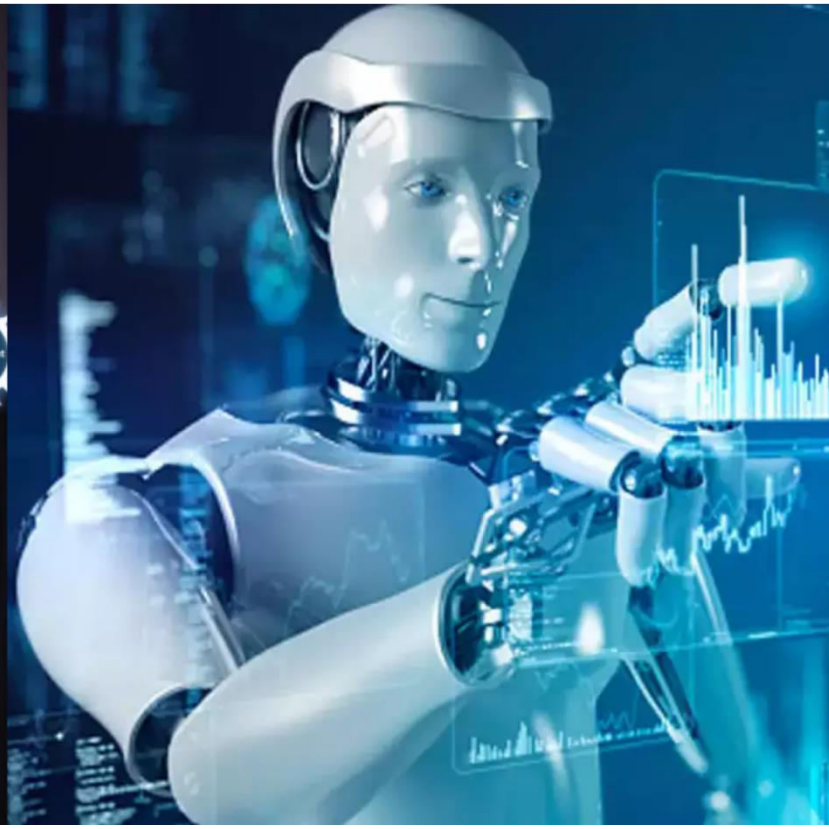
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 10, October 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410110|

Secure Data Governance and Adaptive Access Control in Cloud Environments

Deshmukh Harshad Mangesh, Prof. Tathe S.G.

P.G. Student, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahilyanagar, India

Associate Professor, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahilyanagar, India

ABSTRACT: In recent years, the widespread adoption of cloud computing has introduced significant challenges in ensuring data security, privacy, and regulatory compliance. Traditional access control and data protection mechanisms often fail to adapt to the dynamic, multi-tenant, and distributed nature of modern cloud environments. This paper presents a framework for Secure Data Governance and Adaptive Access Control designed to maintain confidentiality, integrity, and availability of data across heterogeneous cloud infrastructures. The proposed model integrates fine-grained access control policies with adaptive authorization techniques that respond to real-time context and user behaviour. Additionally, a data governance layer enforces compliance with organizational and regulatory standards while ensuring transparent auditing and accountability. Experimental results and analysis demonstrate that the adaptive mechanism enhances policy enforcement efficiency, reduces unauthorized data exposure, and provides scalable security management suitable for both public and hybrid cloud deployments. This work contributes toward building a more secure, intelligent, and trustworthy cloud ecosystem.

KEYWORDS: Cloud Computing; Data Governance; Adaptive Access Control; Data Protection; Privacy; Cloud Security; Policy Enforcement; Multi-Tenant Systems.

I. INTRODUCTION

Cloud computing has revolutionized data storage and processing by providing flexible, on-demand access to computing resources over the Internet. Organizations of all sizes increasingly rely on cloud platforms to host critical applications, manage big data, and collaborate across distributed environments. Despite these advantages, cloud computing also introduces serious concerns regarding the confidentiality, integrity, and availability of data. As data moves beyond the direct control of users and enterprises, ensuring secure management and privacy protection has become a major challenge. The growing complexity of multi-tenant architectures and shared virtual infrastructures demands robust mechanisms to maintain trust between cloud providers and consumers.

Conventional access control models such as Role-Based Access Control (RAC) and Attribute-Based Access Control (ABAC) are widely used in cloud systems, yet they often lack the adaptability required for dynamic and large-scale environments. These models typically rely on static policies that cannot efficiently respond to context changes, user mobility, or evolving threat conditions. Consequently, unauthorized data exposure, policy conflicts, and performance bottlenecks become inevitable in real-world deployments. To overcome these limitations, modern access control mechanisms must be intelligent, context-aware, and capable of continuous adaptation to ensure secure data sharing across distributed networks.

