Shodhshauryam, International Scientific Refereed Research Journal
Available online at : www.shisrrj.com
OPEN ACCESS
© 2024 SHISRRJ | Volume 7 | Issue 2
ISSN : 2581-6306
doi : https://doi.org/10.32628/SHISRRJ

Dual Access Control for Cloud-Based Data Storage and Sharing

Ms. N. Bavana[1], M. Induu[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India
[2]Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

Article Info

Article History
Received : 25 March 2024
Published : 10 April 2024

Publication Issue :
March-April-2024
Volume 7, Issue 2

Page Number : 435-439

ABSTRACT

In recent years, cloud-based data storage systems have become more and more popular in academia and industry due to their efficient and reasonably priced management. Because service providers operate in an open network, it is essential that they Adopt secure data storage and exchange practices to protect customer confidentiality and privacy. Encrypt is the most popular technique for guarding against the compromise of private information. However, data encryption on its own—using AES, for instance—is unable to satisfy the practical need for data management. A robust download request access control system is also necessary to guard against attacks such attempts to prevent users from using the service, such as Financial Denial of Sustainability (EDoS). In this work, we explore the use of dual access control for cloud-based storage, ensuring that security and efficiency are maintained while establishing a control mechanism for download and data access requests. In this study, 2 dual authentication systems are built, one for a particular planned context. There is also a security analysis and an experimental review of the systems.

Keywords : Access Pattern, Search Pattern, Multi-Keyword Searching, Multi-User Access, Searchable Encryption.

I. INTRODUCTION

1.1 Motivation:

The reasons for implementing dual access control for cloud-based data storage and sharing are as follows: maintaining client and stakeholder trust; protecting intellectual property; ensuring enhanced security; providing comfort; and gaining a competitive edge.

1.2 Problem Synopsis:

Secure dual access control is a major issue in cloud-based data storage and sharing environments, necessitating the creation of robust solutions that protect private information while allowing authorized user participation.

1.3 Project Objective:

It is envisaged that dual access control would enhance the security and privacy of sensitive information while maintaining efficient teamwork and data accessibility for cloud-based data sharing and storage.

1.4 Scope:

Setting up a comprehensive security framework that allows administrators and users to authenticate and grant access to sensitive data stored in the cloud is necessary for bidirectional access control for sharing and storing data in the cloud order to guarantee data privacy, integrity, and accountability.

1.5 Project Overview:

Over the past few decades, Academic and industry communities have shown a great deal of interest in cloud-based storage systems. corporate worlds. Owing to its many advantages, including free local data management and flexible access, it might be widely utilized in a range of Internet-based commercial applications (like Apple iCould). Nowadays, a growing number of people and businesses choose to outsource their data to remote clouds in order to avoid having to pay for the upkeep of their local infrastructure and data management equipment.

In this study, we address the two aforementioned issues by providing a novel solution that we call two-way access control. One potential solution for improving security for data in cloud-based storage systems is attribute-based encryption (ABE) [9]. It allows for fine-grained influence over the data which is contracted while maintaining data confidentiality. In particular, CP-ABE (Ciphertext-Policy ABE) [5] offers a useful method of encrypting data such that access policies may be correctly defined over encrypted data, determining the access privilege of possible recipients of the encrypted data. Take note that in this study, we discuss how we used CP-ABE in our methodology. Nevertheless, developing a sophisticated It takes more than simply the CP-ABE technique to create a system that guarantees control over download requests as well as data access.

II. SURVEY OF LITERATURE

2.1 CONNECTED WORK

ABE has been proposed as a smooth policy-based oversight of encrypted data in the literature [9], [29]. ABE, in particular, has two major and unique study branches available: CP-ABE and KP-ABE, or keypolicy ABE. This article focuses mostly on the former. The ciphertext is combined with the access strategy in a CP-ABE, or an attribute set is linked to the decryption key. Because of this functionality, CP-ABE is a great option for sending data securely via the cloud. Due to KP-ABE requires that the decryption key be tied to the access policy, cloud customers face considerable storage expenses.

