International Journal on Applications in Engineering and Technology
Volume 9 : Issue 2 : April 2023, pp 27 -31 www.aetsjournal.com ISSN (Online) : 2455 - 0523

DUAL ACCESS CONTROL FOR CLOUD-BASED DATA SHARING AND STORAGE SECURITY

M.THANGAVEL , BHUVANESHWARI G

***Abstract*—** Due to its effective and affordable management, cloud-based data storage has recently attracted growing interest from both academia and industry. Since services are delivered over 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 fully met by merely 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. In this essay.In the context of cloud-based storage, we take into account dual access control in the sense that we create a control mechanism over both data access and download requests without sacrificing security and effectiveness. This paper 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 analysis. Security Dual Access Control for Data Sharingand Storage in the Cloud

Keywords: Rescue bag, Rescue techniques, Borewell rescue, Child safety

I. INTRODUCTION

Due to its extensive list of advantages, which includes access freedom and the lack of local data management, in many Internet-based commercial products (such as Apple iCould). 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.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. Here, conventional public key encryption is used (e.g., Paillier Encryption),That cannot be used since it requires the encryptor to know who the data recipient is beforehand. It is therefore desirable to provide a policy-based encryption method over the outsourced photographs, such that Alice may use the mechanism to set access policies over the encrypted photos to ensure that only a select group of authorized people can access the photos. A frequent exploit known as a resource-exhaustion attack exists in cloud-based storage services. A malicious service user may launch denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks to consume the resources of the cloud storage service server in order to disrupt the cloud service.

Because a (public) cloud may not have any control over download requests (i.e., a service user may send an unlimited number of download requests to

M.Thangavel , Professor , Department of Computer Applications , Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.
(Email : thangavelpamu@gmail.com)

Bhuvaneshwari G, PG Scholar , Department of Computer Applications, Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.
(Email : bhuvanagunasekar1999@gmail.com)

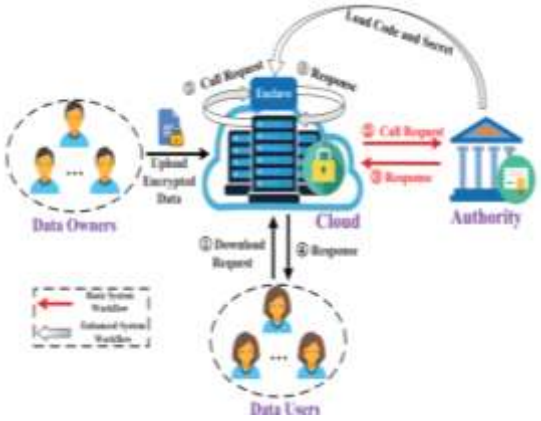
the cloud server).Could not fulfill the service needs of sincere customers. Due to increased resource demand, the "pay-as-you-go" model runs the risk of upsetting the economy. Users of cloud services will experience a sharp increase in costs as the attacks intensify. This is referred to as an Economic Denial of Sustainability (EDoS) assault [32, 33], which attacks the financial resources of cloud adopters. Beyond monetary loss, unrestricted downloads itself could provide network attackers access to encrypted download data, which could result in some potential information leaking (e.g., file size). As a result, it is also necessary to have an effective control on download requests for external (encrypted) data

II. LITERATURE SURVEY

By showcasing two effective and safe cloud-based dual access control systems1 in various scenarios, we answer the aforementioned issue in the positive. We briefly outline the technical road map below with the intention of offering an effective dual access control method. We begin with a CP-ABE system[36], which is viewed as one of the building blocks, to ensure the confidentiality of outsourced data without sacrificing policy-based access control. Ontop of the CP-ABE system, we also apply an efficient control over data consumers' download requests. We come up with a fresh strategy to do away with the practice of "testing" encrypted text. We specifically enable the creation of download requests by data users. Upon receiving the download request, with assistance from the enclave or the authority,A cloud server called Intel SGX is able to determine whether a user of the data is permitted to view it. The cloud server just learns whether the user is authorized; no other information is disclosed. On the basis of the aforementioned process, the cloud keeps control of the download request. The systems we suggest have the following distinctive characteristics:

1. Data privacy when it is outsourced. The outsourced data is encrypted in our suggested systems before being uploaded to the cloud. Without authorizedaccess, nobody can access them.
2. Data sharing anonymity. Given an outsourced data, a cloud server cannot determine the data owner, guaranteeing the owner's anonymity in data exchange and storage.
3. Strict access control for data that has been outsourced and/or encrypted. After the data is uploaded to the cloud, the data owner still maintains access control over his encrypted data. In particular, a data owner can encrypt the data that was outsourced under a defined access policy so that only a select number of authorized users who comply with the access policy may access the data.
4. Command over the resistance to EDoS assaults and anonymous download requests. Any system user may send a download request, but a cloud server has control over it and can set the request to be anonymous. We claim that our systems are protected against EDoS attacks thanks to the management over download requests.
5. Extremely effective. The CP-ABE system is the foundation for our suggested systems [36]. When compared to [36]