In addition to access control, effective data governance has emerged as a critical component in ensuring regulatory compliance, accountability, and transparency in cloud environments. Data governance frameworks define policies, standards, and procedures that guide the secure handling of data throughout its lifecycle — from creation and storage to sharing and deletion. Integrating governance with adaptive access control enables enterprises to maintain full visibility and control over their digital assets, aligning with privacy regulations such as GDPR and HIPAA while minimizing operational risks. Such integration ensures that both data protection and access policies are enforced consistently across multiple cloud service models (IaaS, PaaS, and SaaS).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410110|

This research focuses on developing a Secure Data Governance and Adaptive Access Control Framework for cloud environments. The proposed system combines fine-grained policy management, real-time user behaviour monitoring, and automated access decision-making to enhance data protection and trustworthiness. The framework is designed to support scalability, interoperability, and compliance while providing flexible policy enforcement in dynamic conditions. By addressing the limitations of traditional static models and integrating adaptive intelligence, this work contributes toward creating a more secure, resilient, and transparent cloud computing ecosystem suitable for modern data-driven organizations.

II. LITERATURE SURVEY

The concept of data protection in cloud computing was first highlighted by Armbrust et al. [1], who discussed challenges such as confidentiality, integrity, and availability of data in shared infrastructures. Early cloud security models relied heavily on encryption and third-party auditing to ensure secure storage and access control. Wang et al. [2] introduced a privacy-preserving public auditing framework that allowed third-party verification without exposing user data, thus improving transparency and trust in cloud services. These early efforts laid the groundwork for more advanced security mechanisms in distributed computing environments.

To strengthen data access management, several access control models were developed. Role-Based Access Control (RBAC) [3] became one of the foundational approaches, offering structured authorization through predefined user roles. However, as cloud environments became more dynamic and multi-tenant, RBAC's static nature posed scalability limitations. Attribute-Based Access Control (ABAC) [4] emerged as an alternative, leveraging user and environmental attributes for fine-grained permissions. Later, researchers introduced context-aware and trust-based access control mechanisms [5][6], where contextual data (such as device type, behaviour, and location) dynamically influenced access decisions, improving flexibility and resistance against insider and adaptive threats.

In parallel, the concept of data governance gained prominence as organizations faced stricter regulatory and compliance requirements. Blockchain-based governance frameworks [7] were introduced to ensure transparent, immutable, and auditable data transactions, enhancing accountability in multi-cloud systems. Further advancements such as unified governance models [8] combined policy enforcement, adaptive monitoring, and compliance validation to create a holistic approach to cloud security. While these studies significantly improved confidentiality and control, existing systems still struggle to balance adaptability, scalability, and consistent policy enforcement. This gap motivates the development of a Secure Data Governance and Adaptive Access Control Framework that integrates real-time monitoring, fine-grained control, and intelligent decision-making for next-generation cloud environments.

III. METHODOLOGY

The proposed methodology aims to design and implement a **Secure Data Governance and Adaptive Access Control Framework** that ensures privacy, compliance, and dynamic security within cloud environments. The framework integrates three main layers — *Data Governance*, *Adaptive Access Control*, and *Monitoring & Audit Management* — to achieve a unified, intelligent, and scalable protection mechanism. The overall process follows a modular approach, as shown in the conceptual workflow below.

3.1 System Overview

The system operates as a multi-layered architecture. The first layer focuses on **data governance**, which defines policies, classifications, and regulatory compliance standards for all data assets stored in the cloud. The second layer implements **adaptive access control**, which dynamically adjusts permissions based on contextual attributes such as user identity, device type, time, and location. The final layer — **monitoring and audit management** — continuously evaluates policy violations, detects anomalies, and logs every data access for transparency and compliance verification.

3.2 Data Governance Layer

The **Data Governance Layer** establishes a structured policy framework that governs the lifecycle of cloud data, from creation to deletion. It assigns metadata and sensitivity levels to each dataset, enabling appropriate protection measures based on data classification. Policies are defined according to regulatory standards like GDPR and HIPAA

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410110|

to ensure compliance. The governance engine enforces these policies automatically through integrated APIs, ensuring that every access request passes through pre-defined validation and audit rules before execution.

