IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15643

A Blockchain-Enabled Data Privacy and Governance Framework for Multi-Cloud Environments

Sukhwinder Kaur[1*], Dr Pooja Rana[2]

School of Computational Science, GNA University[1]

Assistant Professor, School of Computational Science, GNA University[2]

Abstract: Multi-cloud architectures have been selected by industries today to achieve enhanced scalability, resilience and flexible operation capabilities and non-vendor lock-in. Organizations can boost their system uptime and service performance by spreading their computing tasks and storage needs across multiple cloud service providers; however, this approach causes major difficulties for organizations because they need to maintain uniformity in their data control processes, protection of personal information, and auditing procedures, and their ability to meet legal requirements. The research investigates traditional centralized governance systems because they do not work effectively with their existing systems of access control systems inside multiple cloud environments. The study creates a blockchain-based system that protects data privacy rights and establishes governance standards that apply to multiple cloud computing environments. The proposed architecture uses a permissioned blockchain system combined with smart contracts to create unchangeable governance rules and permanent audit trails, while Attribute-Based Encryption (ABE) controls access to sensitive information through precise security measures. The system implements off-chain storing solutions in order to achieve both. performance enhancement and efficient operations, whereas compliance monitoring system. conducts automatic evaluations that comply with the regulations of both GDPR and CCPA. The study aims at developing a decentralized system of governance that is secure and transparent and offers wide multi-cloud management systems.

Keywords: Blockchain, Multi-Cloud Computing, Data Governance, Smart Contracts, Attribute-Based Encryption.

1. INTRODUCTION

Cloud computing is a fundamental infrastructure that organizations use to establish digital. scales since it gives them scalable and flexible computing resources that. they have access to it anytime. Enterprises have adopted multi-cloud architectures in recent years after they previously relied on single-cloud strategies. The organization applies this method to distribute its operational tasks and data storage needs across various cloud service providers. This is a technique that the organization employs in order to create an improved system uptime and operational improvement. cost-effectiveness and compliance with regulations coupled with preventing vendor lock-in [1]. Now, as mankind has fought the necessary building of a fragile environment that supports not only man's spiritual estate with various signs of meaning but nature itself, shifting rationales are in motion, ever growing in multiple ways.

The different cloud providers in multi-cloud environments operate their systems through separate access control systems, logging tools, policy enforcement methods, and compliance standards. The different access control systems used by cloud providers create multiple security challenges because they produce different ways to monitor data access, which makes it hard to maintain control over all data activities [2]. The traditional governance practices rely on. Central trust assumptions combined with provider-managed controls, which inhibit organizations on the use of standard security policies across the various cloud platforms as they carry out independent compliance audit [1]. This has put in place a situation that frequently presupposes a lower level of transparency and offers access to decision-making and, consequently, makes interoperability and accountability systems in the distributed context make it less functional.

The security and privacy dangers of multi-cloud deployments increase because different identity management systems, bad configurations, incomplete audit records, and different platforms fail to work together [3], [4]. The existing problems create two distinct consequences, which lead to increased chances of data breaches and create difficulties with compliance reporting. General Data Protection Regulation (GDPR) and California Consumer. Privacy Act (CCPA) present organizations with the need to demonstrate their data processing operations by full traceability systems, that offer transparent operation visibility and construction. Accountability [5]. The organization needs to have integrated governance within its multi-cloud systems. since any inability to do so will be dealt with by compliance infractions, monetary fines and. tarnishment of its reputation.

DOI: 10.17148/IJARCCE.2026.15643

Scientists examine blockchain technology as a decentralized trust system to solve those issues that provides long-term record keeping and openness to information and systems that implement. without human intervention [6], [7]. Blockchain systems obtain protection of failure. by their construction, which shares control records with all network nodes, but at the same time assuring the users of secure and permanent means of verification. The current rather than providing total security protection, they put their efforts in solutions, building security enhancements.

In order to address these issues, scientists investigate blockchain technology as a decentralization of the trust system that provides enduring record keeping and open access to information and systems to enforce regulations without a human touch [6], [7]. Blockchain systems achieve failure protection through their design, which distributes control records among all network nodes, while simultaneously providing users with secure and permanent verification methods. The current solutions, instead of achieving complete security protection, concentrate their efforts on building security enhancements.

