www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 438-443

e-ISSN : 2583-1062
Impact Factor : 7.001

ADVANCING CLOUD SECURITY: DATA SECURITY OF DYNAMIC AND ROBUST ROLE BASED ACCESS CONTROL FROM MULTIPLE AUTHORITIES IN CLOUD

Prof. Snehal Thorave[1], Rohit Jadhav[2], Krishna Patil[3], Rudraksha Chaure[4], Shubhanshu Uttekar[5]

[1]Professor, DPCOE, Savitribai Phule Pune University, Pune, Maharashtra, India.

[2,3,4,5]BE Scholar,Dhole Patil College of Engineering, Pune, India.

DOI: https://www.doi.org/10.58257/IJPREMS36614

ABSTRACT

Improving cloud security for data protection necessitate the dynamic and consistent deployment of Role-Based Access Control (RBAC) by numerous authorities. This technique intends to improve the security of sensitive data stored in the cloud by utilizing role-based dynamic access privilege modification. The system integrates RBAC procedures from many authorities to offer broad protection coverage and adaptability to changing organizational structures. This technique improves data security and makes it easier to manage access credentials across various cloud settings. Implementing dynamic and resilient RBAC in cloud security is a critical step toward strengthening data protection and access control methods in the cloud computing environment, despite problems such as guaranteeing consistency and interoperability across several authorities.

Keywords- Key generation, AES-128 Encryption and RBAC, Data security, Cloud Security, java, Multi-Authority Systems, Dynamic Access Control, Robust Access Control, Privacy Preservation in Cloud, Access Control Models, Secure Data Sharing, Policy Enforcement in Cloud.

1. INTRODUCTION

Cloud security allows you to consolidate protection of cloud-based networks for streamlined, continuous monitoring and analysis of numerous devices, endpoints, and systems. It also enables you to centrally manage software updates and policies from one place and even implement and action disaster recovery plans. Cloud data security protects data that is stored (at rest) or moving in and out of the cloud (in motion) from security threats, unauthorized access, theft, and corruption. The high-level objectives of cloud security are to: Ensure cloud data, users, and underlying systems are sufficiently secured against threats such as bot-driven distributed denial-of-service (DDoS) attacks, API exploitation, and data corruption vulnerabilities. Encryption is one of the best ways to secure your cloud computing systems. There are several different ways of using encryption, and they may be offered by a cloud provider or by a separate cloud security solutions provider: Communications encryption with the cloud in their entirety. it's worth mentioning that each cloud platform offers a marketplace where customers can make use of third-party vendor applications to meet specific security requirements. AWS and Azure are leading the way on this, with GCP trying to catch up.

1. Enhanced Security for Multi-Tenancy and Cloud Environments: -

Cloud infrastructures are shared by various tenants and organizations, necessitating powerful and adaptable access controls. RBAC enables the development of roles based on users' responsibilities, ensuring that only authorized individuals have access to specified resources. Dynamic and robust RBAC solves the need for real-time flexibility as roles change (for example, when employees switch departments) while ensuring data protection across several tenants.

2. Multiple Authorities and Decentralization: -

Cloud services sometimes require numerous authorities or parties controlling various resources (for example, third-party services, dispersed cloud providers). A dynamic RBAC system ensures that security enforcement is uniform across all of these entities, even when they function independently. Using various authorities improves security by decentralizing access control choices, lowering the danger of a single point of failure or breach.

2. PROBLEM STATEMENT

In the modern cloud environment, data security remains a critical challenge due to the increasing reliance on both trusted and untrusted cloud service providers. Current approaches to cloud security, while effective to some extent, fall short in providing comprehensive protection against sophisticated threats such as collusion attacks, especially in scenarios where multiple entities interact with the data, including the data owner, users, third-party auditors (TPA), and authorities. The need for secure, long-term communication between these parties without compromising data integrity is paramount.

The proposed research aims to design and implement a Dynamic and Robust Role-Based Access Control (RBAC) system that can mitigate the risks posed by collusion attacks in both trusted and untrusted cloud environments. By

involving multiple authorities to manage access control and enforcing dynamic role adjustments based on real-time changes in user tasks or security needs, the system will offer enhanced data security.

Leveraging advanced security techniques, such as AES encryption, multi-factor authentication, and multi-authority key management, this system will provide superior protection compared to existing models. Additionally, the system will ensure secure communication between all stakeholders (data owners, users, TPA, and authorities) over extended periods. The solution seeks to address the growing complexity of cloud environments while ensuring data remains protected, even in the face of sophisticated internal and external attacks. Ultimately, the goal is to create a robust, scalable, and highly secure cloud security framework that outperforms current approaches in safeguarding sensitive information across dynamic, multi-authority cloud platforms.

