



Implementation of Dual Access Control for Cloud Based Data Storage and Sharing

¹Arati Sanjay Doibale, ²Professor Suvarna Lehekar, ³Dr. V B Kamble

¹ Mtech Student, ²Professor Dept CSE, ³HOD Dept CSE

^{[1][2][3]}Computer Science and Engineering

^{[1][2][3]}PES College of Engineering, Aurangabad, India

Abstract

In today's world of handling data, cloud computing has become really important. It's like a new way of managing data for both organizations and regular people. It's great because it's easy to use and can grow as you need it to. But, there's a big problem with it, keeping your data safe and making sure only the right people can access it. Sometimes, bad things happen, like someone getting into your data without permission. This research paper looks at two ways to make sure only the right people can get to your data in the cloud. Think of it like having two locks on a door to keep your stuff safe. We compare these two ways, one called Attribute-Based Access Control (ABAC) and the other Role-Based Access Control (RBAC). We're talking about how to control who can get to your data and who can download it, all while making sure it stays safe and works well. We also did some tests to see how well these two ways work and how safe they are. It's all about making sure your important information stays protected in the cloud.

Keywords: Cloud Computing, Data Security, Dual Access Control, ABAC, RBAC, Comparative Analysis, EDoS.

INTRODUCTION

In the last few years, cloud computing has completely changed how we handle our data. It's like a big shift in how we store, organize, and get to our information. The cloud is really good because it can grow as you need it, it doesn't cost too much, and you can get to your data from anywhere. But there's a big problem too – sometimes, people who shouldn't get into your stuff can. This can lead to serious issues like data breaches and people snooping on your private information. The thing is, cloud companies have to take care of data from lots of customers on the same computers, which makes it even more important to make sure everything stays safe and private. So, keeping your data secure and private in the cloud has become a really big deal.

Older ways of controlling who gets to use what in computer systems, like Role-Based Access Control (RBAC), have been around for a while. They're good for managing who can do what with data in a system. But when it comes to the cloud, things get more complicated. The cloud is all about being flexible and spread out, which

makes the old ways not so great. That's where Attribute-Based Access Control (ABAC) comes in. It's a newer way of deciding who can do what with data in the cloud. Instead of just looking at someone's role or job, it considers lots of different things about them, the data, and the situation. This makes it much better at handling the complex and changing world of cloud computing.

RELATED WORK

Numerous studies have explored access control mechanisms in cloud environments, each offering unique perspectives on tackling the security challenges. Traditional RBAC has been widely used to manage permissions and roles, but its limitations in handling complex scenarios and dynamic access requirements have led researchers to investigate more advanced models. ABAC, on the other hand, has gained attention for its attribute-centric approach, allowing for dynamic and context-aware access decisions. However, the practical implementation and integration of these models into existing cloud infrastructures remain areas of ongoing research.

This paper builds upon the foundation laid by previous research by proposing a comprehensive dual access control framework that draws from the strengths of both RBAC and ABAC. By doing so, we aim to address the shortcomings of existing methods and provide a more robust solution for secure data storage in the cloud. In the subsequent sections, we will outline the design, implementation, and evaluation of the dual access control framework, along with a discussion of the results and implications of this research.

In this paper, we propose a dual access control framework that integrates RBAC and ABAC principles to enhance the security posture of cloud-based data storage systems. By combining the strengths of both models, we aim to establish a robust and flexible access control mechanism that not only ensures the right users have access to the right data but also considers contextual information during access decisions. This framework seeks to mitigate the vulnerabilities associated with traditional access control methods in cloud environments and contribute to the overarching goal of achieving data confidentiality, integrity, and availability.

ABAC

ABAC enables the creation of policies based on attributes associated with users, objects, and the environment. This enables fine-grained control over who can access what under specific conditions. User attributes may include roles, department, location, and security clearance. Object attributes can comprise sensitivity level, owner, and creation date.

RBAC

RBAC simplifies access control by categorizing users into roles and assigning permissions to roles. Users acquire the privileges associated with their roles, allowing for efficient management. Roles can be predefined (e.g., admin, user) or customized based on organizational requirements.

Antonis Michalas proposed a data sharing protocol that combines symmetric searchable encryption and ABE, which allows users to directly search over encrypted data. To implement the functionality of key revocation

in ABE, the protocol utilizes SGX to host a revocation authority. Bakas and Michalas later extended the protocol and proposed a hybrid encryption scheme that reduces the problem of multi-user data sharing to that of a single-user. In particular, the symmetric key used for data encryption is stored in an SGX enclave, which is encrypted with an ABE scheme. It deals with the revocation problem in the context of ABE by employing the SGX enclave.

