IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12348

Dual Access Control For Cloud-Based Data Storage And Sharing

Karukuri Silpa Kala[1], Dr.Gobi Natesan[2]

Student, School of Computer Science and IT, Jain (Deemed-to-be) University, Bangalore, India[1]

Assistant Professor, School of Computer Science and IT, Jain (Deemed-to-be) University, Bangalore, India[2]

Abstract: In recently cloud data storage increasing interest from both industry and academia due to its efficient and affordable Management. Service providers take on storage data and sharing mechanism as services are provided over an open network that protects user privacy and data confidentiality. The Encryption method is used for prevent sensitive data from being compromised. However, the actual requirement to just encrypt the data (using AES for example) will not completely solve the data management needs. In addition, to prevent EDOS (Economic Denial of Sustainability) attacks, which are carried out to prevent users from using the service, robust access control of download requests should be considered. The control access in the cloud storage here we can develop over control mechanism download requests as well as data access without compromising efficiency or security. This article designs the two dual access control systems, each used for conscious environment. An experimental and safety analysis of system is also presented.

Keywords: Cloud data sharing, Advantage of cloud capacity, Control, Attribute based encryption.

I. INTRODUCTION

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 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 encryptor 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 ciphertexts to confirm the receiver’s data decryption permissions is a crude solution to checking download requests. Specifically, it requires the owner of the data, say Alice, to upload some "test" ciphertexts alongside the "real" data encryption to the cloud where the "test" ciphertexts exist. Dummy message encryption is like as “real” data to access as subject to same access restrictions. Cloud requests that a user named Bob download one of the "test" ciphertexts, which Bob then decrypts at random. The "current" data is available to Alice if result is successful or returned the decryption, indicating the Bob has the authority in legitimate decryption. It allows to Bob can download ciphertext relevant from the cloud.

II. SURVEY MOTIVATION AND METHODS

This Survey Provides the use of ABE to achieve Fine-grained Policy based encryption can control at encrypted data. A CP-ABE and KP-ABE, both of which are referred to as key research branches of ABE, are policies ABE. The main subject of this survey is the first. A CP-ABE links the attribute set and the decryption key together with encrypted text that is part of the access policy. CP-ABE is a fantastic option for safe cloud data sharing because of its feature (compared to KP-ABE).

Noting that KP-requirement ABE's decryption key is connected to policy access it leads for high cost storage to cloud users. Since the initial release of CP-ABE, numerous papers have advocated its use in a range of applications. Although this can provide the Fine-grained access policy, The CP-ABE can be working as standalone solution, it cannot be

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12348

successfully assaults on EDOS, this can happen when DDoS occurs on cloud context. A number of assault securities have been proposed in the literature. It provides a method for defend to sharing cloud data against to attack.

This survey examines the access control strategies existing by the others. Then it can describe the proposed solution for access control in distributed computing. FADE is given by the Y. Tang and his colleagues. It is important to approach, another access control. In cloud it repurposing the information, this technique can be provides the Fine-grained access control for secure deletion. For this actually it does not need the strategy. The data owners and the specialized cooperatives in the same idea. HASBE, is a plan presented by Z. Wan, J. Liu, and R. H. Deng, it is another control access plan. It is the most important in downside it is less customizable than other schemes. S. Yu and his colleagues Distributed Computing Access Control Mechanism.

KPABE (Key Policy Attribute Based Encryption) used in this technique this method is not customizable. The complication of encryption and decryption is increasing. The temporary access can be provided by the Y. Zhu and his colleagues. In distributed computing approach, these approaches can be applicable only for frameworks which can contain data. The owner and the professional co-operatives are familiar to the same space. The other major plots are described and provided by M. Li and his group. However, the plan is expensive the M. Zhou and his colleagues are preserving privacy access control for distributed computing.

