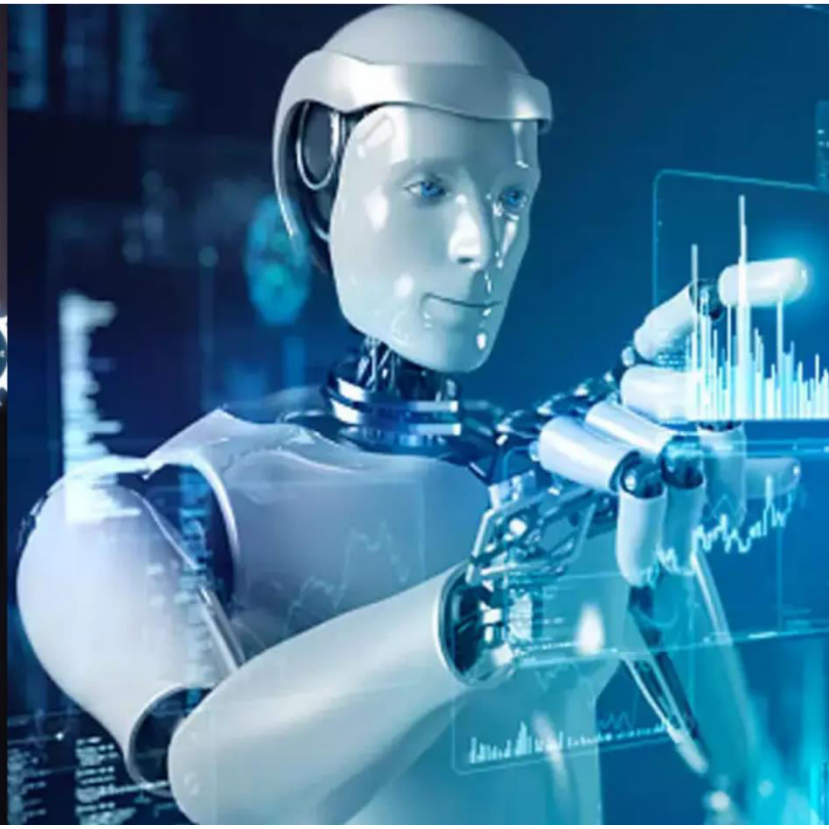
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 11, November 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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411024|

Data Security of Dynamic and Robust Role Based Access Control from Multiple Authorities in Cloud Environment

Kavita Tatyaba Kad[1], Prof.S. C. Puranik[2]

ME Student, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahilyanagar, Maharashtra, Savitribai Phule Pune University, Pune, India[1]

Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahilyanagar, Maharashtra, Savitribai Phule Pune University, Pune, India[2]

ABSTRACT: In the modern era of digital transformation, cloud computing has become a vital technology for storing and managing massive volumes of data. However, ensuring data security and privacy in distributed cloud environments remains one of the most critical challenges. The proposed project aims to provide a secure, efficient, and flexible access control mechanism that protects sensitive cloud data from unauthorized access. The system is developed as a Java-based web application that implements Role-Based Access Control (RBAC) techniques to manage user permissions dynamically. By distributing the data into multiple chunks and storing them across different nodes in a simulated cloud environment (localhost setup), the system enhances confidentiality and reduces the risk of data breaches. The project introduces four main modules - User, Data Owner, Third Party Auditor (TPA), and Investigator—each designed to ensure security and accountability in the cloud ecosystem. The Data Owner module manages secure data sharing and revocation, while the User module ensures that only authorized users can access the required data based on predefined roles. The TPA validates and verifies user access requests to ensure authenticity, and the Investigator module monitors suspicious activity, analyzing the probability of unauthorized access or insider threats. The integration of these modules ensures not only data protection but also dynamic and efficient access control, enabling real-time monitoring and secure data transactions. Overall, this project demonstrates how the combination of RBAC and multi-authority validation can enhance cloud data security. By applying cryptographic techniques and robust access verification protocols, it minimizes data vulnerability and provides a reliable framework for secure cloud-based data management. The system's modular structure, scalability, and flexibility make it adaptable to various organizational scenarios, promoting secure and privacy-preserving data sharing in multi-user and distributed environments.