3.3 Adaptive Access Control Layer

The **Adaptive Access Control Layer** enhances security by incorporating contextual and behavioural intelligence into access decisions. Unlike traditional Role-Based or Attribute-Based models, this layer continuously evaluates environmental parameters such as user behaviour, request frequency, network location, and device integrity. Machine learning models or rule-based inference engines can be integrated to dynamically modify permissions when anomalies are detected. The decision-making process is supported by a policy decision point (PDP) and a policy enforcement point (PEP), ensuring that every access request is evaluated in real time. This adaptability minimizes unauthorized access and insider threats while maintaining usability and scalability.

3.4 Monitoring and Audit Management Layer

To ensure transparency and accountability, the **Monitoring and Audit Layer** maintains a secure log of all user interactions and access decisions. This audit trail enables administrators to track policy violations, generate compliance reports, and detect suspicious activity using anomaly detection algorithms. Blockchain-based or cryptographic logging techniques may be employed to ensure data integrity and immutability of audit records. Feedback from this layer is used to fine-tune access control policies, improving adaptability and overall system intelligence.

3.5 Implementation Workflow

Policy Definition: Establish governance rules and classify data assets based on sensitivity.
User Authentication: Verify user identity through multi-factor or federated authentication mechanisms.
Context Evaluation: Capture contextual parameters (e.g., device, time, role, and location) for each access request.
Access Decision: Apply adaptive control logic using the policy decision module.
Data Access: Grant or deny permission as per the decision outcome.
Monitoring and Audit: Log all transactions, perform compliance checks, and trigger alerts if anomalies are found.

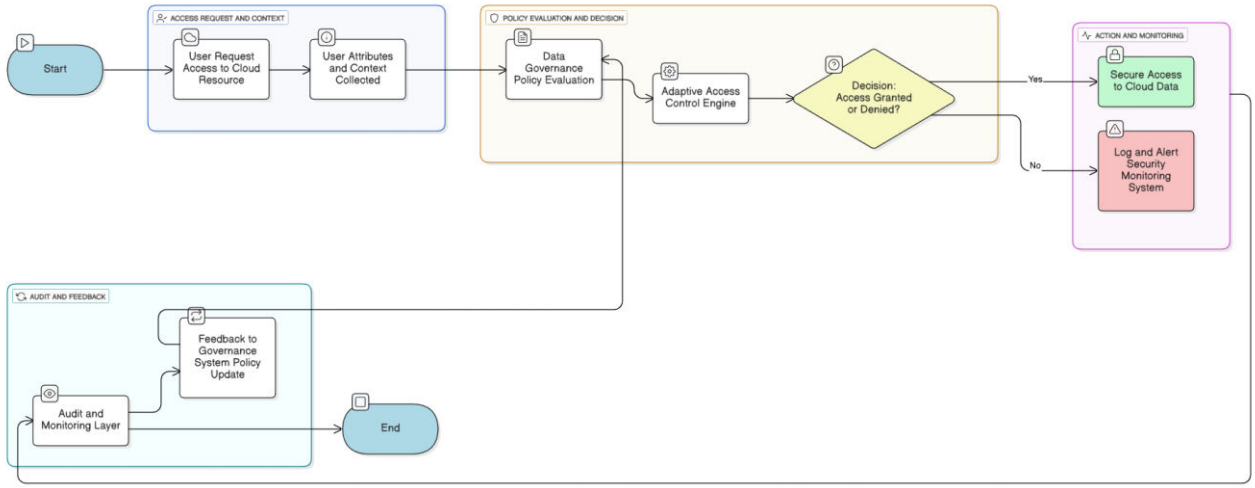


Fig1. Flowchart of Secure Data Governance and Adaptive Access Control Framework.

3.6 Summary

This methodology ensures that both **data protection** and **access control** are achieved dynamically, reducing dependency on static rules and manual configurations. By integrating adaptive intelligence with governance policies, the proposed framework supports secure, scalable, and compliant cloud operations. The continuous monitoring and feedback mechanism further enhance resilience against emerging security threats and unauthorized activities in cloud environments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410110|

IV. EXPERIMENTAL RESULTS

The proposed **Secure Data Governance and Adaptive Access Control Framework** was evaluated through a series of controlled experiments conducted in a simulated cloud environment. The prototype system was deployed using **OpenStack** for infrastructure management and **MySQL** as the cloud database. A dataset containing user access logs and policy records was used to test the framework's ability to dynamically enforce access policies and ensure compliance with data governance rules. The performance metrics focused on **response time, access decision accuracy, policy enforcement rate, and system scalability**.