ARCHITECTURE

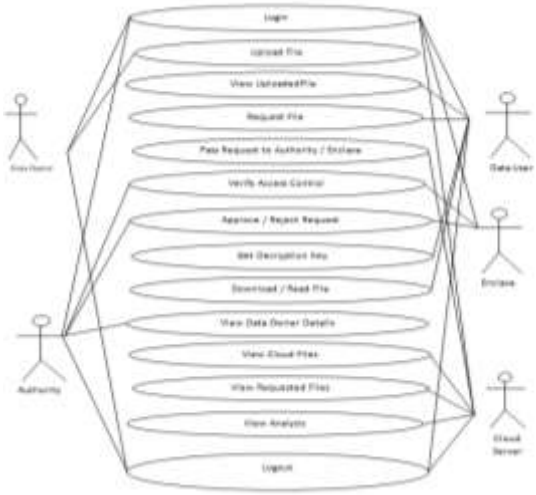


III. METHODOLOGY

To protect the data, we use a hybrid system, which combines the effectiveness of symmetric-key systems with the practicality of public-key systems. Particularly, the Key/Data Encapsulation Mechanism (KEM/DEM) option is used for both of the proposed dual access control systems [31]. An effective symmetric-key encryption strategy is used to encrypt the message, as opposed to the

ineffective public-key scheme (CP-ABE), which solely employed to encrypt and decrypt a brief key value.We use the following methods to meet the security criteria of anonymous data sharing, data confidentiality, and access control on shared data:CP-ABE technique as the fundamental cornerstone. Because of its effectiveness, we specifically present the construction based on the CP-ABE scheme in [36]. and sophisticated design.

1) Use case diagram



IV. EXISTING SYSTEM

- Antonis Michalas proposed a data sharing protocol that combines symmetric searchable encryption and ABE, which allows users to directly search over encrypted data. To implement the functionality of key revocation in ABE, the protocol utilizes SGX to host a revocation authority.
- Bakas and Michalas later extended the protocol and proposed a hybrid encryption scheme that reduces the problem of multi-user data sharing to that of a single-user. In particular, the symmetric key used for data encryption is stored in an SGX enclave, which is encrypted with an ABE scheme. It deals with the revocation problem in the context of ABE by employing the SGX enclave.

Disadvantages

- The worry of security breach over outsourced data may be one of the main obstacles hindering Internet users from widely using cloud-based storage service.
- Apart from economic loss, unlimited download itself could open a window for network attackers to observe the encrypted download data that may lead to some potential information leakage (e.g., file size).
- In the existing system the data owner is required to generate a set of challenge ciphertexts in order to resist the attack, which enhances its computational burden. Second, a data user is required to decrypt one of the challenge ciphertexts as a test, which costs a plenty of expensive operations (e.g., pairing).
- The computational complexity of both parties is inevitably increased and meanwhile, high network bandwidth is required for the delivery of ciphertexts. The considerable computational power of cloud is not fully considered

V. PROPOSED SYSTEM

- In this project, we propose a new mechanism, dubbed dual access control, to tackle the existing system problem. To guarantee the confidentiality of outsourced data without loss of policybased access control, we start with a CP-ABE system, which is seen as one of the building blocks. We further employ an effective control over data users' download request on the top of the CP-ABE system. We design a new approach to avoid using the technique of "testing" ciphertext. Specifically, we allow data user to generate a download request. Upon receiving the download request, with help of the authority or the enclave of Intel SGX, a cloud server is able to check if the data user is authorized to gain access to the data. No other information is revealed to the cloud server except the knowledge of whether the user is authorized. Based on the above mechanism, the cloud maintains the control of the download request.
- In our proposed systems, the outsourced data is encrypted prior to being uploaded to cloud. No one can access them without valid access rights. Given an outsourced data, cloud server cannot identify data owner, so that the anonymity of owner can be guaranteed in data storage and sharing.Data owner keeps controlling his encrypted data via access

policy after uploading the data to cloud. In particular, a data owner can encrypt his outsourced data under a specified access policy such that only a group of authorized data users, matching the access policy, can access the data. A cloud server is able to control the download request issued by any system user, where the download request can set to be anonymous. With the control over download request, we state that our systems are resistant to EDoS attacks.

Advantages

- ❖ Confidentiality of outsourced data
- ❖ Anonymity of data sharing
- ❖ Fine-grained access control over outsourced (encrypted) data
- ❖ Control over anonymous download request and EDoS attacks resistance
- ❖ High efficiency

VI. IMPLEMENTATION AND EXECUTION

The implementation of this application is split into following modules.