KEYWORDS: - Cloud Computing, Data Security, Role-Based Access Control (RBAC), Distributed Environment, Data Chunking, Third Party Auditor (TPA), Investigator Module, Java Web Application, Data Encryption, Access Revocation, etc.

I. INTRODUCTION

demand resources over the internet. However, the shared and distributed nature of cloud infrastructure introduces significant security concerns, especially regarding data access, integrity, and privacy. Traditional access control mechanisms are often insufficient to handle the complexities of multi-user, multi-tenant cloud environments where different users possess varying access privileges. In this context, implementing a dynamic and robust Role-Based Access Control (RBAC) system offers a structured and flexible way to manage permissions based on user roles, responsibilities, and authority levels.

The proposed system focuses on designing a secure and efficient cloud data management framework that prevents unauthorized access and misuse of sensitive information. Using Java technology, the system simulates a distributed cloud setup on a localhost, where files or data are divided into multiple encrypted chunks and stored across different nodes. This approach ensures that even if one part of the system is compromised, the complete data remains secure. The RBAC mechanism dynamically assigns, updates, and revokes user permissions based on the actions and requests

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411024|

made within the cloud environment. Additionally, the use of multiple authorities for access validation ensures that data access is verified through a trusted multi-party authentication process.

To further strengthen security, the project integrates the roles of Data Owner, User, Third Party Auditor (TPA), and Investigator. The Data Owner securely uploads and manages data access permissions, while the User accesses data only within authorized limits. The TPA independently verifies the user's credentials and ensures the integrity of the stored data, while the Investigator monitors potential threats or irregular activities to detect unauthorized attempts. This layered security model enhances reliability, reduces vulnerabilities, and ensures accountability across all access points. The system ultimately contributes to achieving secure, transparent, and scalable data management within a cloud-based environment.

PROBLEM STATEMENT

Traditional cloud storage systems face security risks like unauthorized access, data leakage, and poor role management. There is a lack of dynamic and multi-authority-based mechanisms that can effectively handle user authentication, data revocation, and auditing. Hence, a secure and robust system is needed that can ensure only verified users can access data while detecting and preventing malicious activities.

II. LITERATURE SURVEY

- **J. Umamageswaran et al. (2025)** In their research titled "Developing a More Adaptive and Dynamic Trust Evaluation System Using a Task Role Based Access Control Module (T-RBAC)", the authors present a dynamic and flexible trust evaluation model that extends the traditional Role-Based Access Control (RBAC) by integrating task-oriented trust management. The T-RBAC model adapts user permissions dynamically based on task context and trust levels, thereby enhancing decision-making in real-time collaborative cloud systems. The study highlights the significance of continuous trust assessment for improving security, especially in environments where users' roles and responsibilities frequently change. The proposed system leverages user behavioral analysis and trust score calculation to mitigate risks associated with malicious insiders or unauthorized access. Through simulation results, the authors demonstrate that the T-RBAC framework provides higher adaptability, reduced access delay, and improved accuracy in trust-based decision making compared to static RBAC models, making it highly suitable for dynamic cloud and distributed computing environments.

- **Y. Zhu et al. (2024)** In "From RBAC to ABAC: Constructing Flexible Data Access Control for Cloud Storage Services", the authors propose an innovative transition model from Role-Based Access Control (RBAC) to Attribute-Based Access Control (ABAC) to enable fine-grained and context-aware access control in cloud storage systems. This research emphasizes flexibility, scalability, and expressiveness by incorporating user, resource, and environmental attributes into the access policy framework. The paper outlines the limitations of RBAC in managing dynamic cloud environments and demonstrates how ABAC overcomes these challenges by supporting multi-dimensional attribute mapping and logical policy enforcement. The proposed hybrid model ensures seamless policy migration between RBAC and ABAC, enabling organizations to maintain legacy access structures while progressively adopting modern access paradigms. Experimental evaluations confirm that the system enhances access precision and security efficiency with minimal computational overhead, thus offering a balanced approach between usability and security for large-scale cloud deployments.