3. SCOPE AND OBJECTIVE

1. PROJECT SCOPE

Enhancing security measures to ensure the confidentiality and integrity of data stored in the cloud.

Implementing RBAC mechanisms that can adapt to changing organizational structures and diverse cloud environments for efficient access control management.

The scope of this project is to design, implement, and evaluate a comprehensive cloud security framework that addresses data security challenges in trusted and untrusted cloud environments. The focus will be on developing a Dynamic and Robust Role-Based Access Control (RBAC) system, supported by multiple authorities, to secure sensitive data from both internal and external threats, including collusion attacks.

Key areas covered within the project scope include:

1. Design of a Multi-Authority RBAC System: A role-based access control system that dynamically adjusts user roles and permissions based on real-time changes in tasks, responsibilities, or security requirements.

Multiple authorities will manage their own access controls while ensuring consistent enforcement of security policies across the cloud.

2. Enhanced Data Security: Implementation of advanced encryption techniques, such as AES encryption, to secure data both at rest and in transit.Use of multi-factor authentication (MFA) and secure communication protocols to prevent unauthorized access.

3. Protection Against Collusion Attacks: The system will provide robust mechanisms to mitigate collusion attacks, where multiple malicious entities might conspire to gain unauthorized access to cloud data.

4. Trusted and Untrusted Cloud Environments: The solution will work in both trusted cloud environments (where security assumptions are higher) and untrusted environments (where service providers might not be fully trusted), providing flexibility and security across various cloud platforms.

5. Real-Time Role Management: The system will enable real-time updates to user roles and permissions, ensuring that changes are reflected immediately without causing downtime or disrupting access.

6. Communication Security: Focus on securing long-term communication between key stakeholders such as data owners, users, third-party auditors (TPA), and authorities to ensure data integrity and confidentiality.

7. Performance and Scalability: The system will be designed to handle large-scale cloud environments while maintaining high performance and scalability.

Optimization of communication, storage, and computation to ensure efficient use of cloud resources.

8. Compliance with Security Standards: The framework will adhere to industry standards and best practices in cloud security, ensuring that it can be adopted in real-time projects with strict data protection requirements.

4. OBJECTIVES

In today's interconnected digital world, cloud computing has become a foundational technology for organizations, allowing flexible access to resources and data across distributed platforms. However, as cloud adoption increases, so does the need for robust security measures to protect sensitive data from ever-evolving internal and external threats. One crucial aspect of cloud security is ensuring that data access is controlled dynamically and securely, particularly when multiple authorities are involved in granting permissions. The integration of advanced cryptographic techniques and innovative security protocols plays a vital role in this process.

Robust Security Against Attacks

Cloud environments are vulnerable to both internal and external threats, which include malicious attacks from outside actors, as well as insider threats such as data breaches caused by collusion between compromised entities. Ensuring robust security against these attacks requires the implementation of resilient defence mechanisms. The dynamic and

robust Role-Based Access Control (RBAC) system provides an effective solution by regulating user access to cloud data based on predefined roles and responsibilities. Unlike traditional systems, dynamic RBAC systems can adapt in real-time to changes in user roles, ensuring that access permissions remain appropriate as users' roles evolve. Additionally, these systems are designed to resist complex threats such as collusion attacks, where two or more malicious users may conspire to gain unauthorized access to data. To counter these threats, this system integrates advanced security protocols that enable multi-level authentication and verification procedures. For example, SQL injection attacks, which exploit vulnerabilities in a database by injecting malicious code, are mitigated by robust query validation processes and constant monitoring for suspicious activity.

AES Encryption Integration

Data security is a critical concern in cloud environments, particularly when sensitive information is being shared across multiple authorities or stored in decentralized systems. One of the most reliable ways to protect data in transit and at rest is through AES (Advanced Encryption Standard) encryption, which has become a widely accepted standard for securing data due to its strength and efficiency.I n this system, AES encryption is seamlessly integrated into the cloud architecture, ensuring that all data stored or transmitted within the system is encrypted using strong cryptographic methods. AES provides a high level of security by using key lengths of 128, 192, or 256 bits, making it resistant to brute-force attacks. By encrypting data before it is shared with any authorized user, this approach prevents unauthorized access even in the event of a breach, ensuring that only users with the proper decryption keys can access the data. Furthermore, the integration of AES within the system's access control mechanisms guarantees that encrypted data can only be accessed by users with appropriate roles and permissions, enhancing both data confidentiality and integrity.

