JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

TWO-FACTOR AUTHENTICATION FOR DATA STORAGE AND SHARING IN CLOUD-BASED SYSTEM

G Vamsee Krishna #1, K Gayathri Priya #2, P Lakshmi Tejaswini #3, B Nagabala #4, T Prasanth Pavan #5

#1Asst. Professor, #2,3,4,5 B.Tech.., Scholars

Department of Computer Science and Engineering,

QIS College of Engineering and Technology

ABSTRACT

It's no secret that the efficiency and low cost management of cloud-based data storage services have attracted growing attention from the academic and business communities in recent years. To protect the privacy of its customers and the confidentiality of their data, a service provider must adopt a reliable system for storing and exchanging user information via the Internet. Encryption is the most common technology used to prevent unauthorized access to private information. However, the actual need of data management goes beyond what can be met by just encrypting data (e.g., using AES). In addition, it is important to think about access control over download requests so that consumers are not disrupted by Economic Denial of Service (edos) assaults. In this research, we examine the issue of dual access control in the context of cloud storage by developing a system to regulate both data access and download request without compromising on either security or efficiency. In this study, we propose two separate dual access control systems, each tailored to a specific environment. Additionally, the systems' experimental analysis and security findings are detailed.

1. INTRODUCTION

Recently, cloud-based storage services have received a lot of interest from researchers and businesses alike. Because of its numerous advantages, such as easy accessibility and no need for local data storage, it may find widespread usage in Internet-based commercial apps (such as Apple's icould). Many people and businesses increasingly use distant cloud storage rather to invest in expensive upgrades to their on-premises data management infrastructure. While cloud-based storage has many advantages, its widespread adoption may be hampered by consumers' understandable apprehension about the safety of their data in its outsourced form. Many real-world uses for outsourced information need further collaboration. If Alice uses Dropbox, she may easily send her pals a snapshot and invite them to comment. Alice has to establish a sharing link, then send the link to her pals, all without resorting to data encryption. There will be protection against the connection being seen by people who aren't supposed to see it (e.g., those who aren't friends of Alice), but it doesn't mean that it won't be visible to others who are the Dropbox management layer (e.g., only the administrator may access the link). If you want to be sure your data is safe and secure on the cloud, you need encrypt it first since the cloud (which is

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

installed in an open network) cannot be trusted completely. That said, one way to ensure that only authorised cloud users have access to the data is to encrypt it first (using a method like AES) before storing it there.

2. RELATED WORK

In order to exercise granular policy-based control over encrypted data, the literature has proposed ABE [9], [29]. Specific areas of study under ABE include Critical Policy Analysis and Evaluation (CP-ABE) and Keypolicy Analysis and Evaluation (KP-ABE). The former is the primary focus of this study. The CP-ABE embeds the access policy into the ciphertext and links the decryption key to the attribute set. Because of this, CP-ABE may be used for safe cloud storage and exchange of sensitive information 1. The term "dual access control" will be used from now on to describe the ability to regulate both the availability of encrypted data and requests to access it. (when compared to KP-ABE). This is because KP-ABE forces cloud users to incur high storage costs due to the need of associating decryption keys with access policies. Many works have been suggested to use CP-ABE in different contexts since its first publication [9]. These contexts range from multi-authority [10], [17], outsourced [15], [16], [21], and extensible [34] to responsible and traceable [22], [23], [24], [25] CP-ABE.

To defend against edos attacks [11], which are the case of ddos in the cloud context, CP-ABE functioning as a single solution is neither very practical or effective. Multiple defences against the assault have been offered in the literature [12, 33]. On the other hand, Xue et al. [38] claimed that the aforementioned works did not adequately protect against edos attacks at the algorithmic (or protocol) level, and therefore provided a way to securing cloud data sharing. But [38] has two major flaws that make it undesirable. To begin with, the owner of the data must increase the computational load by generating a series of challenge ciphertexts to use in an effort to thwart the assault.

Second, a data user must decode one of the challenge ciphertexts as a test, which involves a large number of costly operations (e.g., pairing). This situation increases the computational complexity for both parties and necessitates a large amount of network capacity for the transmission of ciphertexts. The vast cloud-based computing resources are underutilised in [38]. In this research, we propose a novel approach that can withstand an edos assault with little resources used on computing and communication. In a recent paper, Antonis Michalas [20] suggested a data sharing protocol that combines symmetric searchable encryption with ABE, enabling users to directly search through encrypted data.

Key revocation in ABE is achieved by having a revocation authority hosted by SGX.

