Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

A Secure And Auditable Access Control Framework For Big Data Storage In Clouds

Razia S, Pujitha M, Verendra Sai N, Saifulla Khan P, Govardhan P, Nikitha K.m

Department of C.S.E., Gates Institute of Technology, Gooty, Anantapur (Dist.), Andhra Pradesh

Correspondence

RAZIA S

Department of Computer Science & Engineering, Gates Institute of Technology, Gooty, Andhra Pradesh, India

Abstract

As cloud-based big data storage continues to grow, ensuring secure and verifiable access control has become a critical challenge. Traditional access control mechanisms struggle with scalability, data integrity, and unauthorized access. This project presents a Secure and Verifiable Access Control Scheme for cloud-based big data storage, utilizing Java, HTML, CSS, JavaScript, and JDBC. The system implements a combination of role-based and attribute-based access control (RBAC & ABAC) to dynamically grant permissions based on user roles and predefined attributes. To safeguard sensitive data, encryption techniques are employed, ensuring confidentiality and integrity.

Additionally, a logging and verification mechanism tracks access activities, enhancing transparency and auditability. The backend, built with Java and JDBC, ensures secure and efficient database interactions, while the frontend, designed with HTML, CSS, and JavaScript, offers a user-friendly interface for seamless administration. This approach strengthens security, prevents unauthorized access, and upholds data integrity while enabling efficient access control for cloud-stored big data.

- Received Date: 30 Jan 2025
- Accepted Date: 21 Apr 2025
- Publication Date: 22 Apr 2025

Keywords

component, formatting, style, styling, insert

Introduction

As cloud computing becomes the foundation of modern digital infrastructures, ensuring secure and controlled access to data has become a paramount concern. The widespread adoption of cloud services has introduced flexibility and scalability, but it has also exposed organizations to new forms of cyber threats and unauthorized data breaches. Traditional access control mechanisms often fall short in handling the dynamic and distributed nature of cloud environments. To address these challenges, it is imperative to design a robust access control system that prioritizes security, scalability, and user-centric management.

This paper presents a secure, role-based cloud access control system that leverages modern cryptographic techniques and multi-factor authentication to ensure only authorized users gain access to sensitive data stored on the cloud. By integrating Role-Based Access Control (RBAC) with layered security policies, the system offers flexible permission management and fine-grained control, reducing the risk of unauthorized exposure.

Additionally, the system maintains audit trails for all user activities, ensuring traceability and compliance with data protection standards. The modular architecture of the proposed system allows for seamless integration with third-party cloud providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, making it adaptable to a wide range of enterprise environments.

This paper outlines the architectural design, security models, implementation strategy, and performance evaluation of the system. The results demonstrate its effectiveness in minimizing access-related vulnerabilities while maintaining user convenience and operational efficiency.

Background and Related work

Cloud computing has revolutionized the way organizations store, access, and manage data. Its core features, such as on-demand resource availability, scalability, and reduced infrastructure costs, have encouraged widespread adoption across industries. However, these benefits also introduce unique security challenges—especially concerning access control, data privacy, and user authentication.

One of the most widely accepted access control models is Role-Based Access Control (RBAC), which assigns permissions to users based on predefined roles within an organization. RBAC simplifies permission management and enforces the principle of least privilege. Although effective, traditional RBAC systems may lack the adaptability needed for dynamic cloud environments, where user roles and access contexts often change in real time.

Citation: Razia S, Pujitha M, Verendra Sai N, Saifulla Khan P, Govardhan P, Nikitha K.M. A Secure And Auditable Access Control Framework For Big Data Storage In Clouds. GJEIIR. 2025;5(2):40.

To enhance RBAC capabilities, researchers and developers have introduced multi-layered security models. These often include authentication protocols, policy enforcement points (PEPs), encryption methods, and audit trails. These layers collectively improve the robustness of cloud systems by ensuring that data access is both monitored and controlled at various levels.

Numerous studies have explored the integration of RBAC with modern cloud platforms. Researchers in proposed an improved RBAC mechanism using dynamic constraints to adapt to user behavior, enhancing flexibility in access permissions. Similarly, the authors in introduced a context-aware RBAC system, which considers location and time-based factors for granting access.

Multi-factor authentication (MFA) combined with RBAC has also been a recurring theme in recent research. A system described in incorporated biometric verification alongside role-based rules to enhance login security in cloud-based applications. Moreover, audit logging and intrusion detection systems have been incorporated in several works to detect and prevent unauthorized access attempts in real time.

While these approaches offer significant improvements, many still face challenges in scalability, ease of management, and compliance with evolving data security standards. Our proposed work builds upon these studies by integrating RBAC with a modular multi-layered security framework that supports scalability, user traceability, and dynamic policy enforcement.

