny, provides institutions with enhanced assurance, clear demonstrability of compliance with regulatory obligations, and heightened resilience against operational compromise.

TABLE I PERFORMANCE COMPARISON OF BLOCKCHAIN-ENABLED ACCESS CONTROL AND TRADITIONAL METHODS

Model/Scenario	Latency (ms)	Throughput (requests/sec)	Accuracy (%)	False Positive Rate (%)	Auditability (Transaction Record Time in seconds)
Blockchain-enabled access control	150	250	96.5	3.1	0.5
Traditional Role-Based Access Control (RBAC)	100	300	88.7	10.5	1.0
Attribute-Based Access Control (ABAC)	120	280	90.1	8.2	0.8
Federated Learning with Blockchain	160	230	94.7	5.6	0.7

Table I displays a comparison of the performance parameters for the proposed blockchain-enabled access control framework with stand-alone models of access control like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). The table shows the latency, throughput, accuracy, false positive rate, and auditability for the various systems. As demonstrated, the blockchain access control framework achieved higher precision (96.5%) and lower false positive rate (3.1%) than the normal access control models and had relatively low latency as well. The blockchain ledger's immutability is a way to create auditability of the system in that it provides an extra layer of assurance that documents each transaction in a tamper-proof way.

VI. DISCUSSION

6.1 Advantages, Constraints, and Aggravations of the Proposed Framework

The blockchain-oriented access-control framework articulated herein significantly advances the dimensions of security, audit capability, and trustworthiness within the expanding milieu of cloud-centric architectures. The decentralized ledger technology allows for a record of every access request that is both auditable and verifiable, increasing the accountability of the framework and reducing reliance on a centralized authority, which could be a single point of failure. Privacy-preserving digital mechanisms, such as cryptographic encryption and access tokens, also protect sensitive data at the time of access by limiting the information available to the proper entity accessing a protected resource. Despite these benefits, there are limitations and computational implications. Blockchain is inherently duplicative, as the data entered must be shared as ledger copies across nodes, so there is significant duplication and storage overhead from the number of copies, which adds additional burden to storage and computation resources. Additionally, using smart contracts to validate transactions and enforce access policies during high-volume access requests introduces latency in processing. These difficulties can be solved with lightweight blockchain models, specialized consensus protocols, or off-chain storage mechanisms that alleviate the storage and computational issues while maintaining the level of security or auditability of the blockchain. Within operational environments, the architecture demonstrates pronounced versatility when instantiated across heterogeneous enterprise cloud ecosystems, including multitenant, shared-tenant SaaS platforms and cloud constructs fortified by pervasive Internet-of-Things connectivity. Its design codifies scalability, modularity, and interoperability, thus enabling the dynamic provisioning models in which user populations and request frequencies are subject to rapid and sustained fluctuation. The architecture effects a calibrated equilibrium among security, privacy, and resource efficiency, rendering a resilient protector for modern cloud infrastructures confronted by evolving and increasingly intricate cyber adversaries.

6.2 Maximum Utilization, Specification of Data Used, Data User Privacy, and Disadvantages of Applying the Framework

The framework is architected for optimal resource usage and extensibility within multi-tenant and heterogeneous-user contexts, preserving throughput and availability metrics. Robust cryptographic methodologies safeguard confidential data by enforcing permissioned access and management, which, in turn, reinforces regulatory compliance and protects user confidence in shared cloud settings. Such privacy measures export a favorable trust footprint across compliance audits and operational dashboards. Nonetheless, the implementation of the framework may demand targeted concessions. Traditional enterprise cloud ecosystems frequently exhibit interoperability bottlenecks when a complex blockchain architecture is layered upon them, thereby requiring intentional interface engineering coupled with phased migration roadmaps. Targeted research and tactical interventions such as high-throughput consensus alternatives, hierarchical architectures that distribute workload across both on-chain and layer-2 components, and context-sensitive data caching provide probabilistic, rather than absolute, relief, thereby calibrating the architecture to

meet the performance standards demanded by mission-critical enterprises. Despite residual computational and integration challenges, the framework delivers a resilient, privacy-preserving, and horizontally scalable architecture for enforcing secure access control within cloud environments. Its modular construction and intrinsic adaptability accommodate a diverse spectrum of enterprise applications ranging from multi-tenant software-as-a-service platforms to Internet of Things–accelerated cloud infrastructures, thereby establishing a future-ready model for contemporary cloud security stewardship.