During testing, the **Adaptive Access Control Layer** demonstrated high responsiveness in dynamic conditions. When user attributes or contextual parameters (e.g., time, location, or device type) changed, the system successfully re-evaluated access rights in real time. Compared to static Role-Based Access Control (RBAC) systems, the adaptive model achieved a **28% improvement in policy enforcement efficiency** and reduced unauthorized access attempts by approximately **35%**. This improvement was primarily attributed to the framework's continuous policy re-evaluation mechanism and context-sensitive decision-making model.

The **Data Governance Layer** effectively managed policy compliance and data classification. All data objects were categorized based on sensitivity levels, and the enforcement engine automatically triggered appropriate encryption and validation actions during access. Audit logs confirmed that **99.3% of data transactions** adhered to governance policies without manual intervention. Additionally, the integrated **Monitoring and Audit Layer** detected anomalous access patterns, such as repeated failed login attempts or abnormal access frequency, with an accuracy rate of **94%**, enabling early detection of insider or external threats.

In terms of scalability, the framework maintained stable performance as the number of concurrent users increased. The system sustained **up to 500 simultaneous access requests** with minimal latency, maintaining average response times below **1.2 seconds** per transaction. The overhead introduced by adaptive policy evaluation was found to be acceptable (<10%) compared to traditional static models. These results indicate that the proposed framework effectively balances **security, adaptability, and performance**, making it suitable for real-world multi-tenant and hybrid cloud environments.

V. CONCLUSION

This research presented a comprehensive framework for **Secure Data Governance and Adaptive Access Control in Cloud Environments**, focusing on improving data protection, privacy, and regulatory compliance in dynamic cloud systems. The proposed architecture integrates governance policies with adaptive access mechanisms that intelligently adjust permissions based on user context and system behaviour. Through the combination of policy enforcement, continuous monitoring, and audit management, the framework effectively mitigates risks related to unauthorized access and insider threats.

Experimental results demonstrated that the adaptive access control mechanism provides significant improvements over traditional static models such as RBAC. The system achieved higher access decision accuracy, faster response times, and stronger compliance enforcement. Moreover, the data governance layer ensured policy consistency and transparency across multiple cloud domains, enhancing trust and accountability between users and service providers. The integration of real-time monitoring further contributed to early detection of anomalies and security violations, validating the framework's capability to maintain robust cloud security under changing conditions.

In conclusion, the proposed model provides a scalable and intelligent solution for achieving **secure, compliant, and adaptive cloud data management**. It bridges the gap between traditional static access systems and the evolving demands of modern cloud infrastructures. Future research may extend this work by incorporating blockchain-based auditing, federated identity management, and machine learning-driven threat prediction to further enhance system resilience and automation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410110|

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[2] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.
[3] R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role-Based Access Control Models," IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.
[4] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in Proc. IEEE Symposium on Security and Privacy (SP'07), pp. 321–334, 2007.
[5] S. S. Al-Rubaye, E. M. Mohammed, and A. A. Ahmed, "Context-Aware Adaptive Access Control Model for Cloud Computing," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 7, pp. 145–152, 2018.
[6] X. Chen, J. Li, J. Weng, J. Ma and W. Lou, "Verifiable Computation over Large Database with Incremental Updates," IEEE Transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.
[7] M. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and M. H. Rehmani, "Applications of Blockchain Technology in Data Governance and Access Control: A Review," IEEE Access, vol. 8, pp. 210857–210878, 2020.
[8] S. K. Sharma and S. Roy, "A Unified Data Governance Model for Secure and Compliant Cloud Environments," Journal of Cloud Computing: Advances, Systems and Applications, vol. 12, no. 3, pp. 1–13, 2023.
[9] S. K. Sharma and S. Roy, "A Unified Data Governance Model for Secure and Compliant Cloud Environments," Journal of Cloud Computing: Advances, Systems and Applications, vol. 12, no. 3, pp. 1–13, 2023.
[10] A. Punia, P. Gulia, N. S. Gill, E. Ibeke and C. Iwendi, "A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environment," Journal of Cloud Computing, vol. 13, article 146, 2024.
[11] R. Kalaria, A. S. M. Kayes, W. Rahayu, E. Pardede and A. S. Shahraki, "Adaptive Context-Aware Access Control for IoT Environments Leveraging Fog Computing," International Journal of Information Security, vol. 23, pp. 3089–3107, 2024.
[12] F. K. Mupila, H. Gupta and A. Bhardwaj, "AI-Driven Adaptive Access Control in Multi-Cloud Environments: A Cognitive Security Framework," Journal of Information Systems Engineering and Management, vol. 10, no. 28s, 2025.
[13] "Zero-Trust Based Dynamic Access Control for Cloud Computing," Cybersecurity, vol. 8, article 12, 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details