2. RELATED WORK

2.1 Data Governance in Cloud and Multi-Cloud Systems

Data governance in traditional cloud environments has primarily relied on centralized mechanisms such as role-based access control (RBAC), encryption protocols, identity and access management (IAM), and provider-managed audit logging systems. The approaches work well for single-cloud deployments because their governance policies function under a single administrative control. The system performance in multi-cloud environments decreases because different providers use their own architectures, and their policy enforcement methods are inconsistent, while their platforms have limited ability to work together [1].

The lack of standardized governance frameworks between cloud providers prevents organizations from establishing consistent data management practices, and it reduces their ability to monitor systems across different platforms according to Jensen et al [2]. Centralized governance systems need to trust cloud service providers for three critical functions, which include maintaining log integrity, enforcing policies, and providing audit transparency. The growing adoption of multi-cloud systems will create operational difficulties for organizations because these systems will generate multiple compliance reports, which will result in governance problems.

2.2 Blockchain-Based Data Governance

Researchers have studied blockchain technology as a decentralized governance solution because it helps build trust and enables auditability. The governance enforcement of distributed systems can use blockchain technology because it provides three essential functions: immutable records, distributed consensus, and tamper-proof logging [8], Zhang and Datta developed a data governance framework that uses blockchain technology to combine attribute-based encryption (ABE) with decentralized data storage for secure data sharing and precise access control [7]. Their framework shows that when cryptographic systems combine with distributed ledger technology, the resulting system achieves better protection of data while still maintaining its ability to track activities. Research demonstrates that smart contracts enable automatic execution of policy validation procedures, access approval processes, and compliance verification tasks within distributed systems [9]. The research shows that blockchain technology functions as an effective system that improves governance transparency. The research studies concentrate on establishing secure data distribution methods while they ignore the complete process of managing multiple cloud systems.

2.3 Blockchain in Multi-Cloud Environments

Researchers have developed blockchain applications to function across multiple cloud environments because this approach enhances trust and system interoperability. The researchers introduced blockchain-based trust systems to enable secure data transfer between different cloud systems while maintaining data protection and tracking capabilities [5]. Furthermore, blockchain technology has been experimented with as a means to verify data integrity and reduce trust expressed in centralizing authorities over multi-cloud infrastructures [8].

Existing methods focus on trust establishment together with secure communication methods, but they do not include complete governance systems. The fundamental elements of automated regulatory compliance monitoring, together with cross-cloud policy synchronization and scalability modeling, still need better development [6], [3]. The current situation prevents organizations from deploying blockchain technology because of ongoing interoperability issues between different blockchain layers and various cloud system architectures [4].

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15643

2.4 Research Gap

The literature review demonstrates that previous studies researched different parts of cloud governance, which include encryption mechanisms [10], mart contract automation [9], decentralized trust management [5], and blockchain-based audit transparency [6], [7]. However, there exists a major gap in the development of a unified governance architecture that simultaneously includes:

- Granular policy application is an aspect of policy enforcement that can be improved further.
- Ensuring governance synchronization across different cloud providers.
- Use automated techniques to verify regulatory compliance with GDPR and/or CCPA.
- Privacy Preserving Fine Grained Access Control Mechanisms
- Enterprise multi-Cloud environment conceptual scaling modeling

Existing frameworks typically focus either on security enhancement or trust establishment, without providing a complete governance framework that enforces policies and automates compliance and supports interoperability through the implementation of a single decentralized system.

The present research develops a blockchain-based governance framework that supports multi-cloud environments to solve this existing gap. The framework integrates five components, which include permissioned blockchain systems, smart contract-based policy execution, attribute-based encryption, decentralized storage security, and automatic compliance tracking. The research uses formal modeling and conceptual evaluation to develop a regulation-compliant governance system that enables multiple security solutions to work together in a complete system for multi-cloud governance.

