JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DUAL ACCESS CONTROL FRAMEWORK FOR CLOUD BASED DATA STORAGE

Arati Sanjay Doibale

Student, Master of Technology, Computer Science and Engineering,

P.E.S. College of Engineering, Aurangabad, India

Abstract

This paper addresses the challenges posed by cloud computing in terms of data security, privacy, and efficient sharing. While cloud-based data storage has revolutionized accessibility and collaboration, it necessitates robust security measures. The proposed solution introduces a novel dual access control mechanism tailored for cloud-based data storage and sharing. The popularity of such services in academia and industry has surged due to their cost-effective management. However, operating within an open network demands secure mechanisms to ensure data confidentiality and user privacy. While encryption is a commonly used security measure, it alone falls short of practical data management requirements. Additionally, the paper emphasizes the need for effective access control over download requests to prevent Economic Denial of Sustainability (EDoS) attacks. The key innovation lies in a dual approach to access control addressing data access and download requests while upholding security and efficiency. The paper outlines two distinct dual access control systems, each catering to specific settings, and provides security analyses and experimental findings for both systems.

Keywords: Cloud Computing, ABAC, RBAC, Comparative Analysis, EDoS, CP-ABE.

Introduction

Dual access control in the context of cloud-based data storage and security refers to a mechanism where data access is controlled by two distinct factors or entities, adding an extra layer of security. This can involve combining traditional authentication methods (such as usernames and passwords) with additional factors like biometric authentication, hardware tokens, or time-based constraints.

Dual access control adds an extra layer of security, making it more difficult for unauthorized users to gain access to sensitive data. Even if one factor is compromised, the attacker would still need to overcome the second factor.

Dual access control is a form of multi-factor authentication, where users are required to provide two or more authentication factors before gaining access. This significantly reduces the risk of unauthorized access resulting from stolen passwords or credentials. By requiring multiple factors for access, the likelihood of successful cyberattacks and data breaches is lowered. This is especially important for organizations dealing with sensitive or confidential data. Many industries are subject to strict compliance and regulatory standards, such as HIPAA in healthcare or GDPR in Europe. Dual access control can help organizations meet these requirements by demonstrating a higher level of security.

Dual access control can help protect user privacy by ensuring that only authorized personnel can access personal or sensitive data. Cloud-based storage often involves remote access. Dual access control helps secure remote access points and prevents unauthorized individuals from gaining entry. By requiring multiple authentication factors, organizations can establish a clearer trail of accountability for data access. This can be crucial in case of unauthorized access incidents. Dual access control makes it more difficult for attackers to succeed in phishing attacks. Even if a user's password is compromised through phishing, the attacker would still need the second factor to gain access. Dual access control can be used to grant temporary access to users for specific tasks or time periods. Once the time limit expires, access is automatically revoked. Organizations can implement different levels of access control for different data or resources, ensuring that only authorized individuals can access specific parts of the cloud storage

Incorporating dual access control into cloud-based data storage and security strategies can provide robust protection against unauthorized access, data breaches, and cyber threats. However, it's important to carefully implement and manage such systems to balance security with user convenience and usability.

In recent years, cloud-based storage services have become really popular in both academic and business circles. These services are commonly used in various online applications like Apple’s iCloud. The reason they’re so popular is because they offer a bunch of benefits, like easy access to data and not having to worry about managing data on your own devices. Lots of people and companies now choose to store their data on remote cloud severs. This way, they can avoid spending a lot of money on upgrading their own data storage systems. However, there's a big concern about the security of data stored on these remote servers. People worry that their data might be accessed or stolen by unauthorized individuals. This fear of security issues is a major reason why many internet users are hesitant to use cloud-based storage services extensively.

Background and Related Work

In cloud-based storage services, there's a known type of attack called a resource-exhaustion attack. Imagine the cloud as a big storage space where people can download their files from. But because the cloud doesn't really limit how many times someone can ask to download something, a person with bad intentions could send tons and tons of download requests to the cloud server. This would be like flooding it with too many requests, and as a result, the cloud service wouldn't be able to handle all these requests, leaving regular users without proper access. This is called a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack. It's like someone messing with the cloud so that it can't work properly for everyone else. This can cause

problems in how the cloud service charges people, because if it uses a "pay-as-you-go" system, the costs might go up a lot when dealing with these attacks. Basically, the bills for using the cloud service could become really high when these attacks happen often.

But that's not the only problem. Allowing unlimited downloads could also let attackers sneak a peek at encrypted data that's being downloaded, even if they can't read it. This could give them hints about things like the size of the files, which could be a form of information leakage. So, it's really important to have a good way to control how many download requests happen for the data stored on the cloud, especially if it's encrypted.

In this paper, we suggest a fresh solution called "dual access control" to solve the two problems we mentioned earlier. To make sure data is safe in cloud-based storage services, we're looking at a method called attribute-based encryption (ABE). It's like a strong lock that keeps data private and also lets us manage who can see it really precisely.