- **J. Mao (2024)** In the paper "Multi-authority attribute encryption scheme based on cloud computing verifiable outsourcing decryption", J. Mao introduces a novel encryption model for secure and verifiable data sharing in cloud computing environments. The proposed approach uses a multi-authority Attribute-Based Encryption (ABE) system that distributes key management responsibilities across different authorities to prevent single-point failures and insider attacks. Furthermore, the scheme supports outsourcing of the decryption process to the cloud while maintaining verifiability and data confidentiality. This significantly reduces the computational burden on end users while ensuring that the outsourced results are authentic and trustworthy. The paper also introduces mathematical formulations for secure key generation, encryption, and decryption validation to guarantee correctness. Simulation results show that the system achieves strong resistance against collusion attacks, minimizes key exposure risk, and maintains high computational efficiency, making it highly suitable for secure data access in distributed cloud infrastructures.

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411024|

- **B. Pei et al. (2022)** The study "Lattice-Based Fine-grained Data Access Control and Sharing Scheme in Fog and Cloud Computing Environments for the 6G Systems" proposes a lattice-based cryptographic framework for securing data sharing in 6G-enabled fog and cloud computing systems. The authors utilize lattice-based encryption to construct a fine-grained and quantum-resistant access control mechanism capable of handling massive data flows across interconnected fog nodes. This model supports flexible access delegation and revocation without re-encryption, thereby improving system efficiency and scalability. The proposed system ensures data confidentiality, integrity, and traceability through mathematical lattice hardness assumptions that resist future quantum attacks. Experimental evaluations demonstrate the effectiveness of this scheme in terms of reduced computation time, low communication cost, and robust resistance to adversarial access. The research contributes significantly to the development of post-quantum cryptography-based access control mechanisms for next-generation cloud ecosystems.

- **Z. Yan et al. (2017)** In their work "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing", the authors propose a trust-driven access control framework that integrates user reputation scores to manage access permissions dynamically in cloud environments. The system evaluates user reliability through behavior tracking and trust propagation models to enhance the robustness of traditional RBAC schemes. The proposed approach ensures that only trustworthy users are granted access to sensitive data, thus minimizing the probability of insider threats and malicious behaviors. The paper also emphasizes the use of reputation aggregation and trust decay models to maintain fairness and adaptiveness in long-term cloud collaborations. The experimental outcomes reveal that this hybrid trust-RBAC mechanism improves security decision accuracy and reduces unauthorized access occurrences. This research provides an essential foundation for developing adaptive and context-aware access control systems that align with evolving user trustworthiness in distributed cloud frameworks.

III. SYSTEM OVERVIEW

The overall system is designed to ensure secure cloud data management using distributed storage, multi-level access control, and continuous monitoring. The process begins when the Data Owner uploads data to the system. Before storage, the data is encrypted and divided into multiple chunks that are distributed across several nodes to simulate a cloud environment. The Data Owner assigns roles and permissions to users based on the RBAC model, determining which users can view, modify, or delete specific files. The system ensures that access privileges are not static but dynamically updated as user roles or organizational needs change.

When a User attempts to access data, the system forwards the request to the Third Party Auditor (TPA), which verifies the user's identity and access rights. The TPA checks digital signatures, validates user credentials, and ensures that the data integrity is maintained. If verification is successful, access is granted; otherwise, the system denies access and logs the event for investigation. The Investigator module periodically reviews logs and analyzes abnormal access patterns to detect insider threats or unauthorized intrusion attempts. In the event of a detected anomaly, it calculates the attack probability and generates alerts to the administrator for corrective actions.

From an implementation perspective, the system leverages Java-based technologies for backend operations, MySQL for secure data storage, and web interfaces for user interaction. The modular structure ensures easy maintenance and future scalability. This framework not only secures cloud-stored data but also improves trust through transparency, auditability, and multi-authority collaboration. By combining RBAC with distributed data management and intelligent monitoring, the proposed system provides a comprehensive solution for ensuring data confidentiality, integrity, and availability in modern cloud environments.

IV. PROPOSED SYSTEM

The proposed system introduces a secure and intelligent cloud data access framework using a combination of Role-Based Access Control (RBAC) and multi-authority verification. It is implemented as a Java-based web application that simulates a distributed cloud environment by dividing data into multiple encrypted chunks and storing them across different nodes within the localhost setup. This distributed data storage mechanism ensures that even if one chunk is compromised, the entire dataset remains protected. The RBAC model dynamically manages user permissions based on assigned roles and privileges, ensuring that only authorized users can perform specific actions such as data upload, sharing, modification, or deletion.