3. PROPOSED BLOCKCHAIN-ENABLED GOVERNANCE FRAMEWORK

3.1 Framework Architecture

The projected framework presents a decentralized governance layer designed to operate individualistically of individual cloud service providers while synchronizing governance policies across heterogeneous multi-cloud infrastructures. Let the multi-cloud environment be represented as: The proposed framework establishes a decentralized governance system that functions autonomously from cloud service providers while it implements unified governance standards across diverse multi-cloud systems. The multi-cloud environment should be represented through the following notation:

$$C = \{C1, C2, C3, \dots, Cn\}$$

The system designates each C_i number as a unique cloud service provider which operates its own identity management system and data storage facilities and security policy enforcement tools. The proposed architectural design will establish centralized governance system that will impose policies in all C_i systems while enabling auditing capabilities and maintaining privacy through controlled access.

The overall framework embraces four primary building bricks:
(1) Permissioned Blockchain Governance Layer
(2) Privacy-Preserving Access Control Module
(3) Decentralized Storage Integration Layer
(4) Compliance and Audit Monitoring Module

The governance layer operates as a control plane that maintains neutrality above cloud providers who participate in the system, according to Figure 1. The blockchain layer uses distributed ledger technology to establish tamper-proof records of governance policies, access events, and compliance evidence instead of replacing provider infrastructure. The system maintains interoperability through its separation, which removes the need for centralized trust components.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15643

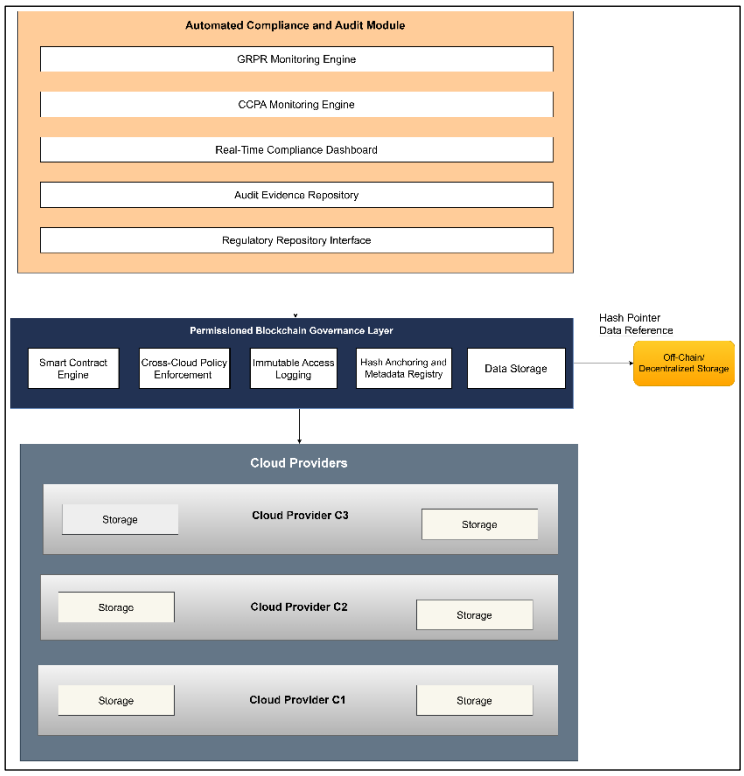

Figure 1: Decentralized Governance Architecture

3.2 Blockchain Governance Layer

The governance backbone uses a permissioned blockchain network as its core system. In this system, only authorized organizational nodes have permission to participate in consensus. The permissioned design establishes trust through distributed systems while the system maintains its unchangeable nature [8], [6].

Everything can be represented as discrete codes in smart contracts, which are singletons, i.e., the ruling vector:

- Access validation rules
- Role-based access control and attribute-based access control
- The conditions for compliance enforcement
- The conditions which trigger audit logging

The smart contract system begins its decision-making process when it receives an access request because it automatically checks all policy conditions before saving its final decision to the ledger. This mechanism guarantees that policy enforcement operates without interference while creating inspection records that can be verified later. The evidence from various enterprise blockchain governance systems shows that smart contracts serve as reliable tools for implementing access control policies and conducting compliance verification processes [11].

The framework achieves two benefits through its decentralization of governance logic because it removes single points of failure and decreases dependence on logging systems that the cloud provider controls.