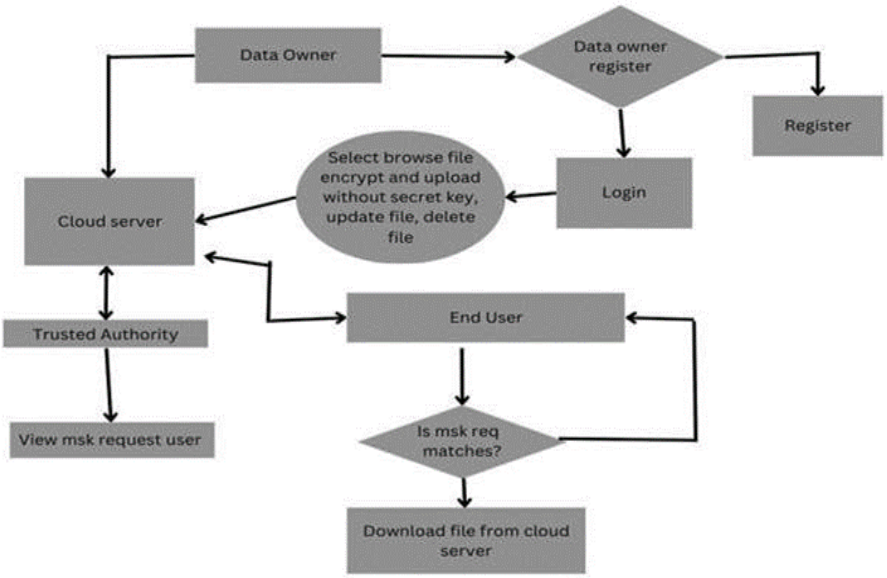
III. SURVEY OUTCOMES

This Survey provides dual access control system for data. The Attribute based encryption (ABE) is used to enable confidentiality of outsourced data. It is for the potential candidates and as well as who having a control over Fine-grained control at outsourced data. The data can be backup to the cloud storage services.

Especially, the CP-ABE can provide the dependable data encryption method. Allows specification to access the rules it specify access rights to future data Recipient, via encryption data. This study can be investigated the uses and importance of the CP-ABE method. By using a CP-ABE alone approach, the system ensures sophisticated control over the both access data and downloading requests. The dummy ciphertext can used to verify recipient's data authority of data can be follows: The Crude Solution is used for to control and download the requests. The "test" Ciphertexts, are encrypting communications that follow similar policies access at "real" cloud here the data can be uploaded to the cloud, with "real" encryption of the data.

For example, when user Bob request a file to download, the cloud can respond to Bob, to decrypt the file. A "test" of the ciphertext, given the correct decryption or result (if Bob decryption is privileged), Alice Bob gave permission to access the data and the cloud give the permission to the user to download request.

IV. FLOW CHART



International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12348

V. CONCLUSION

We introduced two dual access control systems and a wide range of introducing subjects. The DDOS and EDOS attacks cannot be used in the proposed system. we argue with different CP-ABE constructs can "port" the procedures used for execution. Download request control function. The proposed solution does not cause major according to the results of our experiments, computational or communication effort (relative to the CP-ABE underlying building block). The advantage of fact that secrets information can be entered into enclave but in hardened system it can't be recovered. The access patterns in memories or another equivalent channel attacks can prevent enclaves from leak some of his/her secrets to a host. Therefore, it develops transparency and approach enclave execution. The interesting demanding is creating a dual access control for cloud based data storage and data sharing by transparent enclaves.

REFERENCES

[1]. Ittai Anati, Shay Gueron, Simon Johnson and Vincent Scarlata. Innovative technology based on processor certificat ion and sealing.Hardware and Architectural Assistance for Security and Privacy (HASP) Workshop,Volume 13, Pa ge 7. ACM New York, NY, USA, 2013.
[2]. Jiguo Li, Xiaonan Lin, Yichen Zhang and Jingguang Han. Ksfoabe: Outsourced signature-based encryption with keyword search for cloud storage. IEEE Transactions on Service Computing,10(5):715–725, 2017.
[3]. Alexandre Vacas and Antonis Michalas. Modern Family: A reversible hybrid encryption scheme based on the attribute cipher, symmetric lookup cipher, and SGX. In Secure Comm 2019, p. 472-486, 2019.
[4]. J. Ning, X. Huang, E. Susilo, K. Liang, X.Liu and Y. Zhang, "Dual Access Control for CloudBased Data Storage a ndShares", in IEEE Transactions on Trusted and Secure Computing, vol. 19, Number 2, p. 1036_1048, March 1-April 2022.
[5]. Byali, Ramesh & Jyothi, & Shekadar, Megha. (2022). "Dual Access ControlSecurity for CloudBased Data Sharing and Storage. International Journal of Research Publishing and Review. 170-172.