IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306153|

Dual Access Control for Cloud-Based Data Storage and Sharing

Selvi P, Rishi

Assistant Professor, Department of CSE, Jayam College of Engineering and Technology, Dharmapuri, Tamil Nadu, India

Student, Department of Master of Computer Application, Jayam College of Engineering and Technology, Dharmapuri, Tamil Nadu, India

ABSTARCT: 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 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 attacks cannot be launched to hinder users from enjoying service. In this scheme, 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.

KEYWORDS: Data Storage Service, Data Management, Dual Access Control, Public Key Encryption

I. INTRODUCTION

Dual access control for cloud-based data storage and sharing is a security mechanism that provides a layered approach to protecting sensitive data stored in the cloud. It combines two levels of access control: one at the cloud service provider's side and the other at the user's side. The cloud service provider manages the access control policies and enforces them at the cloud level, while users manage their own access control polices and enforce them at the user level. This approach ensures that only authorized users can access and share sensitive data, while preventing unauthorized access. Dual access control is particularly useful for organizations that require strict data security measures to protect confidential information. By implementing dual access control, organizations can enhance the protection of sensitive data and maintain control over who has access to it.

Due to its extensive list of advantages, which includes access freedom and the lack of local data management, inmanyInternet-based commercial products (suchas Apple iCloud). Nowadays, a growing number of people and businesses prefer to outsource their data to faraway clouds in order to avoid having to upgrade their local data management facilities or devices. However, one of the biggest barriers preventing Internet users from embracing cloud-based storage services generally may be their concern about security breaches involving outsourced data. Outsourced data may need to be subsequently shared with others in many practical scenarios. Alice, a Dropbox user, might send her friends pictures [1]. Without employing data encryption, Alice must first create a sharing link and then distribute it to others in order to share the images. The sharing link may be exposed at the Dropbox administration level, even though it guarantees some level of access restriction over unauthorized users (for example, those who are not Alice's friends) (e.g., administrator could reach the link). A simple solution to prevent shared photos from being accessed by system "insiders" is to specify the group of authorized data users before encrypting the data. However, Alice might not always be aware of who will be receiving or using the photos. Alice might only be aware of attributes related to photo receivers. One of the emerging developments is distributed computing.

Recently, both academia and businesses have been paying a lot of attention to cloud storage services. Due to a wide group of benefits, it includes freedom of access and absence limited information management, this can widely using in many internet applications (such as Apple iCloud). Nowadays, most of businesses and people choosing their data

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306153|

outsource to remote clouds. So that they don't have to upgrade their on-premises or data management devices. The main biggest challenge is to preventing users from internet widely adopting the cloud storage services is the fear of involving outsourced data in security breaches. The outsourced data can be shared subsequently to the others in many real-world scenarios. For example, Alice could send her pictures with Dropbox. The set of authorized data users identifying before data is encrypted in a simple technique. To prevent photos shared from read by system "insiders" who have to access the system. However, Alice may occasionally be completely unaware of the recipient or user of the photos. The probability that Alice is single has an understanding of the characteristics of photo receivers. Traditional public key encryption, such as Paillier encryption, cannot be used in this situation because it required to know the encrypt or identity of the receiver data in advance. Therefore, it would be ideal to provide policy based encryption mechanisms on external photos so that Alice can use mechanisms to give access policies for encrypted photos. It can be select only the authorized people, they can access the photos. By using dummy cipher texts to confirm the receiver's data decryption permissions is a crude solution to checking download requests.

II. LITERATURE SURVEY

1. Dual Access Control for Cloud-Based Data Storage and Sharing
Author - JiantingNing, Xinyi Huang
Year-2022
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 article, 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 article, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.

2. Dual Access Control for Cloud Based Data Storage and Sharing
Author - Mrs. T. Ratnamala 2 Syed Ameer Sohail
Year-2023
Dual access control for cloud-based data storage and sharing is a security mechanism that allows authorized users to access and share sensitive data while preventing unauthorized access. This approach employs two levels of access control: one at the cloud service provider's side and the other at the user's side. The cloud service provider manages the access control policies and enforces them at the cloud level, while users manage their own access control policies and enforce them at the user level This approach provides a layered securing model that enhances the protection of sensitive data stored in the cloud, particularly for organizations with strict data security requirements. This abstract summarizes the key concepts of dual access control for cloud-based data storage and sharing and highlights its benefits for ensuring data privacy and security.

3. Dual Access Control for Cloud Based Data Storage and Sharing
Author - Mrs. T. Ratnamala 2 Syed Ameer Sohail
Year-2023
Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent yearsdueto 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 frombeing compromised, the most widely used method is encryption. However, simply encrypting data 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 attacks cannot be launched to hinder users from enjoying service. In this scheme, 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.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306153|

III. EXISTING SYSTEM

Due to its effective and affordable administration, cloud-based data storage has recently attracted growing attention from academia and business. Since services are delivered via an open network, it is critical for service providers to adopt secure data storage and sharing mechanisms to protect user privacy and the confidentiality of data. The most popular technique for preventing the compromise of sensitive data is encryption. The actual necessity for data management, however, cannot be completely met by just encrypting data (for instance, using AES). Additionally, a strong access control over download requests must be taken into account to prevent Economic Denial of Sustainability (EDoS) assaults from being performed to prevent users from using the service. This study takes into account dual access control in the context of cloud-based storage in the sense that we create a control mechanism over both data access and download requests without sacrificing security and effectiveness. This article presents the design of two dual access control systems, one for each intended environment. There is also a presentation of the systems' experimental and security analyses.

DISADVANTAGES

- 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.

IV. PROPOSED SYSTEM

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.

ADVANTAGES

- 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.

V. MODULES DESCRIPTION

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.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306153|

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.

VI. CONCLUSION

We addressed an interesting and long-lasting problem in cloud-based data sharing, and presented two dual access control systems. The proposed systems are resistant to DDoSs/EDoS attacks. We state that the technique used to achieve the feature of control on download request is "transplantable" to other CP-ABE constructions. Our experimental results show that the proposed systems do not impose any significant computational and communication overhead.

VII. FEATURE ENHANCEMENT

In conclusion, dual access control can be an effective security measure for cloud-based data storage and sharing. By using a combination of authentication and authorization controls, dual access control helps to prevent unauthorized access to sensitive data and ensures that only authorized users can view or modify data. In addition, it can help to improve accountability by allowing administrators to monitor access and usage of data. However, it's important to remember that no security measure is fool-proof, and implementing dual access control should be done in conjunction with other security measures such as encryption, regular data backups, and employee training. Overall, dual access control is an important component of a comprehensive security strategy for cloud-based data storage and sharing.

REFERENCES

[1] AlexandrosBakas and AntonisMichalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.
[2] JiantingNing, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei. Auditable σ-time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018.
[3] JiantingNing, Zhenfu Cao, Xiaolei Dong, and Lifei Wei. White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively. IEEE Transactions on Dependable and Secure Computing, 15(5):883–897, 2018.
[4] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. Security Symposium, Security, pages 16–18, 2017.
[5] Ben Fisch, DhinakaranVinayagamurthy, 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.
[6] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. Intel R software guard extensions: Epid provisioning and attestation services. White Paper, 1:1–10, 2016.
[7] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details