Later in [20], Bakas and Michalas [3] suggested a hybrid encryption technique, narrowing the difficulty of multi-user data sharing to that of a single-user.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

In specifically, an SGX enclave encrypted using an ABE technique stores the symmetric key required for data encryption. It uses the SGX enclave to solve the revocation issue in the context of ABE, much like [20]. In this study, we use SGX to provide download request control (to avert ddos/edos assaults). Both our goal and methodology are distinct from the methods described in [3], [20].

3. SYSTEM ANALYSIS

A malicious service user could launch the denial-of-service (dos)/distributed denial-of-service (ddos) attacks to consume the resource of cloud storage service server, making it unable to respond to service requests from honest users, because a (public) cloud may not have any control over download request (namely,a service user may send an unlimited number of download requests to cloud server). Because of this, the "pay as you go" approach may cause economic disruption owing to increased resource use. As the assaults increase in size, the prices for consumers of cloud services will skyrocket. This kind of assault, known as Economic Denial of Sustainability (edos), is directed against the financial resources of a cloud adopter. In addition to financial loss, the very nature of unrestricted downloads may allow network intruders to spy on your private, encrypted download data (e.g., file size). Consequently, it is necessary to have authority over requests to download outsourced (encrypted) data. Consequently, it is necessary to have authority over requests to download outsourced (encrypted) data.

Disadvantages

Client-side user deduplication prevents updating the file's tag. The dynamic Ownerships would be useless if this happened. Briefly put, the current dynamic Ownerships cannot be applied to a multi-user setting. Worries regarding data loss emerge whenever data is changed. Data deduplication systems are defined by the fact that they save data in a manner different from how it was originally created. Therefore, people worry about the security of their information. By using cryptographic hash algorithms, duplicate data may be spotted and removed. It is considered a collision if two separate bits of information produce the same hash value. It's important to note that different hash functions have different collision probabilities but that they're never zero.,

Proposed System:

To address these two issues, this research proposes a novel approach we call dual access control. Attribute-based encryption (ABE) [9] is one of the potential possibilities that permits the confidentiality of outsourced data and fine-grained control over the outsourced data, making it an attractive option for securing data in cloud-based storage services. Ciphertext-Policy ABE (CP-ABE) [5] in particular offers an efficient means of data encryption in such a manner that access rules, defining the access privilege of prospective data receivers, may be specified over encrypted data. It is important to note that in this research, we take into account the possibility of

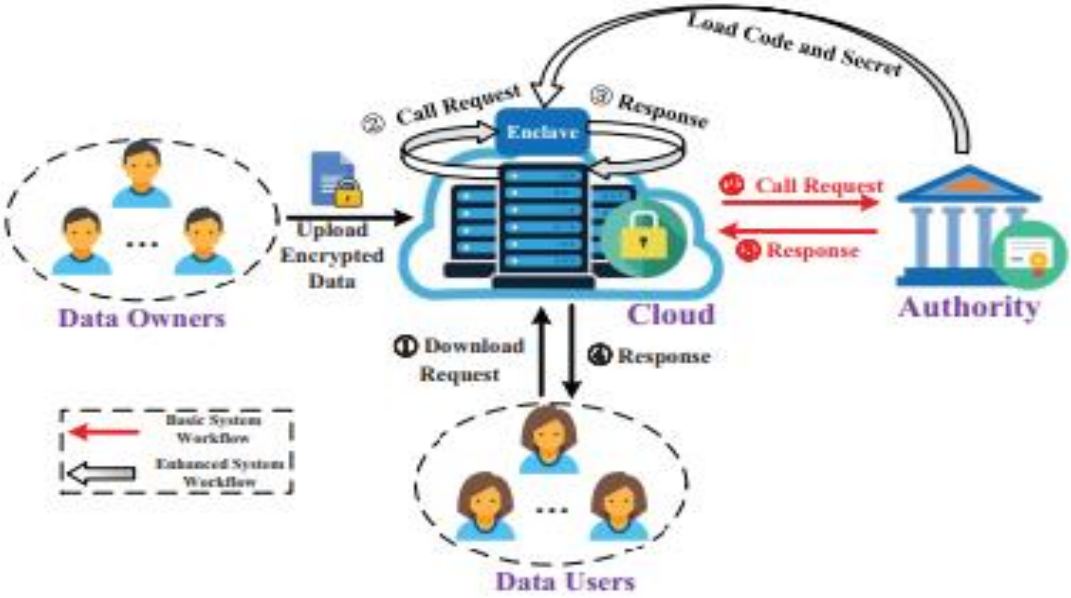
ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

using CP-ABE in our process. While the CP-ABE method is useful, it is not enough on its own to develop a sophisticated system that can regulate both data access and download requests.