The worry of security breach over outsourced data may be one of the main obstacles hindering Internet users from widely using cloud-based storage service. Apart from economic loss, unlimited download itself could open a window for network attackers to observe the encrypted download data that may lead to some potential information leakage (e.g., file size).

In the existing system the data owner is required to generate a set of challenge ciphertexts in order to resist the attack, which enhances its computational burden. Second, a data user is required to decrypt one of the challenge ciphertexts as a test, which costs a plenty of expensive operations (e.g., pairing). The computational complexity of both parties is inevitably increased and meanwhile, high network bandwidth is required for the delivery of ciphertexts. The considerable computational power of cloud is not fully considered.

PROPOSED SYSTEM

In this project, we propose a new mechanism, dubbed dual access control, to tackle the existing system problem. To guarantee the confidentiality of outsourced data without loss of policy based access control, we start with a CP-ABE system, which is seen as one of the building blocks. We further employ an effective control over data users' download request on the top of the CP-ABE system. We design a new approach to avoid using the technique of "testing" ciphertext. Specifically, we allow data user to generate a download request. Upon receiving the download request, with help of the authority or the enclave of Intel SGX, a cloud server is able to check if the data user is authorized to gain access to the data. No other information is revealed to the cloud server except the knowledge of whether the user is authorized. Based on the above mechanism, the cloud maintains the control of the download request.

In our proposed systems, the outsourced data is encrypted prior to being uploaded to cloud. No one can access them without valid access rights. Given an outsourced data, cloud server cannot identify data owner, so that the anonymity of owner can be guaranteed in data storage and sharing. Data owner keeps controlling his encrypted data via access policy after uploading the data to cloud. In particular, a data owner can encrypt his outsourced data under a specified access policy such that only a group of authorized data users, matching the access policy, can access the data. A cloud server is able to control the download request issued by any system user, where the download request can set to be anonymous. With the control over download request, we state that our systems are resistant to EDoS attacks.

An EDOS (Economic Denial of Sustainability) attack, in simple language, is a type of cyberattack where someone tries to harm a company or organization financially by overloading its computer systems or networks. It's like sending so much fake traffic or requests to their computers that they can't keep up, causing their

services to slow down or even crash. This attack can disrupt the normal operation of the company, making it harder for them to make money and provide their services to customers. It's a bit like blocking the entrance to a store, so no one can come in and buy things, which hurts the store's business.