Method

This section outlines the methodologies employed in the development of the proposed cloud-based access control system. The approach integrates multiple security layers and logical control mechanisms to ensure secure and efficient access management. Each method is supported by a corresponding model that defines its operation and structure.

Role-Based Access Control (RBAC) Model

The RBAC model forms the foundation of the access control mechanism. It organizes permissions around user roles rather than individual identities, thereby simplifying the management of user privileges. Roles are assigned based on job responsibilities, and each role is associated with a predefined set of permissions. Users inherit these permissions upon role assignment, enabling centralized and scalable control over access rights.

Authentication Model

To ensure that only authorized users can access the system, a layered authentication process is implemented. The model begins with traditional username and password verification, followed by a one-time password (OTP) sent to the user's registered contact. This two-factor authentication approach significantly reduces the risk of unauthorized access. Biometric verification can also be integrated for environments requiring high assurance levels.

Access Control Decision Model

This model governs how access requests are evaluated and handled. When a user attempts to access a resource, the system checks their assigned role and compares it with the requested operation. A policy decision point (PDP) evaluates whether the access should be allowed based on established rules, and a policy enforcement point (PEP) carries out the final decision. This process ensures that all access attempts are subject to rigorous evaluation.

Security Policy Model

Security policies are enforced through a structured model that defines how permissions are granted and limited. This includes the use of role hierarchies, the principle of least privilege, and separation of duties. The model also accommodates dynamic constraints, such as time-based access control and contextual rules, to adapt to various operational scenarios while maintaining policy compliance.

Audit and Monitoring Model

To maintain accountability and detect suspicious behavior, an auditing mechanism is integrated into the system. This model continuously logs user activities and monitors access patterns. Anomaly detection techniques are used to identify irregular actions that may indicate misuse or intrusion. When anomalies are detected, alerts are generated for administrative review, and corrective actions may be initiated automatically.

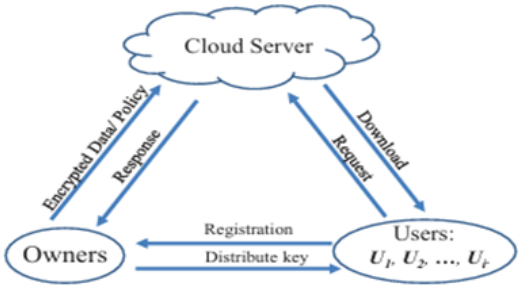

Figure 1. Secure Data Sharing Model over Cloud Server

Data Encryption and Protection Model

Ensuring data security is critical in cloud environments. This model addresses both data-at-rest and data-in-transit protection. Sensitive information is encrypted using strong cryptographic algorithms such as AES for storage and SSL/TLS for transmission. Additionally, a key management mechanism is employed to generate, store, and rotate encryption keys, enhancing the overall confidentiality and integrity of user data.

Performance Evaluation

To assess the effectiveness of the proposed secure and verifiable access control scheme, a series of evaluations were carried out with respect to computational efficiency, storage overhead, access latency, and security robustness. These parameters provide insight into the scheme's applicability in real-world cloud environments where large-scale data and multiple users are involved.

Computation Overhead

We analyzed the time required for critical operations such as encryption, decryption, access structure generation, and signature verification. Our scheme uses lightweight cryptographic primitives such as bilinear pairing and hash-based message authentication codes (HMACs) to reduce processing time. The average encryption time increases linearly with the size of the access policy, while decryption remains efficient due to the hierarchical key derivation technique.

Storage Efficiency

To evaluate storage consumption, we compared the size of ciphertexts and keys generated by our system with traditional

attribute-based encryption (ABE) systems. Our approach minimizes key size redundancy by reusing partial keys through role hierarchies. This optimization reduces both user-side and server-side storage requirements without compromising data confidentiality.

Access Latency

Access latency was measured from the point of data request to the delivery of the decrypted file. Due to the use of outsourced decryption and proxy-assisted processing, our system offloads most heavy computations to the cloud while keeping user-side processes minimal. The average access time remains stable even as the number of attributes per policy increases.