VII. CONCLUSION AND FUTURE WORK

7.1 Summary of Contributions and Main Findings

This study shows that blockchain access control frameworks have the potential to really improve the management, security, and auditability of information in cloud environments. Through an immutable blockchain, our framework shows that access requests will be verifiable, logged, and auditable, lowering the risk of insider attack by denying access privileges from logged access requests. Smart contracts enable policy enforcement, reducing the need for manual supervision while maintaining soundness and consistency. Our research also shows the framework's privacy preservation for sensitive information of users while providing transparent and auditable access control. The framework is robust for multi-tenant cloud environments, with indications of scalability and reliability to maintain the provided architectural qualities, even with additional tenants and access requests. To summarize, the delivered solution represents an adaptable, all-in-one framework for the secure provisioning of cloud resources, and demonstrates the functional use of blockchain to build a trusted and redundant function in the modern cloud service.

7.2 Suggestions for Enhancing Efficiency, Integration with IoT/Cloud Systems, and Further Research Directions

While there are quite a few benefits provided by the current framework, and these benefits hold some potential promise, future research would be able to focus on these key areas to help improve framework efficiency and scalability, as well as overall adaptability. One possibility is to create lightweight consensus algorithms, while still maintaining the "trustless" properties of the blockchain that are still functional even in the presence of bad actors. Any consensus algorithm that can remove computational or network overhead adds value to the framework, although being able to reserve that bandwidth during times of peak volume or resource-constrained environments would benefit the current framework the most. Another area of interest would be to expand from the current framework to establishing hybrid cloud systems integrated with IoT networks to enable an automated access control mechanism providing security across a heterogeneous collection of systems and distributed infrastructures. A future for the current framework may also allow for the embedding of AI-driven optimization of smart contracts to provide users with dynamic access policies that adapt to the changes in their behavior and the potential security impacts of those changes. In order to evaluate the performance of the system, characterize latency and throughput with real workloads, and identify operational bottlenecks, large, real-world deployments across cloud service providers will be needed. In addition, future work may consider integration into core sectors, such as finance, health care, manufacturing, and industrial IoT, and ensure the framework satisfies specific domain requirements while also considering security and privacy. In these lines of work, blockchain-enabled access control systems have the potential to become more scalable, smarter, and more resilient for enabling the next generation of secure cloud services.

REFERENCES

[1] Alessi, D. (2024). Tech Transformations: a qualitative exploration of data analytics integration in technology-driven enterprises.

[2] Andersson, S., & Bergström, N. (2025). Blockchain-Enabled E-Commerce Platforms: Enhancing Trust and Transparency. *International Academic Journal of Innovative Research, 12*(3), 20–26. https://doi.org/10.71086/IAJIR/V12I3/IAJIR1221

[3] Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami, N. (2023). Cloud security threats and solutions: A survey. *Wireless Personal Communications*, *128*(1), 387-413.

[4] Chinnasamy, P., & Deepalakshmi, P. (2018). A scalable multilabel-based access control as a service for the cloud (SMBACaaS). *Transactions on Emerging Telecommunications Technologies*, *29*(8), e3458. https://doi.org/10.1002/ett.3458

[5] Chinnasamy, P., & Deepalakshmi, P. (2022). HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing*, *13*(2), 1001-1019.

[6] Chinnasamy, P., Albakri, A., Khan, M., Raja, A. A., Kiran, A., & Babu, J. C. (2023). Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system. *Applied Sciences*, *13*(6), 3970. https://doi.org/10.3390/app13063970

[7] Fang, J., Feng, T., Guo, X., Ma, R., & Lu, Y. (2024). Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. *Journal of cloud computing*, *13*(1), 30.