3.3 Privacy-Preserving Access Control

The model aims to provide accurate control over access permissions and maintain user privacy through an attribute-based encryption (ABE). The model considers access attributes to decide what data is to be encrypted, rather than using predefined user identities. Only users with the required attributes based on the policy of decryption set can decrypt the protected content [10], [7].

The operational working process is as follows:

1. The Data Owner encrypts their data with the help of ABE policy.
2. Encrypted data are stored in the system out of the blockchain network.
3. The system stores hash information together with metadata on the blockchain.
4. The smart contract system confirms the authenticity of access requests.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15643

5. The system distributes decryption keys when policy necessities are met by users.

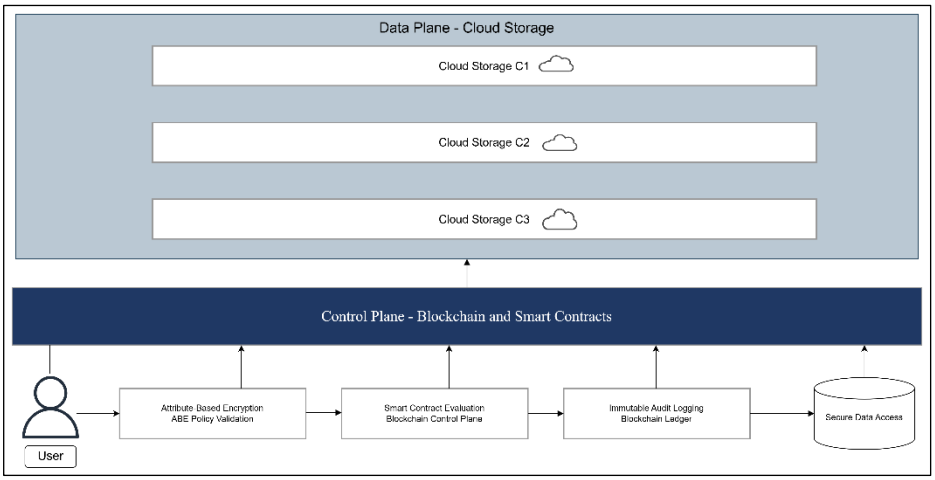

Figure 2. Secure Data Access Framework

Figure 2 shows that blockchain functions as a system that verifies policies and maintains records of accountability, while ABE protects confidential information. The security system uses two layers to enhance access control because it connects authorization decisions through cryptographic methods to permanent audit trails.

3.4 Decentralized Storage Integration

It is inefficient and infeasible to store large amounts of data directly on the blockchain. Hence, the proposed framework incorporates a hybrid storage approach where:

- Data objects are stored in cloud storage solutions or decentralized storage networks.
- Cryptographic hashes, metadata, and references are stored on the blockchain.

This approach is scalable without compromising the verification of data integrity. Each time data is accessed, its integrity is checked by matching the calculated hash with the one recorded on the blockchain.

Organizations that want to use blockchain-based multi-cloud storage systems must establish complete life cycle management procedures, which need to implement integrity tracking methods throughout all storage services [12]. Any form of unacceptable data modifications can be detected using hash mismatch validation, thereby deepening trust and traceability.

3.5 Compliance and Audit Module

The ongoing operation of multi-cloud systems faces difficulties because they must comply with regulatory requirements. The GDPR and CCPA regulations demand organizations to provide clear information about their data processing activities while establishing who has access to their systems and maintaining complete records of their processing activities [13].

The proposed compliance module continuously tracks blockchain transactions while it evaluates governance events through established regulatory standards that are programmed into smart contracts. Automated validation ensures:

- Finally, real-time-watching-over compliance
- Keeping a tab, keeping track of workflows
- Rolling out an immutable ledger
- Compact organizational load