Improved Efficiency and Authentication

Security measures in cloud environments must not only protect against attacks but also ensure that the system remains efficient and user-friendly. Slow response times or cumbersome authentication processes can hinder system usability, reducing productivity and increasing the likelihood of user error. To address these challenges, the proposed access control system incorporates innovative methods to enhance both time efficiency and the effectiveness of authentication protocols. The system introduces new verification and authentication protocols that streamline the process of granting access while maintaining high security standards. Multi-factor authentication (MFA), including biometrics, one-time passwords (OTPs), or cryptographic keys, can be employed to ensure that access is granted only to verified users. These measures reduce the likelihood of unauthorized access by requiring multiple forms of authentication, even if one factor is compromised. At the same time, the system enhances time efficiency by leveraging optimized algorithms for role assignment and permission verification. Users can be authenticated quickly, without experiencing long delays during login or access requests. By improving the efficiency of both authentication and access control processes, the system ensures that users have timely access to the resources they need while maintaining a strong security posture.

5. LITERATURE SURVEY

Sr. No	Paper Title	Author Name	Year	Description
1.	Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions	ISHU GUPTA	2022	A large number of researchers, academia, government sectors, and business enterprises are adopting the cloud environment due to the least upfront capital investment, maximum scalability, and several other features of it. Despite the multiple features supported by the cloud environment, it also suffers several challenges. Data protection is the primary concern in the area of information security and cloud computing.
2.	Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud	S. Tamilselvan A. Pasumpon Pandian	2024	To this end, the overhead in running the cryptographic operation at the end-user device is small. In addition, we develop secure access policy sharing and re-encryption protocol to enable users having write privilege to update the data and request the proxy to perform data reencryption. Finally, we present the evaluation and experiments to

	Computing Environments			demonstrate the efficiency and practicality of our system.
3.	Achieving Secure Rolebased Access Control on Encrypted Data in Cloud Storage	Lan Zhou	2024	With the rapid developments occurring in cloud computing and services, there has been a growing trend to use the cloud for large-scale data storage. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud

6. METHODOLOGY

There are multiple main strategies for dealing with data security concerns in Dynamic and Robust Role-Based Access Control (RBAC) from different authorities in cloud environments. First, a requirement analysis is performed to discover the cloud environment's specific data security requirements, such as the types of data stored, user roles, and the interaction of several authorities governing access control. The following stage is to design a role-based policy architecture that defines access control policies for specific roles, ensuring that permissions are assigned to roles rather than individuals. This provides flexibility as user responsibilities change dynamically.

