International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Optimizing Cloud Storage and Sharing Through Dual Access Control

Ramaprabha M[1], Ketan Mallik[2], Ishaan Asri[3], Suryansh Yadav[4]

[1]Assistant Professor, [2,3,4] Department of Computer Science and Engineering

SRM Institute of Science and Technology, Ramapuram,Chennai.

ramapram@srmist.edu.in, kg9694@srmist.edu.in, Ia1315@srmist.edu.in, sy4685@srmist.edu.in

ABSTRACT

Many institutions alongside various businesses show increasing interest in Cloud-based data storage service since its recent emergence. The necessity to protect open network services requires immediate attention because this system operates through an open network. Security measures must be applied by service providers for their data storage and sharing operations to protect both database confidential information and user privacy. Most providers protect sensitive data through the commonly used security method of encryption. The basic process of data encryption fails to meet the operational requirements of data management systems. Since economic denial-of-sustainability attacks must be prevented it becomes vital to establish robust controls for download requests. Service users completely protected from Economic Denial of Sustainability type of attacks that aim to block their usage of service. We have designed a control mechanism that serves as dual access control in cloud-based storage perspectives.

I. INTRODUCTION

The proposed solution addresses these two issues through dual access control mechanism. To The promising candidate for data security in cloud-based storage service is attribute-based encryption (ABE).

The system provides secure handling of outsourced data by maintaining data confidentiality and precise control capabilities. In CP-ABE operates as a powerful system for data encryption because it enables the specification of access policies on encrypted data. Data receivers receive their access definitions through policies which attach themselves to encrypted data. This paper adopts CP-ABE as the fundamental encryption principle. Using this technique alone cannot produce a graceful control system to manage both data accessibility and download requests.

The access definition methods of data receivers depend on attached policies within encrypted data which both protect unauthorized access and enable authorized users to easily retrieve information. CP-ABE stands as the selected encryption basis because it provides adaptability and robust security mechanisms. Employing CP-ABE as the single encryption principle alone does not lead to a well-rounded control system which manages data accessibility and download requests thus requiring supplementary security and usability features.

Through secure management of the outsourced data stored in the system users have access to both data confidentiality and tight control capabilities. The system provides secure data protection through policy-based access control combined with encryption techniques in multi-user cloud systems.

II. LITERATURE SURVEY

A range of research has investigated methods of implementing dual access controls to improve cloud environment data protection. The research paper in Child Studies in Asia-Pacific Contexts (2022) developed a dual access system with QR codes functioning as dynamic identification tokens to bolster authentication protection alongside easy user experiences.

A hybrid cryptographic method developed by researchers for dual access control of cloud-based data storage and sharing was introduced through an IEEE Conference Publication (2022). The International Journal for Multidisciplinary Research (2024) studied dual access control mechanisms which enhanced cloud-based security while improving resource utilization for better performance.

At CLOSER 2022 the International Conference on Cloud Computing and Services Science investigated RBAC and ABAC mechanisms to establish scalable data administration with secure access management capabilities. Researchers at the IEEE Conference Publication (2024) explored the possibility of using hybrid cryptography with QR codes to enhance cloud resource allocation security Modern research works to enhance security by keeping operational effectiveness at equal priority. The International Journal for Multidisciplinary Research (2024) presented a dual access control method to optimize cloud environment resources and security capabilities. The implementations offer better security together with resource administration but they generate challenges by increasing system complexity and producing performance penalties as well as scalability difficulties.

III. PROPOSED SYSTEM

The principal method to defend classified information against breaches depends on encryption technologies. AES encryption on its own fails to satisfy the essential operational requirements needed for secure data storage systems based in the cloud. The encryption of data enables confidentiality yet lacks an access control system to authorize data downloads or retrievals needed to protect systems from exploitation.

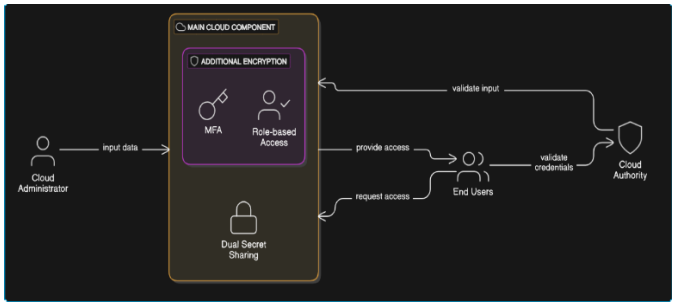
The system requires a specialized method to confirm or decline download requests through security policies in order to stop Economic Denial of Sustainability (EDoS) attacks. Illegal cloud operation exploitation through repetitive costly procedure initiation results in increased service provider financial costs. The system proposes a dual access control system with authentication features for user credentials along with evaluation procedures for download requests to determine authorized access.