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15643

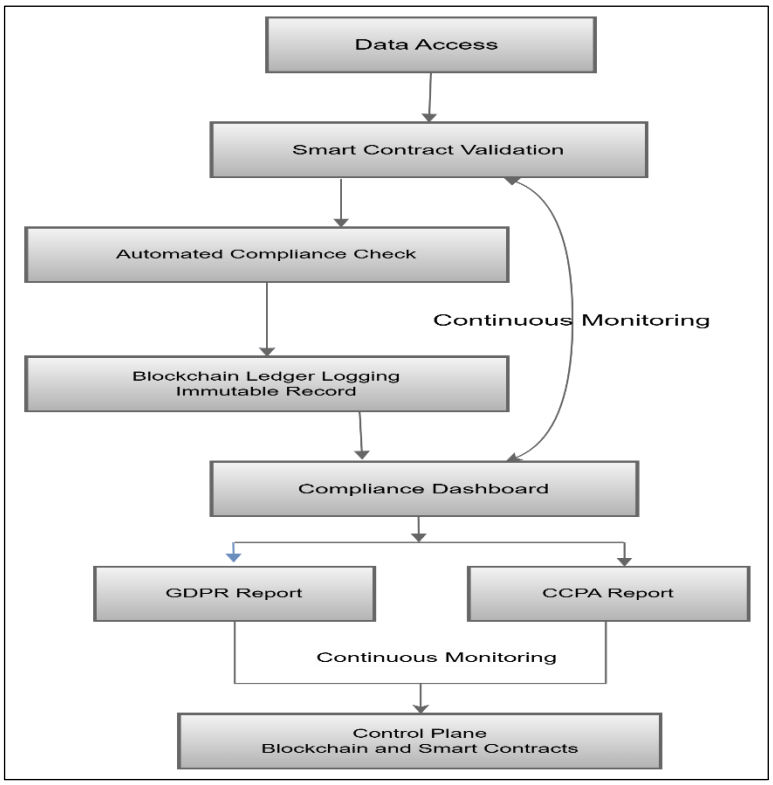

Figure 3. Regulatory Compliance Model

The smart contract system uses regulatory policies to validate compliance through automated system testing. The framework uses compliance rules that are built into its governance framework to detect regulatory violations before they happen, instead of waiting for audits to find problems.

4. EVALUATION AND DISCUSSION

4.1 Evaluation Metrics

The proposed framework is assessed using a conceptual governance-oriented assessment model based on existing research on blockchain-enabled governance and enterprise data management [6], [1], [7]. Because the proposed framework is an architectural contribution, the assessment is based on qualitative and analytical metrics rather than empirical metrics. The following governance performance dimensions are taken into account:

- **Governance Transparency:** The degree to which decisions on access, executions of policy, and efforts of compliance can be traced and verified over a set of multiple cloud domains.
- **Auditability:** Ability to produce tamper-proof and independently verifiable audit trails without dependence on cloud logging infrastructure.
- **Access Accountability:** The extent to which user access activities are cryptographically linked to identity attributes and stored in an immutable fashion.
- **Scalability:** Ability of the governance framework to sustain the same level of policy enforcement efficiency as the number of cloud providers increases.
- **Compliance Readiness:** Extent to which automated compliance with regulatory requirements such as GDPR and CCPA is supported.

In the literature on distributed governance and enterprise systems based on blockchain, these metrics are regarded to be very significant [6], [7], which may provide a structured comparison.

4.2 Comparative Governance Analysis

The proposed architecture is tested for its effectiveness through a conceptual evaluation, which compares traditional centralized cloud governance models with the blockchain-based framework of the study.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15643

Table 1: **Governance Capability Comparison**

Feature	**Centralized Cloud Governance**	**Proposed Blockchain Framework**
Policy Consistency	Limited to Provider Scope	Cross-Cloud Unified Enforcement
Auditability	Provider-Dependent Logs	Immutable & Verifiable Ledger
Privacy Enforcement	Fractional / Role-Based	Strong (ABE + Smart Contracts)
Compliance Computerization	Manual / Semi-Automated	Built-In Smart Contract Logic
Solo Point of Failure	Current	Rejected (Distributed Ledger)

The comparison shows that centralized governance models depend on provider-controlled mechanisms, which create trust requirements and restrict cross-cloud synchronization abilities [2], [1]. On the contrary, the blockchain-based model separates the governance logic and individual cloud providers from builds a distributed trust infrastructure, thus improving resilience and verifiability [8], [6].

4.3 Result Discussion

The evaluation analysis reveals that governance using blockchain technology will be better openness and responsibility to multi-cloud ecosystems. This is because the technology provides a way to record access events and policy states in a permissioned distributed ledger, which ensures that logging is tamper-proof and can be verified independently. This is in relation to the visibility challenges that exist in multi-cloud environments [3], [4].