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411024|

The system architecture includes four key modules: User, Data Owner, Third Party Auditor (TPA), and Investigator. The Data Owner uploads and manages data files, defines user roles, and can revoke access dynamically. The User module facilitates secure data access, ensuring that users can only retrieve data they are permitted to. The TPA module acts as a neutral validator that authenticates user access requests, verifies the integrity of stored data, and audits access logs. The Investigator module monitors and analyzes system logs to detect suspicious activities or unauthorized access attempts, providing a probability score for potential attacks. These components collectively enhance trust, transparency, and accountability in the system.

In addition to RBAC, the system employs cryptographic techniques such as encryption and hashing to secure data at rest and in transit. A two-step verification process further strengthens the authentication mechanism, while access revocation ensures immediate denial of rights when a user no longer needs access. The modular design of the proposed framework makes it highly adaptable to different organizational needs and scalable for future integration with real cloud infrastructures. Overall, the system aims to create a secure, dynamic, and auditable environment for data storage and sharing in the cloud.

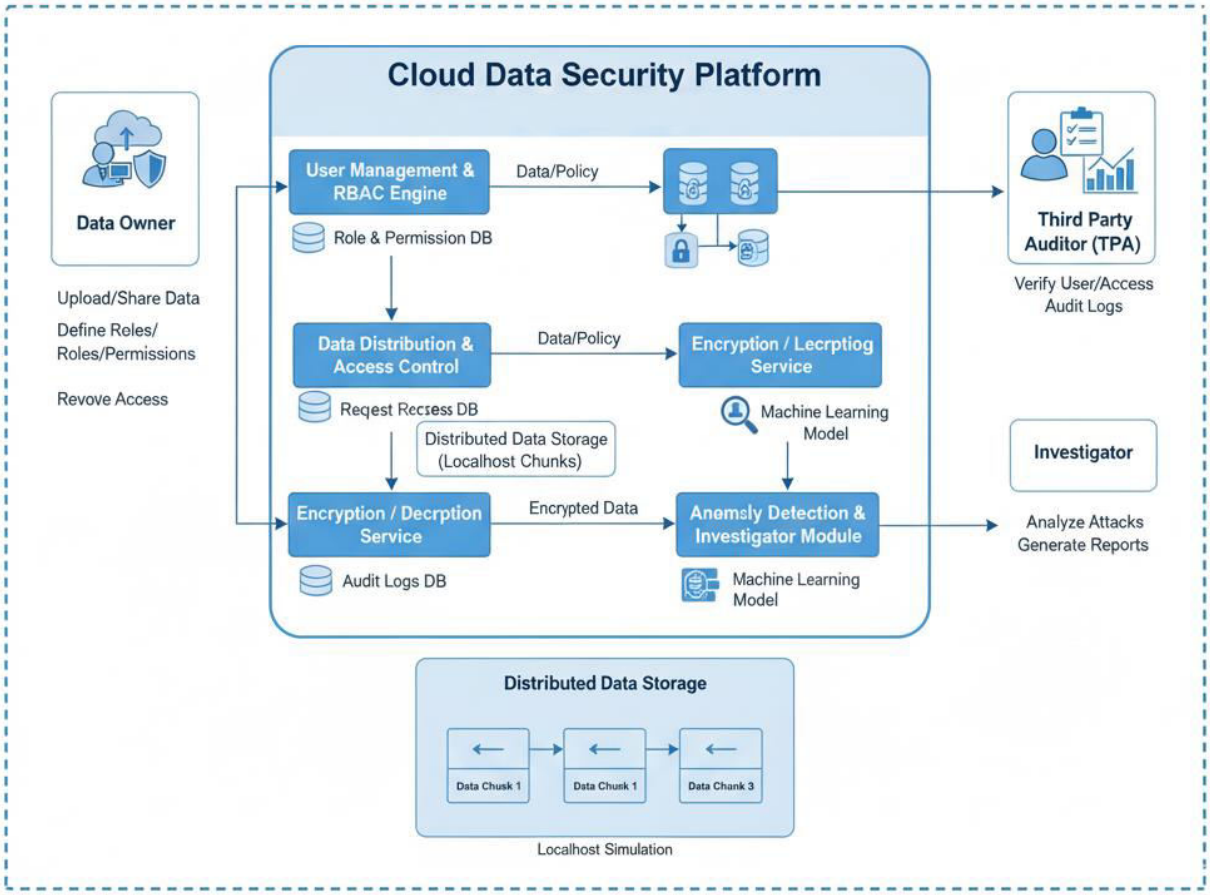


Fig.1: System Architecture Design

V. CONCLUSON

In this paper the proposed system effectively demonstrates a secure and reliable approach for managing cloud data access in a distributed environment. By integrating Role-Based Access Control (RBAC) with multi-authority validation, the system ensures that only authorized users can access sensitive data. The use of data chunking and encryption provides enhanced data confidentiality, while Third Party Auditor (TPA) and Investigator modules enable continuous monitoring and validation of user actions, making the system highly resistant to unauthorized access and insider threats.

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411024|

The design and implementation of this Java-based web application show that secure cloud data management is achievable without compromising usability. Each module, from user access and data sharing to auditing and investigation, works together to maintain integrity, trust, and accountability. The multi-authority framework adds flexibility, allowing dynamic role updates and real-time verification while preventing single points of failure, making the system robust for real-world deployment in organizations or multi-user cloud environments.