SYSTEM DESIGN

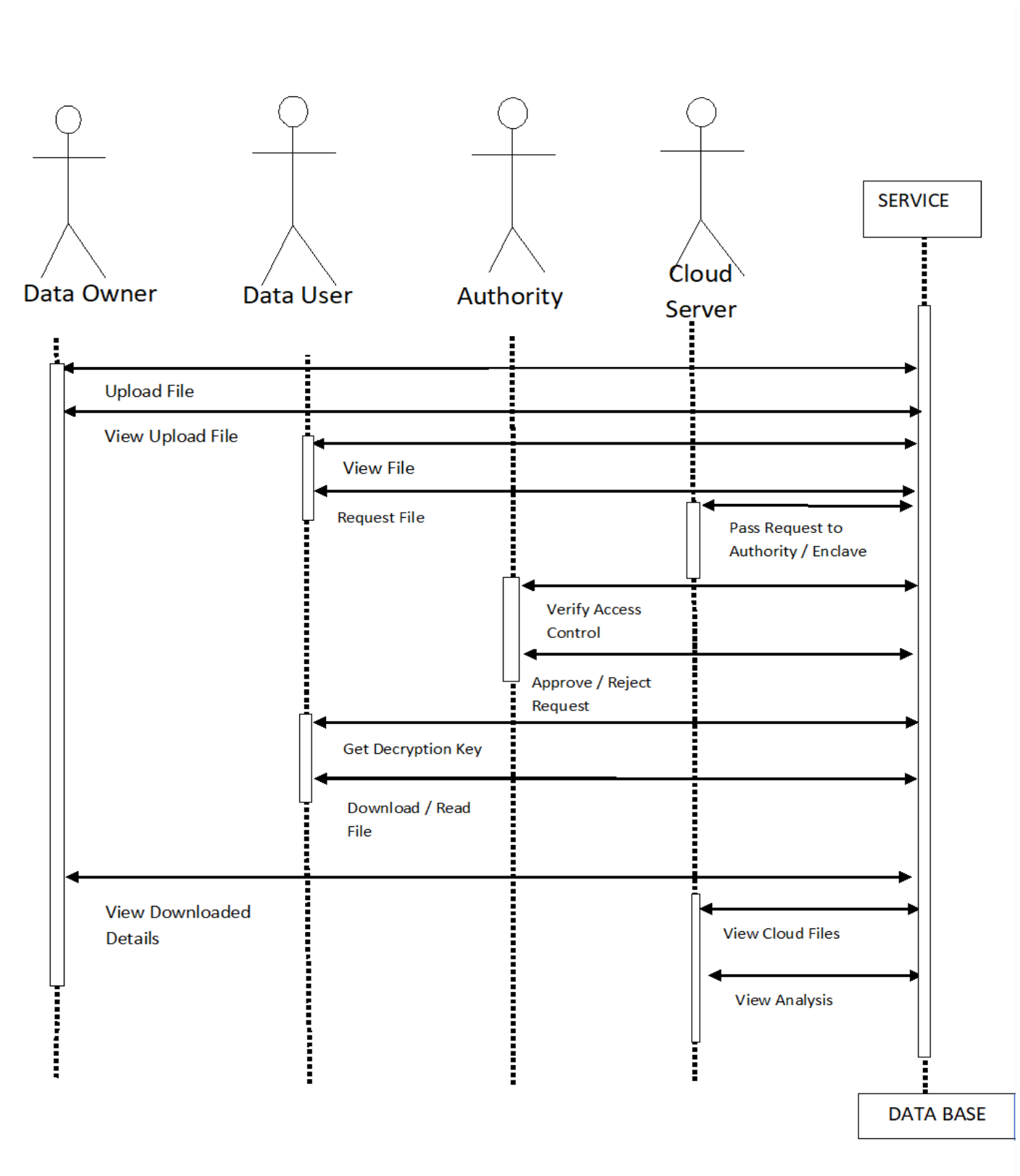
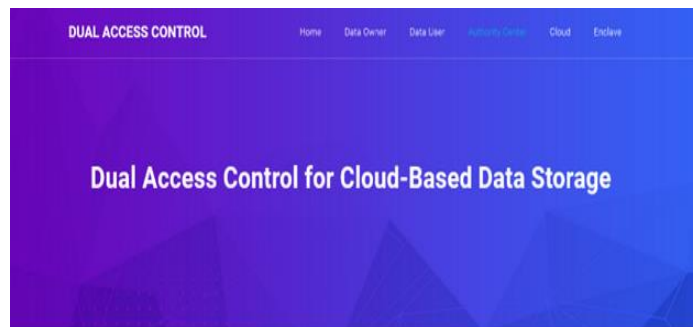


Fig. Sequence Diagram for System Design

In system design the sequence diagram are used to present the dual access control framework. A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes

operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

RESULTS



ABSTRACT

Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low cost management. Since it provides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.



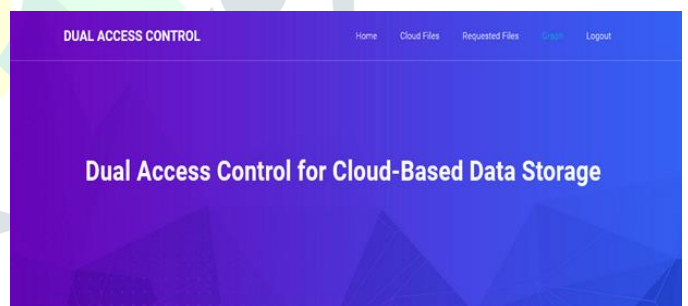
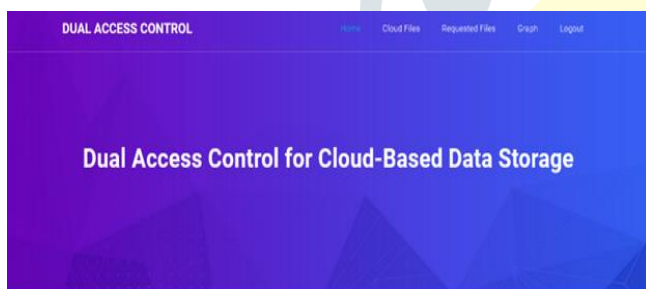
Authority Login

Email:

Password:

Fig. 2 Home Screen

Fig. 3 Authority Login



Welcome To Cloud Server!