In terms of scalability, this is what the representation of the governance efficiency function looks like:

$$G(n)$$

where n represents the number of cloud service providers. In centralized governance structures, the efficiency of governance is expected to gradually decrease as n increases. On the other hand, the new decentralized governance structure will ensure that the efficiency of enforcement remains constant, as the verification of policies is carried out by distributed smart contracts that are not dependent on.

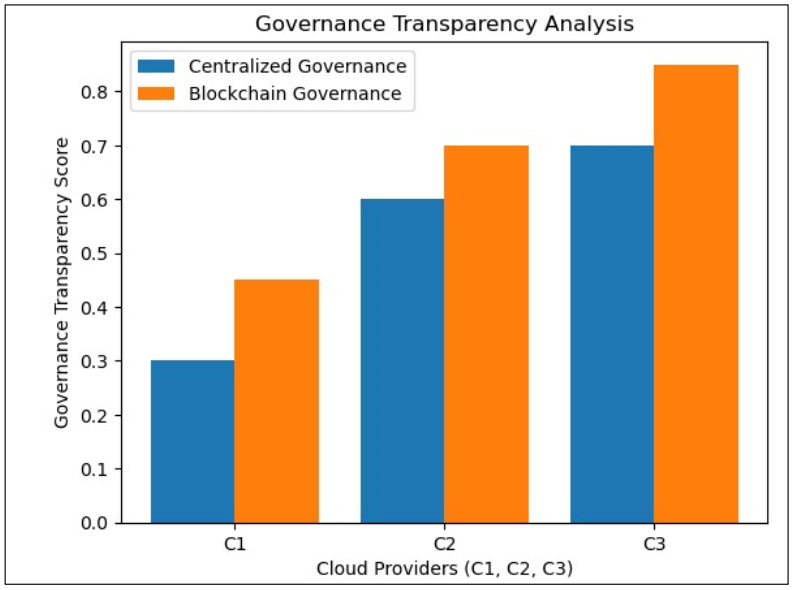

Figure 4: Governance Transparency Analysis

Figure 4 represents the conceptual enhancement in the transparency of governance with the increase in the number of cloud service providers. The blockchain model sustains a constant level of transparency and traceability, whereas the centralized governance model indicates a decreasing level of effectiveness due to the fragmentation of policies across the distributed network.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15643

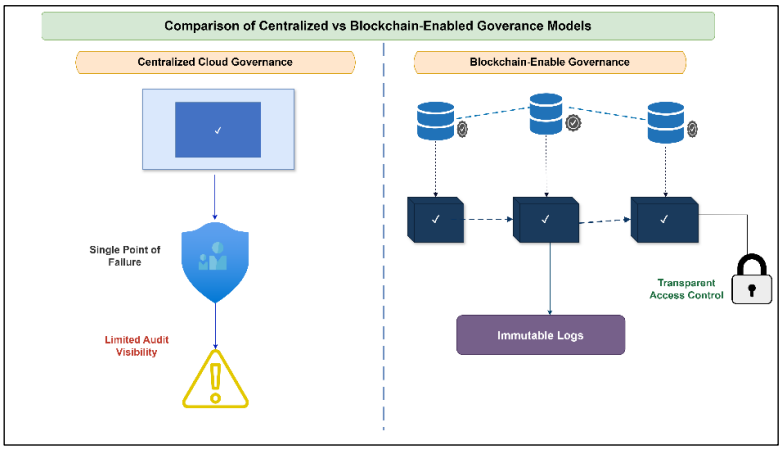

Figure 5. Governance Model Comparison

Figure 5 depicts a systematic architectural comparison between the centralized and decentralized governance models. The architectural design of the decentralized governance model indicates better inter-cloud policy consistency and less trust dependency.