VI. ACKNOWLEGEMENT

I would like to sincerely thank the researchers and publishers for making their valuable resources available. I am also grateful to my guide for their constant support and guidance, and to the reviewers for their insightful suggestions. Finally, I thank the college authorities for providing the necessary infrastructure and support throughout the course of this project.

REFERENCES

1. J. Umamageswaran, A. Shivakumar, A. S. Varshith and P. M, "Developing a More Adaptive and Dynamic Trust Evaluation System Using a Task Role Based Access Control Module (T-RBAC)," 2025 International Conference on Data Science and Business Systems (ICDSBS), Chennai, India, 2025, pp. 1-5, doi: 10.1109/ICDSBS63635.2025.11031714.
2. Y. Zhu, D. Huang, C. -J. Hu and X. Wang, "From RBAC to ABAC: Constructing Flexible Data Access Control for Cloud Storage Services," in IEEE Transactions on Services Computing, vol. 8, no. 4, pp. 601-616, 1 July-Aug. 2024, doi: 10.1109/TSC.2024.2363474.
3. J. Mao, "Multi-authority attribute encryption scheme based on cloud computing verifiable outsourcing decryption," 6th International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM 2024), Hybrid Conference, Frankfurt, Germany, 2024, pp. 99-106, doi: 10.1049/icp.2024.4209.
4. B. Pei, X. Zhou and R. Jiang, "Lattice-Based Fine-grained Data Access Control and Sharing Scheme in Fog and Cloud Computing Environments for the 6G Systems," 2022 18th International Conference on Mobility, Sensing and Networking (MSN), Guangzhou, China, 2022, pp. 563-570, doi: 10.1109/MSN57253.2022.00094.
5. Z. Yan, X. Li, M. Wang and A. V. Vasilakos, "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2469662.
6. W. K. Roslin Dayana, “Trust Aware Cryptographic Role Based Access Control,” Annals of Telecommunications, 2023.
7. S. Luo, “A New Access Control Method Based on Multi-Authority in Cloud Storage Services,” International Journal of Computational Intelligence Systems, 2018.
8. Pribadi Kalapaaking, I. Khalil, M. S. Rahman, A. Bouras, “Blockchain-based Access Control for Secure Smart Industry Management Systems,” 2023.
9. J. Liu, H. Tang, C. Li, R. Sun, X. Du, M. Guizani, “vFAC: Fine-Grained Access Control with Versatility for Cloud Storage,” 2018.
10. N. H. Sultan, V. Varadharajan, L. Zhou, F. A. Barbhuiya, “A Role-Based Encryption Scheme for Securing Outsourced Cloud Data in a Multi-Organization Context,” 2020.

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