The system uses hybrid cryptography and policy-control features to boost security of data access so users can only get permitted data files. The system stopping unauthorized intruders serves to keep cloud services active while safeguarding users who need access to vital cloud resources from sustainability attacks. The system operates more efficiently because it uses its resources effectively and deducts the computational costs from multiple authentication activities.

Dual access control features enable the application to develop a secure scalable framework for cloud storage that safeguards data confidentiality and manages access control and defends against economic exploitation. The security mechanisms increase reliability along with durability of cloud services while maintaining their ability to tackle emerging cyber intrusions.

International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

IV. SYSTEM ARCHITECTURE



The architecture implements a dual access method of control which boosts security controls in cloud storage platforms. The system incorporates four main components namely the "Cloud Administrator" with the "Cloud Authority" and End users along with the main cloud component to provide secure storage, controlled access and protection from unauthorized breaches.

The Cloud Administrator executes tasks to manage the Cloud storage inserting data into the cloud simultaneously executing additional encryption measures that protect the data before the final implementation. The access policies are established by the admin so that the data accessibility depends on the user authentication levels and assigned roles. The Main Cloud Component functions as the fundamental storage and processing area while implementing Multi-Factor Authentication (MFA) alongside Role Based Access Control (RBAC) as core security features. The MFA method requires users to very themselves through multiple methods while RBAC security policies determine which system access each user role should have. The Dual Secret Sharing method guarantees safe access to sensitive data because users must fulfil several accurate authentication steps before making any attempts at modifying the data.

The Cloud Access gets granted once the end users pass authentication tests with their credentials after verification is successful. The system implements strong user authentication requirements that grant users selective retrieval capabilities to specific files, this ensures reduced vulnerability from Economic Denial of Sustainability (EDoS) attacks. Users must verify their credentials with the Cloud Authority for authentication before being granted access to the data while protecting against data breaches

The data access function works through a well-defined structure. The Cloud Administrator inputs the information into the system before encryption and subsequent storage that occurs with predefined access control mechanisms. Upon requests by the End Users, the Cloud Authority examines their credentials to ensure necessary protocol adherence. Successful authentication enables access permission when enforcing both MFA and RBAC policy rules. The Access to download data only happens when all security criteria are me. Failure to meet ant of these results in denial of access to the data for security purposes.

V. METHODOLOGY

The methodology for Cloud: A dual access control system operates within the proposed cloud storage security method to provide enhanced protection. To protect data access and protect against download from unauthorized sources and invasion by a security defence, Multi Factor Authentication (MFA) and Role Based Access control (RBAC) and dual secret sharing have also been implemented into the program to make its implementation. The operational mechanisms of the access control design allow the effective authorizations to work with its protection

systems. First duty of the Cloud Admin is to deposit data in the cloud storage system. AES encryption is a first step of data storage, which is followed by a whole series of procedures to guarantee an authorized personnel access. The reason that the user access control can be based on Attribute Based Encryption (ABE) is that when defining who can access what data, this is defined by the access polices which determine which parties can access which data.

Both encryption method forms two levels of security protection and makes difficult for unauthorized parties obtain crucial confidential data. Thus, MFA provides enhanced security authentication by requiring users to prove their identity by using at least 2 different methods, for instance, password along with OTPs or the biometric verification. RBAC ensures that under users' permission to view data are granted by defined role based access controls which prevent anything unauthorized to access. Implementing this approach makes the security framework stronger and strengthens the user privilege control.

The user credentials are filtrated from the end system to the Cloud Authority to authenticate them. User identity is authenticated by the Cloud Authority by means of authentication policies set up in advance. It allows accessing the requested data records until the credentials of a user match the security conditions established for the authentication process. The system blocks access to users under certain specific security instances. This step provides a sense of security to the authentic users who could stop any non-authorized personnel from accessing the cloud system resources.