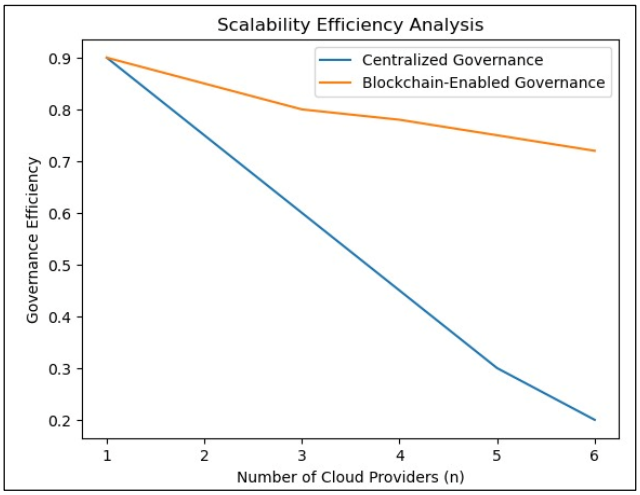

Figure 6. Scalability Efficiency Analysis

Figure 6 illustrates the conceptual scalability behavior of both models. Although the efficiency of centralized governance decreases with the size of the system, the blockchain-enabled framework has a consistent set of performance characteristics because of distributed validation and off-chain storage integration.

Although blockchain causes computational overhead, the permissioned consensus approach and hybrid off-chain storage system reduce latency and scalability issues [7]. By restricting on-chain activities to metadata anchoring and policy enforcement, the framework maintains efficiency while ensuring integrity and transparency.

The assessment above clearly shows that the decentralized blockchain-based governance system is more transparent, auditable, resilient, and regulatory-compliant than the traditional provider-centric governance model. The framework thus provides a feasible architectural solution for secure and scalable governance in a multi-cloud environment.

5. LIMITATIONS AND FUTURE WORK

The blockchain-enabled multi-cloud governance framework, which has been developed, achieves better results in three areas through its improved transparency and auditability and its ability to enforce policies across multiple cloud environments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15643

The framework has achieved its first validation through architectural design and analytical evaluation because it needs to establish its functionality through real-world tests at large scale. The deployment of the system in diverse cloud environments will create operational difficulties, which will stem from three main issues: compatibility problems, increased network delays, and challenges in connecting with current identity and access management systems used by enterprises. The next study will revolve around carrying out real test programs to. evaluate the system performance, software scalability, and operational outcomes as per the normal user conditions.

The system is built on off-chain storage and hash anchoring, to make it scalable. However, this has not been experimented by researchers on how blockchain transaction throughput and smart contract implementation has an impact on system performance. The network will experience delays because users will access permissioned blockchain networks at high frequencies. The research team will analyze system performance through testing, which will measure transaction latency and throughput, storage overhead, and computational cost to determine system efficiency in large-scale multi-cloud environments.

The current system implements its policies in a deterministic manner utilizing laid down policies rules. This method gives a predictable result and allows tracking of the regulations but does not. adjust to changing compliance needs and nonstandard behavior detection. The upcoming study will explore the ways to integrate artificial intelligence-based policy optimization with systems. that detect abnormal activities. Machine learning models can be applied in the governance layer that offer three capabilities: adaptive access control, predictive compliance risk assessment, and automated policy refinement with behavioral analysis.

Additional research needs to be conducted to study these specific research areas:

- Research needs to determine optimal cross-chain interoperability solutions for hybrid and consortium blockchain systems.
- preserving computation techniques use secure multi-party computation and zero-knowledge proofs to enhance data confidentiality protection.
- The development of sustainable energy consumption blockchain networks requires the creation of energy-efficient governance-specific consensus protocols.
- Smart contract security checks are done using formal verification techniques, to remove all known logic-based vulnerabilities.

Conclusively, although the proposed framework provides a systematic and clear governance framework of multi-cloud ecosystems, the future work will focus on empirical validation, smart policy automation, and scalability solutions to enable the conceptual infrastructure to convert into production ready solutions.