One version of ABE, known as Ciphertext-Policy ABE (CP-ABE), is a smart way to hide data. With this, we can set rules about who gets to see the data, even if it's hidden. It's like we're putting a secret note on the data and only certain people who meet the rules can read it. This is what we're using in our solution. But just using CP-ABE isn't enough to make everything work smoothly. We need to do more to make sure we control both who can access the data and how many times they can download it. Cloud computing is super handy for storing and sharing data, but we're still worried about people getting into our stuff without permission. This paper talks about a new way to deal with these worries. It's like having two strong locks to keep our data safe. The idea is to combine two important ideas: one about who can do what (called ABAC), and the other about what roles people have (called RBAC). By putting these two ideas together, we can make sure that the right people have the right access to the data, and we can prevent sneaky stuff from happening.

Dual Access Control Framework

The practical implementation of the dual access control framework is described, including how ABAC and RBAC policies are defined, enforced, and integrated into the cloud environment.

Data owner*:*

Data owner holds the data and wants to outsource his data to the cloud. In particular, data owners only want to share their data with those who satisfy certain conditions (e.g., student, professors or principal). They will be offline once their data have been uploaded to the cloud.

Data User*:*

Data user wants to download and decrypt the encrypted data shared in the cloud. Those who are authorized can download the encrypted file and further decrypt it to access the plaintext.

Authority*:*

Authority is responsible for initializing system parameters and data user registration. Also, it handles the call request from the cloud in the first proposed construction.

Cloud Server:

Cloud provides convenient storage service for data owners and data users. Specifically, it stores the outsourced data from data users and handles the download requests sent by data users.

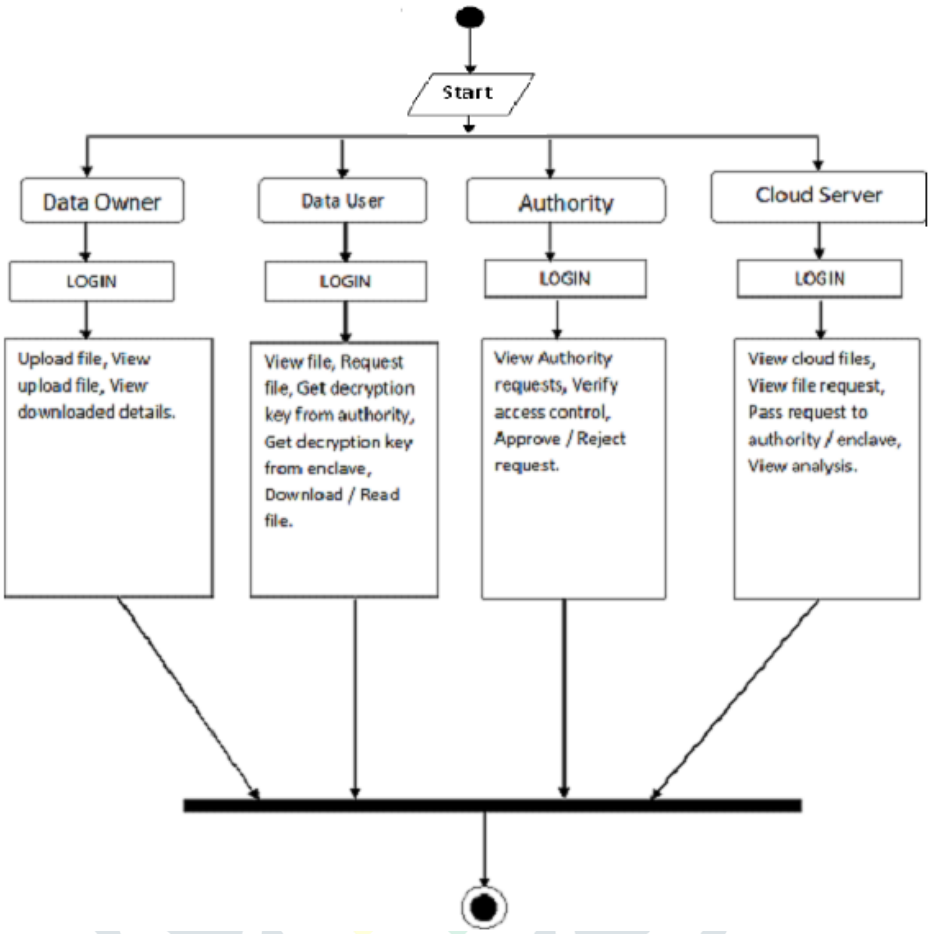

Fig.1 Dual access control framework

Enclave*:*

Enclave handles the call request from the cloud (used in the second system).

Conclusion

We tackled a challenging and long-lasting issue related to sharing data in cloud systems. We introduced two special ways to control who can access this data. These methods are designed to resist attacks that try to disrupt the service. We also mentioned that the way we manage download requests could be used in other similar setups.

Our tests showed that the new systems we proposed don't slow things down much, which is a good thing. However, in our advanced system, we used a special place to hide secrets so they can't be taken out. But it turns out this special place can sometimes accidentally give away a tiny bit of information to bad actors. This happens through things like how the memory is used. So, we're thinking about how to solve this in the future.

We want to build a system that controls sharing in the cloud using this special setup that's harder to break into. This is something we'll work on in our future projects.

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, IJARCCE 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," Journl 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