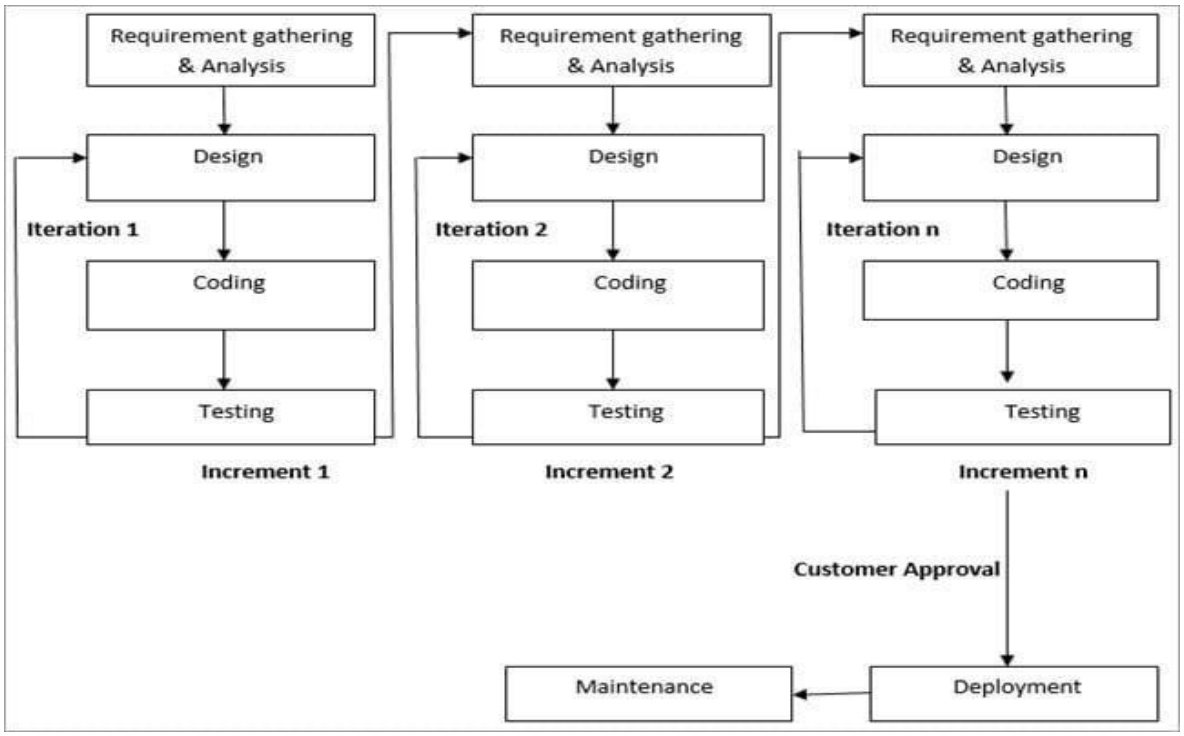
Methodologies Of Problem Solving: -

There are multiple main strategies for dealing with data security concerns in Dynamic and Robust Role-Based Access Control (RBAC) from different authorities in cloud environments. First, a requirement analysis is performed to discover the cloud environment's specific data security requirements, such as the types of data stored, user roles, and the interaction of several authorities governing access control. The following stage is to design a role-based policy architecture that defines access control policies for specific roles, ensuring that permissions are assigned to roles rather than individuals. This provides flexibility as user responsibilities change dynamically.

1. SDLC model to be applied

Agile Model

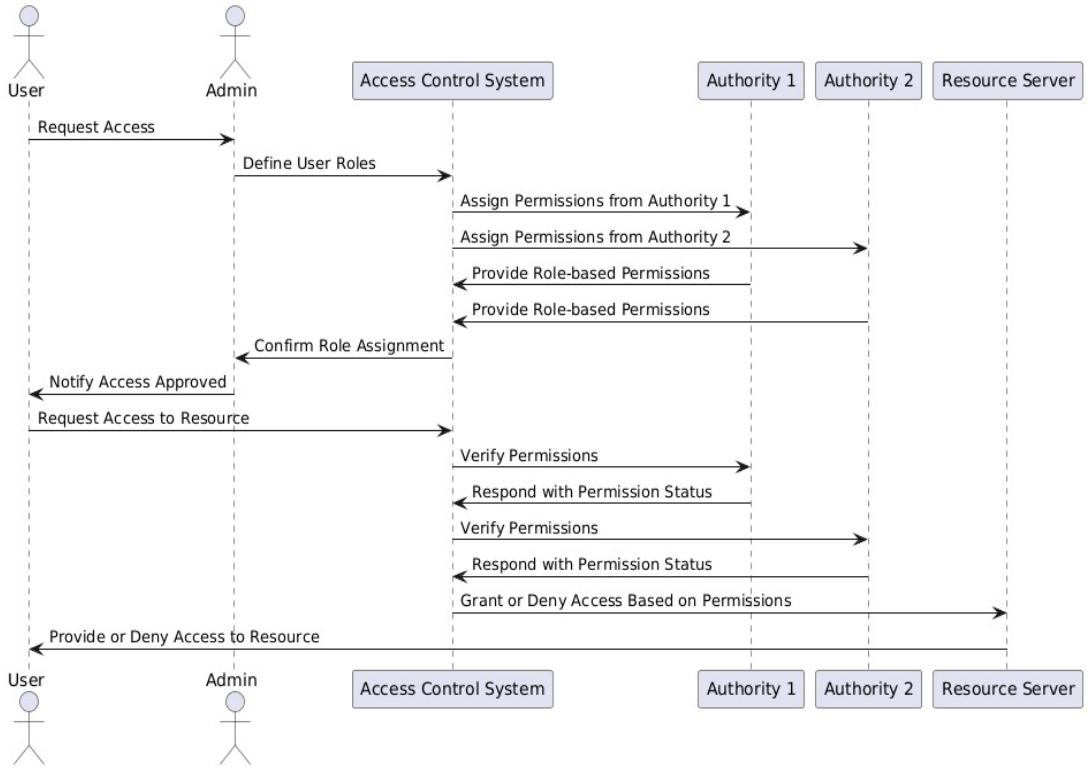
Agile Model is a combination of the Iterative and incremental model. This model focuses more on flexibility while developing a product rather than on the requirement. In Agile, a product is broken into small incremental builds. It is not developed as a complete product in one go. Each build increments in terms of features. The next build is built on previous functionality. In agile iterations are termed as sprints. Each sprint lasts for 2-4 weeks. At the end of each sprint, the product owner verifies the product and after his approval, it is delivered to the customer. Customer feedback is taken for improvement and his suggestions and enhancement are worked on in the next sprint. Testing is done in each sprint to minimize the risk of any failures. In this project we have used agile model. It helps us to done work in efficient way.