6. CONCLUSION

The paper proposed a blockchain-based data privacy and governance model to address the structural shortcomings of traditional governance models in a variety of multi-cloud environments. The proposed architecture provides uniform cross-cloud policy execution, decentralized trust management, and tamper-resilent auditability, by adding a permissioned blockchain control plane that is independent of each cloud provider. The framework employs smart contracts to automate the governance, attribute-based encryption to ensure access is controlled on a very granular basis, and off-chain decentralized storage with hash anchoring to maintain scalability and operation efficiency. Separating the control and data planes makes the architecture even clearer and makes it easier for different cloud infrastructures to work together.
The proposed model shows significant advances in governance transparency, and access accountability, regulatory traceability, and system resilience to single-point failures in contrast to centralized operations of the system. The system also has inbuilt compliance monitoring features to assist in meeting regulatory demands such as GDPR and CCPA and also to ensure readiness to audit in real-time and a uniform policy implementation. The study provides a safe and scalable governance system that helps companies to attain compliance whilst operating their information in multi-cloud settings characterized by complexity.

REFERENCES

[1] A. Katari and M. Ankam, “Data Governance in Multi-Cloud Environments for Financial Services: Challenges and Solutions,” *Int. J. Multidiscip. Curr. Educ. Res.*, vol. 4, no. 1, pp. 339–353, 2022, [Online]. Available: https://www.academia.edu/download/118829041/IJMCER_NN0410339353.pdf
[2] C. Goodness Udeh, “Blockchain-Based Trust and Privacy Preservation in Multi-Cloud Environments,” © *2025 Ijnrd* |, vol. 10, no. 2, pp. 2456–4184, 2025, [Online]. Available: https://doi.org/10.48550/arxiv.2109.14812
[3] Nadia Tabassum, Humaria Naeem, and Asma Batool, “The Data Security and multi-cloud Privacy concerns,” *Int.*

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15643

J. Electron. Crime Investig., vol. 7, no. 1, pp. 49–58, 2023, doi: 10.54692/ijeci.2023.0701128.

[4] N. Paladugu, "European Modern Studies Journal," vol. 9, no. 4, pp. 1304–1315, 2025, doi: 10.59573/emsj.9(4).2025.121.

[5] S. Vethachalam, "Cloud-Driven Security Compliance: Architecting GDPR & CCPA Solutions For Large-Scale Digital Platforms," *Int. J. Technol. Manag. Humanit.*, vol. 10, no. 4, p. 2024, 2024, doi: 10.21590/ijtmh.2024100406.

[6] Z. Li, F. Liang, and H. Hu, "Blockchain-Based and Value-Driven Enterprise Data Governance: A Collaborative Framework," *Sustain.*, vol. 15, no. 11, 2023, doi: 10.3390/su15118578.

[7] J. Zhang and A. Datta, "Blockchain-enabled data governance for privacy-preserved sharing of confidential data," *PeerJ Comput. Sci.*, vol. 10, pp. 1–48, 2024, doi: 10.7717/peerj-cs.2581.

[8] S. Somanathan, "Blockchain For Data Integrity In Multi-Cloud Environments: A Project Management Approach," *Nanotechnol. Perceptions (ISSN 1660-6795)*, vol. 20, p. 13, 2024.

[9] B. Kumar, "Challenges and Solutions for Integrating AI with Multi-Cloud Architectures," vol. 1, no. 1, pp. 71–77, 2022.

[10] M. Fernández, A. F. Tapia, J. Jaimunk, M. M. Chamorro, and B. Thuraisingham, "A data access model for privacy-preserving cloud-iot architectures," *Proc. ACM Symp. Access Control Model. Technol. SACMAT*, no. February, pp. 191–202, 2020, doi: 10.1145/3381991.3395610.

[11] P. Saha and M. Vaithianathan, "Blockchain-Enabled Secure Data Management in Cloud-Based High-Performance Computing Systems," vol. 6, no. 1, pp. 30–41, 2025.

[12] P. M. B. Muddumadappa, S. D. K. Anjanappa, and M. Srikantaswamy, "An Efficient Reconfigurable Cryptographic Model for Dynamic and Secure Unstructured Data Sharing in Multi-Cloud Storage Server," *J. Intell. Syst. Control*, vol. 1, no. 1, pp. 68–78, 2022, doi: 10.56578/jisc010107.

[13] Sanjay Kanth Balachandar, "Blockchain-enabled Data Governance Framework for Enhancing Security and Efficiency in Multi-Cloud Environments through Ethereum, IPFS, and Cloud Infrastructure Integration," *J. Electr. Syst.*, vol. 20, no. 5s, pp. 2132–2139, 2024, doi: 10.52783/jes.2555.