Fig. 4 Cloud Server

Analysis

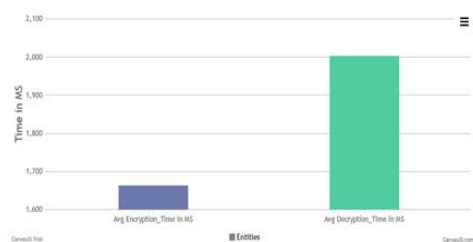
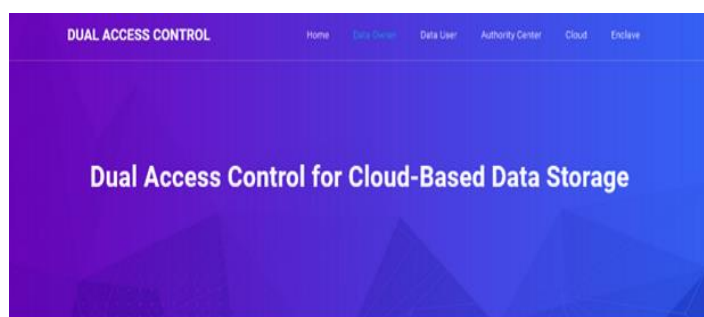
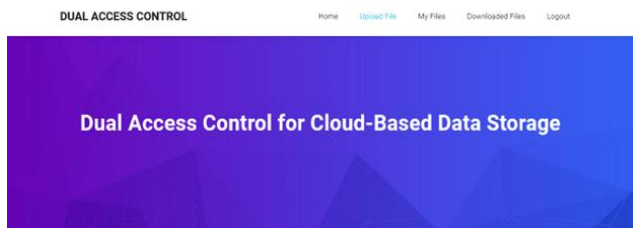



Fig. 5 Encrypted data Analysis

Upload File

File Keyword:

Select File:
 No file selected.

Access Policy:

Select Access Members:
 Student
 Professor
 Principal

Preview File:

Data Owner Login

Email:

Password:

Fig. 6 Data Owner Uploading file

Fig. 7 Data Owner login

CONCLUSION

In our enhanced system, we employ the fact that the secret information loaded into the enclave cannot be extracted. However, recent work shows that enclave may leak some amounts of its secret(s) to a malicious host through the memory access patterns or other related side-channel attacks. The model of transparent enclave execution is hence introduced. Constructing a dual access control system for cloud data sharing from transparent enclave is an interesting problem. In our future work, we will consider the corresponding solution to the problem.

The paper concludes by summarizing the contributions of the dual access control framework to cloud-based data storage and sharing security. Our implementation and performance evaluation indicate that the proposed system effectively addresses the challenges of data security and sharing in cloud environments. Future work could involve exploring additional optimizations and further enhancing the scalability of the system.

References

- [1] Jianting Ning, Xinyi Huang, Willy Susilo, Kaitai Liang, Ximeng Liu, and Yinghui Zhang, Dual Access Control for Cloud-Based Data Storage and Sharing, IEEE paper 2019.
- [2] Shwetha Shree, Mohan Kumar, DUAL ACCESS CONTROL FOR CLOUD BASED DATA STORAGE IRJMETS paper 2022.
- [3] Karukuri Silpa Kala, Dr.Gobi Natesan, Dual Access Control for Cloud based data storage and sharing, IJARCCCE paper 2023.
- [4] Ramesh Byali B., Jyothi C., Megha Chidambar Shekadar D., Dual Access Control for Cloud based data storage and sharing, IJRPR paper 2022.

- [5] Y.G.Min and Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions," *Journal of Security Engineering*, vol. 2, 2012.
- [6] Sahai and B. Waters. "Fuzzy Identity Based Encryption.," In *Advances in CryptologyEurocrypt*, volume 3494 of LNCS, pages 457– 473. Springer, 2005.
- [7] B.Sosinsky, "Cloud Computing Bible,," Ed. United States of America: Wiley,2011.
- [8] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In *Workshop on hardware and architectural support for security and privacy (HASP)*, volume 13, page 7. ACM New York, NY, USA, 2013.
- [9] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In *SecureComm 2019*, pages 472–486, 2019.
- [10] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
- [11] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *S&P 2007*, pages 321–334. IEEE, 2007.
- [12] Victor Costan and Srinivas Devadas. Intel sgx explained. *IACR Cryptology ePrint Archive*, 2016(086):1–118, 2016.
- [13] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017*, pages 765–782, 2017.
- [14] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology-CRYPTO 1999*, pages 537–554. Springer, 1999.