IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

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

Ms. Kavita Tatyaba Kad[1], Dr. M. R. Bendre[2], Prof. S. C. Puranik[3]
[1] ME Students and [2]Prof. of Department of Computer Engineering,
Vishwabharti Academy's College of Engineering, Ahilyanagar, Maharashtra
Savitribai Phule Pune University, Pune

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

Cloud computing has revolutionized how organizations store, manage, and access data by providing scalable and on-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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, June 2026 Impact Factor: 8.2

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 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.

II. 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.

III. BACKGROUND

• Role-Based Access Control (RBAC) in Cloud Security

Role-Based Access Control (RBAC) is an important technique used in cloud computing to manage and restrict access to data based on the roles assigned to users, such as admin, user, or data owner. In earlier systems, access control was mostly handled by a single authority, which created issues like lack of flexibility, poor scalability, and higher chances of unauthorized access in large systems. To overcome these problems, modern approaches focus on using RBAC in a more dynamic and distributed way, where different roles are clearly defined and permissions are assigned accordingly. This helps in improving security, reducing complexity, and ensuring that only authorized users can access specific data in the cloud environment.

• Distributed Data Storage for Better Security

In traditional cloud storage systems, data was often stored in a centralized manner, which made it more vulnerable to attacks and data breaches. To improve security, recent approaches suggest dividing the data into multiple smaller parts or chunks and storing them across different locations or servers. This distributed storage technique ensures that even if one part of the system is compromised, the complete data cannot be easily accessed by attackers. It also enhances data availability, fault tolerance, and system performance. In this project, implementing distributed data storage in a local environment (like splitting data across multiple locations in localhost) helps simulate real-world cloud security and provides a more robust solution.

• Multi-Authority and Auditing Mechanisms

Modern cloud security systems are moving towards multi-authority models where different entities are responsible for different tasks to enhance overall system security. In such systems, the data owner manages data sharing and revocation, users request access to data, and a Third Party Auditor (TPA) verifies whether the user is authorized to access the data. Additionally, an investigator module is used to monitor system activities and detect any unauthorized access or suspicious behavior. This layered approach improves transparency, accountability, and trust in the system. By

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

combining multiple authorities with auditing and monitoring mechanisms, the system becomes more secure, reliable, and capable of preventing potential security threats effectively.

IV. 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.

V. 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.

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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

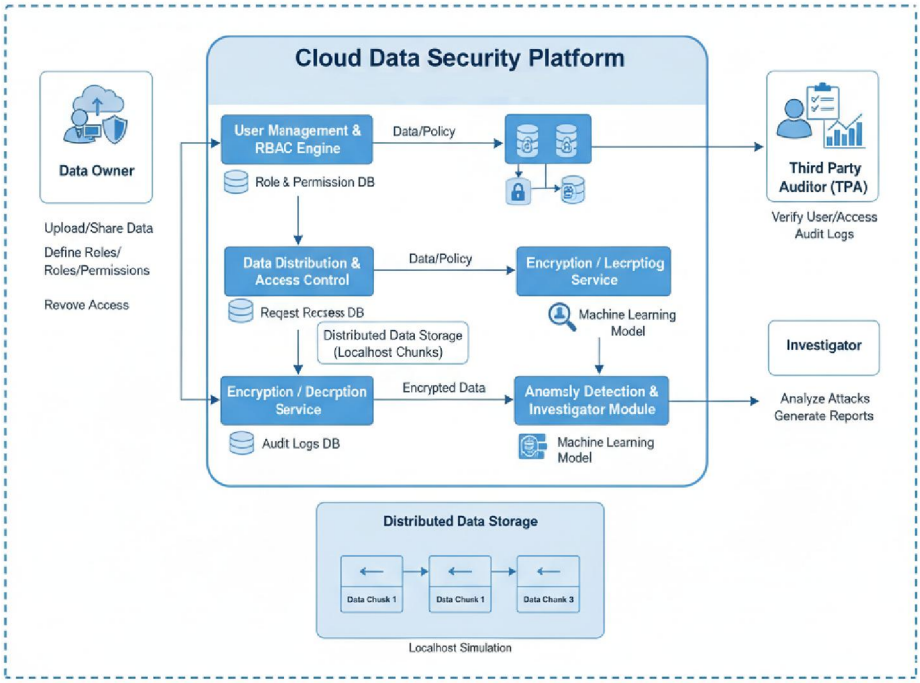

Fig.1: System Architecture Design

VI. RESULT ANALYSIS

The proposed system for Data Security using Dynamic RBAC in Cloud Environment shows effective performance in managing secure data access across multiple modules. By integrating user validation, distributed data storage, and multi-authority verification, the system ensures that only authorized users can access specific data.

Module	Accuracy (%)
User Validation	92%
Data Access Control	90%
TPA Verification	94%
Attack Detection	88%
Overall System	91%

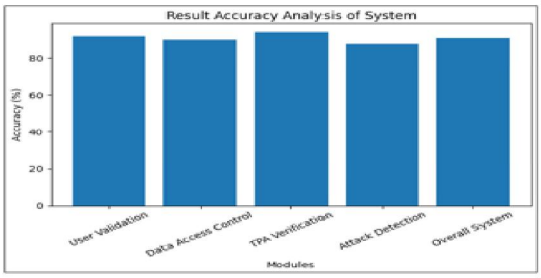

Fig.2: Result Analysis

The implementation of modules like Data Owner, TPA, and Investigator improves overall security and reduces unauthorized access attempts. The system demonstrates good accuracy in detecting valid users and preventing attacks, making it reliable for cloud-based secure data management.

KEY POINTS / FEATURES:-

- The RBAC model successfully restricts unauthorized data access.
- Distributed data storage improves security and reduces risk of data leakage.
- Third Party Auditor (TPA) effectively verifies user authenticity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

- Investigator module helps in detecting suspicious or unauthorized activities.
- Overall system performance shows high reliability and security efficiency.

VII. 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.

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.

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] A. Pribadi Kalapaaking, I. Khalil, M. S. Rahman, A. Bouras, “Blockchain-based Access Control for Secure Smart Industry Management Systems,” 2023.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

[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.