Advantages:-

This system benefits from two features. As a first use case, it may be implemented to avoid the need to distribute decryption keys when sharing sensitive information with users by instead relying on a set of predefined access controls. Second, it protects sensitive information using the industry-recognized definition of semantic security, rather to the less stringent security measures used by other systems. More than that, we proposed a mechanism for transforming a ciphertext over one access policy into ciphertexts of the same plaintext but under different access policies, all without disclosing the underlying plaintext.

System architecture of attribute-based storage with secure Deduplication.:



The RSA Algorithm

RSA is a popular method for digital encryption and decryption on today's computers. It's a kind of cryptographic method known as "asymmetric." In this case, the keys are asymmetric, which means they are not identical. Since one of these keys may be made public, this kind of encryption goes by the name "public key cryptography." The second key should remain secret. Reasoning behind it is how difficult it is to identify the factors of an integer (the factoring problem). RSA was coined in 1978 by researchers Ron Rivest, Adi Shamir, and Leonard Adleman. The public key in RSA is the product of two huge prime numbers plus an additional

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

value that is also made public. The primary factors are classified information. Currently-publicized techniques let anybody to use the public key to encrypt a message, but only someone with knowledge of the prime factors can realistically decode the message if the public key is big enough.

Encryption Algoritm:-

With the use of encryption, sensitive data may be concealed from prying eyes (such as a password). To do this, a code or cypher is used. Encryption refers to the process of hiding information.

Decryption Algorithm:-

The process of decryption converts encrypted data back into readable form. What you see before you is the unencrypted version. Cryptanalysis is the scientific study of encryption. If the code is straightforward, deciphering it may be done manually. Computer key search is required for complex cyphers. The study of how hard it is to crack a cypher is what computer scientists and mathematicians call "decryption."

4. IMPLEMENTATION

Data Owner:

The first step in this section is for the data owner to sign up for an account on the cloud server and be granted appropriate permissions. If the cloud service provider gives the go-ahead, the data owner will encrypt and upload the file to the cloud server, at which point the data owner will request the content key and the master secret key from the authority for the file he uploaded and discovers Find deduplication. If users want to be able to search for and download newly uploaded files, the data owner must first grant them access to do so.

Cloud Server

The cloud storage service is administered by the cloud server. Owners of sensitive data encrypt their files before uploading them to the cloud, where they may be accessed by cloud End users. Users will make a formal request for the MSK master secret key and the content key in order to get access to the shared data files. Plus, the authorization will come from the cloud. , and may see who has accessed the files and who has been making transactions on them.

Authority

The user requests a secret key and a content key, both of which are generated by the authority.

The content key and master secret key for a given file are constructed using the information of the file's owner, allowing authority access to the file.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

End User

Users need to sign up and log in before they may access their cloud-stored documents. The cloud service gives the user the ability to confirm their registration. In order to access the file, the user must first request the MSK master secret key and content key. If the data owner grants access, only then may the user download and search the file.

5. CONCLUSION

We introduced two dual-access control solutions to solve a compelling and enduring issue in cloud-based data sharing. Protected against dos and edos assaults are the suggested systems. We claim that the method utilised to provide control on demand may be "transplanted" to different CP-ABE architectures. The experimental findings presented here demonstrate that the suggested systems incur little computational and communication cost (compared to its underlying CP-ABE building block).

To further strengthen our system, we take use of the fact that the enclave's secure storage prevents any retrieved data from being compromised.

More recent research, however, demonstrates that an enclave may reveal part of its secret(s) to a hostile host through memory access patterns [37] or other similar side-channel attacks [14, 30]. Therefore, in [35], we provide the paradigm of transparent enclave execution. It's a fascinating challenge to design a two-factor authentication solution for cloud data sharing that uses a transparent enclave. We will investigate the corresponding answer to this issue in our next papers.

REFERENCES

[1] Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin. The Charm framework is a tool for quickly developing cryptographic protocols.

[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Using cutting-edge CPU-based attestation and sealing technologies. In the Thirteenth Annual Workshop on Hardware and Architectural Support for Privacy and Security (HASP),

[3] Attributed to Alexandros Bakas and Antonis Michalas Attribute-based encryption, symmetric searchable encryption, and SGX all come together in an up-to-date family of hybrid encryption methods. Published in 2019 at securecomm, pp 472-486.

[4] Amos Beimel. Safe methods of passing down keys and disclosing secrets. Theses and dissertations (Ph.D.) Submitted to and accepted for publication by the Graduate School of Engineering and Computer Science, Technion, Haifa, Israel 1996.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

[5] John Bethencourt, Amit Sahai, and brentwaters. Data security using ciphertext policy attributes. Referenced in S&P 2007, pp. 321-334. IEEE, \s2007.