Since the release of the pioneering CP-ABE, several research have been proposed for its usage in a range of applications [9]. Among them are responsible and multi-authority [10], [17], traceable [22], [23], [24], [25], outsourced [15], [16], [21], and extensible versions [14]. As a stand-alone solution, CP-ABE is not viable nor successful in protecting against EDoS assaults while allowing for fine-grained data access [11], as it is with DDoS in cloud settings [11], [39]. The literature has proposed many countermeasures against the attack [12], [33].

According to Xue et al. [38], previous research were unable to totally repel the computational level EDoS attack, although they did offer a defense against the attack for cloud data sharing security.

However, [8] has two downsides. The data owner's processing overhead is raised since, in order to defend against the assault, they must first produce a sequence of challenge ciphertexts.

Second, a test requires the data user to decode one of the task ciphertexts, requiring several costly processes (such as pairing). In this circumstance, both sides' computing complexity would undoubtedly increase, and the transmission of ciphertexts will need a significant amount of network bandwidth. [38] does not fully account for the cloud's substantial processing capacity. In this paper, we will provide a revolutionary strategy that requires less computing power.

In the face of the DDoS attack, communication costs must stay constant. Users can now search encrypted data thanks to a data sharing mechanism developed by Antonis Michalas [20]. instantaneously. It combines ABE and symmetric searchable encryption.

To achieve Revocation of keys The protocol uses SGX as a revoking entity in ABE. Following [20]'s protocol expansion, Bakas with Michalas [3] created a hybrid encryption method that simplifies multi-user data exchange.

More specifically, an ABE-encrypted SGX enclaves houses the symmetric key needed for data encryption. To be more precise, the symmetric key required for data encryption is present in an SGX compartment encrypted using the ABE technique. In the larger picture of ABE, it takes advantage of the SGX region to address the revocation issue, similar to [20]. In this work, we use SGX to manage download requests, effectively mitigating DDoS/EDoS assaults. In this sense, our objective and methods differ from the procedures described in [3] and [20].

In addition to incurring money loss, uncontrolled downloads may allow network attackers to read encrypted download data, potentially resulting in information leakage. As a result, it is also required to efficiently manage download requests for outsourced and encrypted data.

III. MODULES IMPLEMENTATION

3.1. OWNER OF THE DATA:

Register:

Data owners can sign up and log in using legitimate credentials.

Upload File:

The file may be uploaded by the data supplier.

Inspect File:

The data owner has the option to inspect the uploaded file once to determine if it was uploaded successfully or not.

3.2. USER:

Sign up:

Data users can register by providing their details.

Login:

To access the data kept in the MySQL database, the user must first register.

Look for a File:

A user may look for a file by using a keyword. If the file is found, they can examine it and submit a request to the cloud to download it.

Download and obtain the key:

The user can download the file from the cloud provider when their request has been approved.

3.3. SUPREME SUPPLIER

Login:

Using their credentials, the cloud provider can log in.

View Files:

All submitted files are viewable by Cloud.

View Users:

The cloud has the ability to see every user's information in order to provide access to the website.

View Data Providers:

In order to grant authorization for website login, Cloud is able to view all data providers'

obtains a key from the authority and details.

Send Key Make a request for Authority: It is forwarded to them by the cloud.

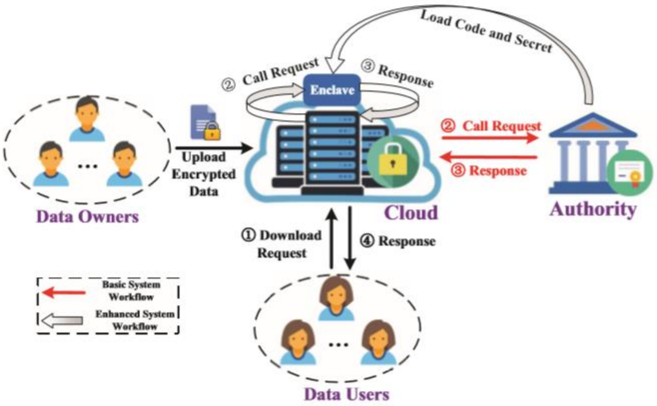
3.4. AUTHORITY:

Log in to see the users and grant permission to people with the authority to log in.