www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 438-443
e-ISSN : 2583-1062
Impact Factor : 7.001

2. Sequence Diagram

Sequence diagrams can be used to provide a graphical representation of object interactions or object coordination over the time. These basically displays a actor or user, and the objects and components they interact with in the execution of a use case. The sequence diagrams displays the own of messages from one object to another object, and as such correspond to the methods and event supported by a class/object



REQUIREMENTS

1. Basic Requirements

- Dynamic Role Assignment: This system must dynamically adjust users' roles and permissions based on changes in tasks, departments, or security requirements. This must happen in real-time without causing system downtime.
- Multi-Authority Management: The system should support multiple authorities, each capable of managing their own access controls while ensuring consistent enforcement across the cloud. This increases security and flexibility by preventing any single authority from having complete control.

2. Functional Requirements

- Role Management: Administrators must be able to assign, modify, and revoke user roles dynamically in real time, ensuring appropriate access levels for current tasks.
- Permissions Configuration: The system must allow for detailed, customizable permissions (e.g., read, write, edit, delete) based on the organization's needs.

3. External Interface Requirements

- User Interface (UI): The UI should be accessible via standard browsers (e.g., IE, Mozilla, Chrome) for user interaction.
- Hardware Interface: Eclipse IDE and minimal libraries are required for the software to run.
- Software Interface: Java is the primary programming tool, with Eclipse IDE as the development platform.

4. Non-Functional Requirements

- Performance: The system should operate optimally with at least 4 GB of RAM. Errors are generated with the preferred feedback.
- Safety: The system is modular, allowing errors to be detected and addressed easily.
- Security: Modular design ensures errors are identified and fixed efficiently.
- **Software Quality Attributes:**

  - Usability: Users should be able to navigate the system easily without extensive training.

- Reliability: The system should be available at all times.
- Performance: The system should start in less than 15 minutes and provide output within 10 -15 min.
- Security: The system allows users to save and reuse previous code.

5. System Requirements

- **Database:** A database is not required; input is provided through images.
- **Software Requirements:**
  - OS: Windows 10
  - Programming Language: Java
  - IDE: Eclipse Oxygen
  - Backend: MySQL 5.5
  - Web Server: Apache Tomcat/XAMPP
- **Hardware Requirements:**
  - Processor: Intel Core i3 or higher
  - RAM: 4 GB or higher
  - Hard Disk: 100 GB minimum

7. CONCLUSION

The advancement of cloud security, particularly through Dynamic and Robust Role-Based Access Control (RBAC) with Multiple Authorities, is crucial for safeguarding sensitive data in cloud environments. This approach offers a flexible and efficient way to manage user access while addressing the growing complexity of distributed cloud systems. By allowing multiple authorities to administer their own access controls and dynamically adjusting user roles in real time, organizations can ensure that data remains protected even as roles, tasks, and security requirements evolve.

The integration of real-time updates, robust encryption techniques, and decentralized management creates a stronger security framework capable of resisting internal and external threats. Furthermore, dynamic RBAC enhances system efficiency by ensuring that users have the appropriate permissions at all times without causing downtime or delays. As real-time projects increasingly rely on cloud-based infrastructures, implementing such secure and adaptable access control systems is vital for maintaining both data integrity and operational agility.

In the future, continued innovation in cloud security will focus on incorporating AI-driven access control, quantum-resistant encryption, and blockchain technology to further improve security, performance, and scalability. This ensures that cloud environments remain secure, flexible, and ready to meet the evolving demands of real-time applications.

8. FUTURE SCOPE

The continuous evolution of cloud technologies presents opportunities for improving security systems that safeguard sensitive data. The future scope for Data Security of Dynamic and Robust Role-Based Access Control (RBAC) from Multiple Authorities in Cloud is broad, with several key areas of innovation and expansion:

9. REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.

[2] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ‘‘A lightweight secure data sharing scheme for mobile cloud computing,’’ IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344– 357, Apr. 2018.

[3] Z. Wan, J. Liu, and R. H. Deng, ‘‘HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,’’ IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[4] T. Nishide, K. Yoneyama, and K. Ohta, ‘‘Attribute-based encryption with partially hidden encryptor-specified access structures,’’ in Applied Cryptography and Network Security (Lecture Notes in Computer Science), vol. 5037. Berlin, Germany: Springer, 2008, pp. 111–129.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ‘‘Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013