[6] are Victor Costan and Srinivas Devadas. Understanding Intel's Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov

[7]. Functional encryption with Intel SGX: IRON. Computer and Communications Security: Proceedings of the 2017 ACM SIGSAC Conference,

[8] The work of Eiichiro Fujisaki and Tatsuaki Okamoto Combining symmetric and asymmetric encryption methods safely.

[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Fine-grained encryption access control depending on data attributes.

10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Attribute-based encryption with a decentralised ciphertext strategy for enhanced privacy and security.

[11] This is Christofer Hoff,. From distributed denial of service (ddos) to enhanced distributed denial of service (edos) in the cloud (economic denial of sustainability).

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson. Tracking down the source of cloud service abuse..Simon Johnson, Vinny Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen

[13]. Epid provisioning and attestation services are an extension of the Intel R software guard14 Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado.

[14] Using branch shadowing to infer state transitions across sgx enclaves. 2016 Proceedings of the 26th USENIX Security Symposium, USENIX Security, pages 16-18.

[15] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han Ksfoabe is a service that encrypts data in the cloud based on keywords you provide, and it uses outsourced attribute-based encryption.

[16] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Attribute-based encryption with full verifiability of decryption services provided by third parties. DOI:

[17] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong. Tmacs is a secure and auditable threshold multi-authority access control

[18] Ben Lynn et al. This is the cryptographic pairing library. Online at [March 27, 2013]: crypto Authors: Frank mckeen, Ilya Alexandrovich, Alex Berenzon, Carlos V. Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Savagaonkar.

[19] New software paradigm and instructions for isolated processing. At page 10 of HASP@ISCA 2013.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

[20] I'm referencing Antonis Michalas here Master of the shares: adaptable data sharing using a hybrid of attribute-based and searchable encryption.

[21] We thank Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei for their contributions to this article. Attribute-based encryption that can be audited in real time for use in the cloud's access management system.

[22] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and lifeiwei White-box \straceable The most efficient methods for detecting leaks of cloud storage account passwords using CP-ABE..

[23] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and Xiaodong Lin [23]. A large-universe ciphertext-policy attribute-based cypher with full white-box auditability.

[24] Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei Attribute-based cloud-based encryption managed by a responsible authority, audited in public.

[25] Xiaodong Lin, Lifei Wei, Zhenfu Cao, Jianting Ning, and Xiaolei Dong [25]. Flexible characteristics are supported by the white-box ciphertext-policy encryption system.

[26] Researchers Olga Ohrimenko, Felix Schuster, and c'edric Fournet, Manuel Costa, Kapil Vaswani, Aastha Mehta, and Sebastian Nowozin. Using trustworthy hardware and many parties' ignorance, we can train a machine to become more efficient.

[27] Based on the work of Ashay Rane, Calvin Lin, and Mohit Tiwari Digital backdoors are sealed using Raccoon's masked code execution.

[28] Computer and Communications Security: 9th ACM Conference Proceedings (pp. 98-107) ACM, 2002.

[29] Thanks to Amit Sahai and Brent Waters encrypted using a key based on a fuzzy identification.

[30] A group of researchers led by Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado T-sgx: Protecting enclave software against assaults through regulated channels.

[31] Victor Shoup. An ISO public key encryption standard proposal (version 2.1). The 112th issue of the IACR's electronic printing archive was released in 2001.

[32] Gaurav Somani, Manoj Singh Gaur, and Dheeraj Sanghi. Everyone is vulnerable to cloud-based distributed denial of service (ddos) attacks.

[33] Mohammed H. Sqalli, Fahd Al-Haidari, and Khaled Salah. To protect cloud infrastructure from edos threats, we developed Edosshield, a two-pronged approach to defence

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

[34] Willy Susilo, Peng Jiang, Fuchun Guo, Guomin Yang, Yong Yu, and Yi Mu. Eacsip stands for "Extendable Access Control System with Integrity Protection," and it is designed to make online teamwork more secure

[35] Elaine Shi, Ari Juels, and Florian Tramer; Fan Zhang; Huang Lin; Jean-Pierre Hubaux; and Elaine Shi. Knowledge may be proven and sold in airtight, see-through enclosures.

[36] Waters, Brent. To encrypt data using a ciphertext policy and its attributes, see: A realisable that expresses itself, works efficiently, and is provably safe.

[37] A trio consisting of Yuanzhong Xu, Weidong Cui, and Marcus Peinado. Controlled-channel attacks are deterministic side channels that may be used against untrusted operating systems

[38] They are Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. Encrypted cloud storage that combines control from data owners and the cloud. Information Forensics and Security: Yonghong Tian, Song Guo, Dapeng Oliver Wu, and Shui Yu