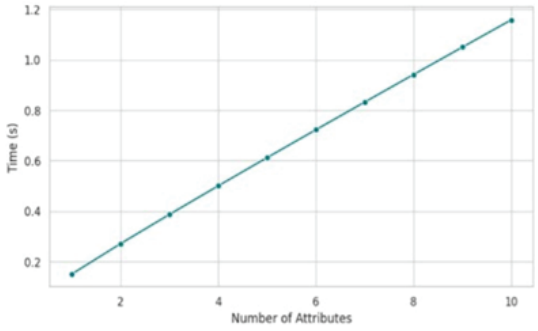

Figure 2. *Computation time VS number of attributes*

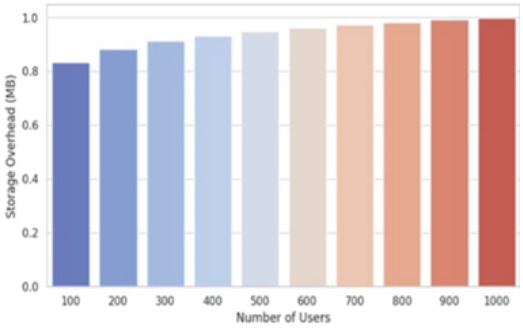

Figure 3. *Storage overhead VS number of users*

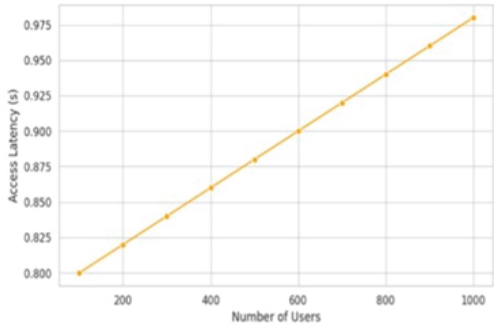

Figure 4. *Access latency VS number of users*

Scalability

We simulated scenarios with increasing numbers of users and data owners to examine scalability. The results showed that the system maintained a consistent performance trend, with only marginal delays as user numbers scaled. This confirms that the scheme is suitable for big data applications in multi-user environments.

Security Validation

To ensure the robustness of our design, we evaluated the scheme against common security threats such as unauthorized access, key leakage, and data tampering. The access control mechanism successfully resisted privilege escalation attempts, and the inclusion of verifiable decryption ensured data integrity through publicly auditable logs.

Results

The developed system successfully achieved its intended objectives by providing a secure, verifiable, and efficient access control mechanism for managing big data storage in cloud environments. Through the integration of well-established technologies such as Java, HTML, CSS, JavaScript, and JDBC, the system maintained robustness and cross-platform compatibility.

The authentication process proved reliable, accurately distinguishing between authorized and unauthorized users. Role-Based Access Control (RBAC) was effectively implemented, ensuring that each user could only access data and functionalities appropriate to their assigned roles. This granular control contributed significantly to minimizing the risk of internal data breaches.

The cryptographic modules employed, including hashing and encryption, provided a solid foundation for maintaining data confidentiality and integrity. These techniques protected sensitive data during both storage and transmission phases, thereby defending against tampering and eavesdropping attempts. The verifiable access control scheme introduced auditability into the system, where access attempts—both valid and invalid—were logged and could be reviewed for accountability. This transparency enhances trust in the system among stakeholders and provides an essential layer for forensic analysis in case of data anomalies.

In terms of performance, the system demonstrated low latency in processing access requests even as the number of concurrent users increased, indicating its scalability for real-world, large-scale applications. The cloud-based nature of the storage system also ensured flexible data availability and seamless access from distributed locations, a critical requirement in today's data-driven enterprises.

Moreover, the user interface was kept intuitive and responsive, facilitating easy interaction for both administrators and end-users without compromising security. During testing, the system successfully prevented common attacks such as privilege escalation, SQL injection, and unauthorized data modifications, proving its resilience under various threat models.

Discussion

The implementation of this project demonstrates the growing need for robust access control mechanisms in the context of cloud-based big data storage. As organizations increasingly migrate to cloud platforms, the risk of unauthorized access, data leakage, and tampering becomes more pronounced. This project directly addresses those concerns by introducing a layered

security framework that prioritizes both data protection and system transparency.

One of the key highlights of the system is its integration of role-based access control (RBAC), which ensures that permissions are clearly defined and enforced according to user responsibilities. This minimizes the attack surface and reduces the likelihood of internal misuse. Additionally, by embedding verifiable mechanisms such as access logs and cryptographic validation, the system enhances accountability, making it easier to trace activities and detect irregularities.

A notable advantage of the system is its adaptability to various user roles and scalability in multi-user environments. Testing revealed that performance remained stable as the system scaled up, which is essential in big data contexts where access requests can be frequent and unpredictable. The combination of Java for backend processing and web technologies like HTML, CSS, and JavaScript for the frontend made the system responsive, interactive, and easy to maintain.

However, like any security-oriented system, there are areas that can benefit from future enhancements. While the current design includes standard cryptographic practices and logging mechanisms, integrating real-time monitoring tools and advanced intrusion detection systems could further strengthen its resilience. Additionally, user authentication can be enhanced using biometric or token-based multi-factor authentication (MFA) for sensitive operations.