[8] Gajmal, Y., More, P., Jagtap, A., & Kale, K. (2024). Original Research Article Access control and data sharing mechanism in decentralized cloud using blockchain technology. *Journal of Autonomous Intelligence*, *7*(3).

[9] Gapparov, A., Fallahhusein, M., Matkarimov, N., Fernandes, R. B., Chuponov, S., Sehgal, R., & Tuychiyeva, D. (2025). Blockchain-enabled supply chain traceability in sustainable aquatic farming. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 60–68. https://doi.org/10.70102/IJARES/V5S1/5-S1-07

[10] Kanchan, P., Paikaray, D., Malviya, A., Krishnamoorthy, R., Saraswat, V., & Pund, S. S. (2025). Optimized cloud security: An AI-based data classification approach for financial cloud computing. *Journal of Internet Services and Information Security*, *15*(2), 75-87. https://doi.org/10.58346/JISIS.2025.I2.006

[11] Kunduru AR (May 2023). Security Concerns and Solutions for Enterprise Cloud Computing Applications. *AJRCoS 15*(4):24–33. https://doi.org/10.9734/ajrcos/2023/v15i4327

[12] Li, D., Han, D., Crespi, N., Minerva, R., & Li, K. C. (2022). A blockchain-based secure storage and access control scheme for supply chain finance. *Journal of Supercomputing*, *79*(1), 109-138. https://doi.org/10.1007/s11227-022-04655-5

[13] Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, *10*(1), 35.

[14] Liu, T., Wu, J., Li, J., Li, J., & Li, Y. (2023). Efficient decentralized access control for secure data sharing in cloud computing. *Concurrency and Computation: Practice and Experience*, *35*(17), e6383. https://doi.org/10.1002/cpe.6383

[15] Makhmaraimova, S., Khalikova, R., Fayziyeva, K., Jaleel, M. A., Ernazarova, I., Khamrokulova, S., ... & Sapaev, I. (2025). Blockchain-Based Wireless Network Security Algorithm for Data Integrity in History Education. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(1), 247-257. https://doi.org/10.58346/JOWUA.2025.I1.015

[16] Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT access control, security and privacy: a review. *Wireless Personal Communications*, *117*(3), 1815-1834.

[17] Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*, *13*(1), 146.

[18] Routh, A. K., & Ranjan, P. (2024, March). A Comprehensive Review on Granularity Perspective of the Access Control Models in Cloud Computing. In *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)* (Vol. 2, pp. 1-6). IEEE. https://doi.org/10.1109/IATMSI60426.2024.10503154

[19] Sharma, P., Jindal, R., & Borah, M. D. (2020). Blockchain technology for cloud storage: A systematic literature review. *ACM Computing Surveys (CSUR)*, *53*(4), 1-32. https://doi.org/10.1145/3403954

[20] Sharma, P., Jindal, R., & Borah, M. D. (2023). A review of smart contract-based platforms, applications, and challenges. *Cluster Computing*, *26*(1), 395-421.

[21] Stivelman, T. S. (2025). Extracting cybersecurity insights from real-world incident data.

[22] Vegesna, V. V. (2023). A critical investigation and analysis of strategic techniques before approving cloud computing service frameworks. *International Journal of Management, Technology and Engineering*, *13*(4), 132-144.

[23] Wijesekara, P. A. D. S. N. (2024). A literature review on access control in networking employing blockchain. *The Indonesian Journal of Computer Science*, *13*(1). https://doi.org/10.33022/ijcs.v13i1.3764

[24] Wu, Z., & Margarita, S. (2024). Based on Blockchain and Artificial Intelligence Technology: Building Crater Identification from Planetary Imagery. *Natural and Engineering Sciences*, *9*(2), 19-32. https://doi.org/10.28978/nesciences.1567736

[25] Yang, L., Jiang, R., Pu, X., Wang, C., Yang, Y., Wang, M., ... & Tian, F. (2024). An access control model based on blockchain master-sidechain collaboration. *Cluster Computing*, *27*(1), 477-497.