The framework provides protection from the attack that tries to reach Economic Denial of Sustainability (EDoS) by requests to download without authorization leading to cloud resource exhaustion. In the Dual Secret Sharing protocols, the system allows data file download only after the user has authorised multiple verifications steps. This approach is installed, and therefore, the chances of an EDoS attack affecting the cloud performance to be accessed by attacker's decreases.

After successful authentication and authorization of the required data, once the Cloud Authority allows them to proceed according to their assigned role and allowed rights. While this system allows data retrieval from this soft limit upwards, it stops users from downloading data beyond safe limits and keeps it as much as possible close to the soft limit. It is the combination of both RBAC and policy based access controls which ensures that the system applies ultimate data access restrictions precisely where data can be accessed.

With these methods, the proposed system ensures protection of the data managed over the cloud while granting access to the authorized files, The solution constitutes the practicality of the data security in the cloud systems, through the combination of the encryption and authentication tools, and access control.

VI. RESULT

Optimizing Cloud Storage and Sharing Through Dual Access Control focuses on the introduction of its security measures as well as on its operational efficiency in accessing data for cloud based platforms. The system uses Attribute Based Encryption (ABS) with Advanced Encryption Standard (AES) so that no one can breach data confidentiality. These are encryption methods that tamper with unauthorized retrieval.

The system conducts test at 3 different points: authentic user authentication, unauthorised access attempts and Economic Denial of Sustainability (EDos) attacks. It was discovered that the users of the system are valid, they access the system quickly and the detection system has blocked all attempts of unauthorized users. The risks of

EDos attacks in the system were minimized by download validation in the system, and as a result, it stopped the excessive use of resources, and preserved the cloud service availability.

Security evaluation metric tests within the framework examined 3 critical areas including system resilience as well as access control accuracy together with encryption strength testing. The system implemented dual encryption together with policy-based access controls to protect itself from typical security threats.

The developed system demonstrates successful cloud security measures together with access control functions that block unauthorized users while better utilizing cloud resources. The encryption system alongside authentication protocols and access control measures shows reliable operation as a valid solution to protect data within cloud storage systems.

VII. CONCLUSION

The proposed Optimizing Cloud Storage and Sharing Through Dual Access Control system produces advanced security measures that make cloud-based storage and sharing more secure and efficient. MFA combining with RBAC and dual secret sharing protocols protects authorized users from all unauthorized parties as the system establishes an additional security layer against EDoS attacks. ABE and AES encryption methods work together to enhance data confidentiality which stops unauthorized data access and breach incidents.

REFERENCES

[1] J. Ning, X. Huang, W. Susilo, K. Liang, Y. Lui, and X. Liu, "Enhancing security for dual access control for cloud-based data storage and sharing," IEEE Trans. Dependable Secure Comput., vol. 19, no. 2, pp. 1036-1048, Mar.-Apr. 2022

[2] K. Logesh and S. Subramanian, "Secure and efficient dual access control scheme in cloud-based data storage and file access with QR code," *Child Stud. Asia-Pac. Contexts*, vol. 12, no. 1, Aug. 2022

[3] A. Liu and T. Yu, "Overview of cloud storage and access control," in *Proc. Int. Conf. Cloud Comput. Serv. Sci. (CLOSER)*, Dec. 2022.

[4] Pais, Mr. Sharan L., et al. 'Overview Of Cloud Storage'. International Journal of Advanced Research in Science, Communication and Technology, Nov. 2021, pp. 188–92.

[5] Pais, Mr. Sharan L., et al. 'Overview Of Cloud Storage'. International Journal of Advanced Research in Science, Communication and Technology, Nov. 2021, pp. 188–92.

[6] L. Malina, V. Benes, J. Hajny, and P. Dzurenda, "Efficient and secure access control system based on programmable smart cards," in Proc. 40th Int. Conf. Telecommun. Signal Process. (TSP), Oct. 2024.

[7] Amazon Web Services, Inc. "Data Warehousing on AWS," AWS Whitepaper. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/data-warehousing-on-aws/data-warehousing-on-aws.html.
Amazon Web Services, Inc., "Logging from

[8] AWS Lambda with Python," AWS Lambda Developer Guide, Mar. 2025. [Online]. Available: https://docs.aws.amazon.com/lambda/latest/dg/python-logging.html.

[9] Serverless, "AWS Lambda," Serverless, [Online]. Available: https://serverless.com/aws-lambda/.