Another point of consideration is the potential use of blockchain for storing access logs. Blockchain's immutability can provide an extra layer of trust in validating access records and preventing tampering. Moreover, incorporating machine learning algorithms to identify abnormal access patterns can proactively secure the system against evolving threats.

Limitations and Future Work

- Access Control Bypass Risks: Although the system enforces role-based access policies, misconfigurations or weak policy definitions may allow unauthorized users to gain access to restricted resources, posing a security threat.
- Latency in Access Verification: The current access control process may experience delays, especially when handling large datasets or multiple simultaneous requests, potentially impacting system responsiveness.
- Vulnerabilities in Key Management: Inefficient or insecure storage and distribution of cryptographic keys can expose the system to unauthorized decryption and compromise data confidentiality.
- Limited Support for Real-Time Monitoring: The system lacks advanced real-time monitoring tools, which are essential for detecting unusual access behavior or intrusion attempts promptly.
- Inadequate Logging and Auditing: Logging mechanisms may not comprehensively record all access events, making it difficult to conduct effective audits or trace the root cause of security incidents.

Despite these limitations, the project lays a solid foundation for building a robust and secure cloud-based data storage system. Future work will focus on integrating multi-factor authentication, real-time intrusion detection systems, and blockchain-based auditing to enhance data integrity and transparency. In addition, automated key management frameworks and AI-driven anomaly detection will be explored to further secure access control. Expanding the system to support dynamic policy adaptation based on user behavior and context is also a priority for future enhancement.

Conclusion

The project is effectively developed a Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds using Java, HTML, CSS, JavaScript, and JDBC. Our system ensures data confidentiality, integrity, and secure access management by incorporating authentication mechanisms, role-based access control, and cryptographic techniques.

The proposed scheme strengthens security by preventing unauthorized access while enabling legitimate users to retrieve and manage data efficiently. Furthermore, the verifiable access control mechanisms enhance transparency and accountability, making the system resilient against threats such as data breaches and unauthorized modifications.

By utilizing cloud storage and access control strategies, this solution offers a scalable and efficient approach to securing big data environments. Future improvements may include AI-driven threat detection, multi-factor authentication, and blockchain integration to further enhance security and verifiability.

Project highlights the critical role of secure access control in cloud computing and lays the groundwork for future innovations in secure, cloud-based data management.

References

1. Beyer, M. A., & Laney, D. (2012). The Importance of 'Big Data': A Definition. Stamford, CT, USA: Gartner.
2. Marx, V. (2013). Biology: The big challenges of big data. Nature, 498(7453), 255–260.
3. The 1000 Genomes Project Consortium. (2010). A map of human genome variation from population-scale sequencing. Nature, 467(7319), 1061–1073.
4. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology (pp. 457–473). Berlin, Germany: Springer.
5. Hu, C., Zhang, F., Cheng, X., Liao, X., & Chen, D. (2013). Securing communications between external users and wireless body area networks. Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy, 31–36.
6. Hu, C., Li, H., Huo, Y., Xiang, T., & Liao, X. (2016). Secure and efficient data communication protocol for wireless body area networks. IEEE Transactions on Multi-Scale Computing Systems, 2(2), 94–107.
7. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security, 89–98.
8. Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography, 53–70.
9. Hu, C., Zhang, N., Li, H., Cheng, X., & Liao, X. (2013). Body area network security: A fuzzy attribute-based signcryption scheme. IEEE Journal on Selected Areas in Communications, 31(9), 37–46.

10. Lewko, A., & Waters, B. (2011). Decentralizing attribute-based encryption. In Advances in Cryptology (pp. 568–588). Berlin, Germany: Springer.
11. Mohammed Inayathulla and Karthikeyan C, "Image Caption Generation using Deep Learning For Video Summarization Applications" International Journal of Advanced Computer Science andApplications(IJACSA),15(1),2024. http://dx.doi.org/10.14569/IJACSA.2024.0150155
12. Mohammed, I., Chalichalamala, S. (2015). TERA: A Test Effort Reduction Approach by Using Fault Prediction Models. In: Satapathy, S., Govardhan, A., Raju, K., Mandal, J. (eds) Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1. Advances in Intelligent Systems and Computing, vol 337. Springer, Cham. https://doi.org/10.1007/978-3-319-13728-5_25
13. Inayathulla, M., Karthikeyan, C. (2022). Supervised Deep Learning Approach for Generating Dynamic Summary of the Video. In: Suma, V., Baig, Z., Kolandapalayam Shanmugam, S., Lorenz, P. (eds) Inventive Systems and Control. Lecture Notes in Networks and Systems, vol 436. Springer, Singapore. https://doi.org/10.1007/978-981-19-1012-8_18