Provide a key to the user:

Users get access to authority.

IV. ARCHITECTURE



V. CONCLUSION

In this work.I showed two dual access control systems and addressed an intriguing and persistent issue with cloud-based data sharing. The suggested systems can withstand DDoS and EDDoS assaults. We assert that the technique for putting the control feature into practice upon It is "transplantable" to download requests for more CP-ABE designs. Our testing results demonstrate that, as compared to the particular underlying CP-ABE building block, the suggested systems have no appreciable computational or communication costs. I take use of the reality that the personal information entered within the enclave cannot be recovered thanks to this enhanced technology. But according to current research, an enclave may be able to give a hostile host a small number of so-fit secrets via memory or related side-channel attacks. access patterns. Hence, the execution paradigm for transparent enclaves is illustrated in. The issue of developing a dual the access control system from a transparent enclaves for cloud data exchange is intriguing. We shall take into consideration pertinent solutions to these challenges in our next study.

VI. REFERENCES

[1]. Aviel D. Rubin, Michael Rushanan, Matthew Green, Ian Miers, Christina Garman, Joseph A. Akinyele, and Matthew W. Pagano. Charm is a framework for quickly iterating over cryptosystem designs. 3(2): 111–128 in Journal of Cryptographic Engineering, 2013.

[2]. Vincent Scarlata, Simon Johnson, Shay Gueron, and Ittai Anati. cutting edge CPU-based attestation and sealing technologies. In Volume 13, Page 7, of Workshop on Hardware and Architectural Support for Security and Privacy (HASP). ACM, 2013, New York, NY, USA.

[3]. Antonis Michalas and Alexandros Bakas. The modern family is a reversible hybrid encryption method built on SGX, symmetric searchable encryption, and attribute-based encryption. Pages472–486in SecureComm 2019.

[4]. Beimel, Amos. Safe protocols for key distribution and secret sharing. PhD dissertation, Technion, Haifa, Israel: Israel Institute of Technology, 1996.

[5]. Amit Sahai, Brent Waters, and John Bethencourt. attribute-based ciphertext-policy encryption. Pages 321–334 of S&P 2007. IEEE, 2007.

[6]. Srinivas Devadas and Victor Costan. The explanation of Intel SGX. 2016(086):1–118, IACR Cryptology ePrint Archive.

[7]. Sergey Gorbunov, Dan Boneh, Dhinakaran Vinayagamurthy, and Ben Fisch. IRON: Intel SGX-based functional encryption. In CCS 2017, pages 765–782, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

[8]. Tatsuaki Okamoto and Eiichiro Fujisaki. Safe combination of symmetric and asymmetric cryptography techniques. Pages 537–554 in Advances in Cryptology–CRYPTO 1999. Springer (1999).

[9]. Brent Waters, Amit Sahai, Omkant Pandey, and Vipul Goyal. For more precise access control over encrypted data, use attribute-based encryption. ACM CCS 2006, 89–98 pages. ACM, 2006.

[10]. Man Ho Allen Au, Jinguang Han, Yi Mu, Jianying Zhou, and Willy Susilo. Enhancing security and privacy in attribute-based decentralized ciphertext-policy encryption. IEEE transactions on security and information forensics, 10(3), 665-678, 2015.

[11]. Cloud computing security: From distributed denial of service (DDoS) to economic denial of sustainability (EDOs), Christofer Hoff. reasonablesurvivability.com/blog/?p=66.

[12]. Doug Jacobson, Mark Tannian, and Joseph Idziorek. connection to unauthorized use of cloud resources. Pages 99–106 in IEEE CLOUD 2012. 2012 IEEE.