- *Data Owner*
- *Data User*
- Authority
- Cloud Server
- Enclave

1) 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.

2) 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.

3) Authority:

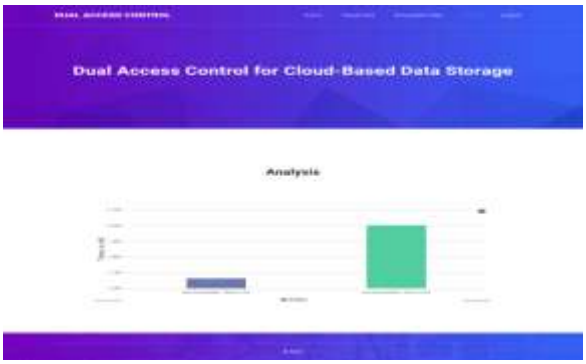
Authority is responsible for initializing system parameters and data user registration. Also, it handles the call request from the cloud in the first proposed construction.

4) 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.

5) Enclave:

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



VII. 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 toDDoS/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(compared to its underlying CP-ABE building block).

VIII. FUTURE ENHANCEMENTS

In our enhanced system, we employ the fact that thesecret information loaded into the enclave cannot be extracted.However, recent work shows that enclave may leaksome amounts of its secret(s) to a malicious host through thememory access patterns or other related side-channelattacks. The model of transparent enclave execution ishence introduced. Constructing a dual access controlsystem for cloud data sharing from transparent enclave isan interesting problem. In our future work, we will considerthe corresponding solution to the problem.

IX. REFERENCES

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew WPagano, Michael Rushanan, Matthew Green, and Aviel D Rubin.Charm: a framework for rapidly prototyping cryptosystems. Journalof Cryptographic Engineering, 3(2):111–128, 2013.

[2] IttaiAnati, Shay Gueron, Simon Johnson, and Vincent Scarlata.Innovative technology for cpu based attestation and sealing. InWorkshop on hardware and architectural support for security and privacy(HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] AlexandrosBakas and AntonisMichalas. Modern family: A revocablehybrid encryption scheme based on attribute-based encryption,symmetric searchable encryption and SGX. In SecureComm2019, pages 472–486, 2019.

[4] Amos Beimel. Secure schemes for secret sharing and key distribution.PhD thesis, PhD thesis, Israel Institute of Technology, Technion,Haifa, Israel, 1996.

[5] John Bethencourt, AmitSahai, and BrentWaters.Ciphertext-policyattribute-based encryption. In S&P 2007, pages 321–334. IEEE,2007.

[6] Victor Costan and SrinivasDevadas. Intel sgx explained. IACRCryptology ePrint Archive, 2016(086):1–118, 2016.

[7] Ben Fisch, DhinakaranVinayagamurthy, Dan Boneh, and SergeyGorbunov. IRON: functional encryption using intel SGX. InProceedings of the 2017 ACM SIGSAC Conference on Computer andCommunications Security, CCS 2017, pages 765–782, 2017.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration ofasymmetric and symmetric encryption schemes. In Advances inCryptology-CRYPTO 1999, pages 537–554. Springer, 1999.

[9] VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters.Attribute-based encryption for fine-grained access control of encrypteddata. In ACM CCS 2006, pages 89–98. ACM, 2006.

[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and ManHo Allen Au. Improving privacy and security in decentralizedciphertext-policy attribute-based encryption. IEEE transactions oninformation forensics and security, 10(3):665–678, 2015.

[11] Christofer Hoff. Cloud computing security: From ddos (distributeddenial of service) to edos (economic denial of sustainability).http://www. rationalsurvivability.com /blog/?p=66.

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson.Attributionof fraudulent resource consumption in the cloud. In IEEE CLOUD2012, pages 99–106. IEEE, 2012.

[13] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. Intel R software guard extensions: Epid provisioningand attestation services. White Paper, 1:1–10, 2016.

[14] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, HyesoonKim, and Marcus Peinado. Inferring fine-grained control flowinside sgx enclaves with branch shadowing. In 26th USENIXSecurity Symposium, USENIX Security, pages 16–18, 2017.

[15] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe:outsourced attribute-based encryption with keyword searchfunction for cloud storage. IEEE Transactions on Services Computing,10(5):715–725, 2017.

[16] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Fullverifiability for outsourced decryption in attribute basedencryption. IEEE Transactions on Services Computing, DOI:10.1109/TSC.2017.2710190, 2017.

[17] Wei Li, KaipingXue, YingjieXue, and Jianan Hong. Tmacs:A robust and verifiable threshold multi-authority access controlsystem in public cloud storage. IEEE Transactions on parallel anddistributed systems, 27(5):1484–1496, 2016.

[18] Ben Lynn et al. The pairing-based cryptography library. Internet:crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.

[19] Frank McKeen, IlyaAlexandrovich, Alex Berenzon, Carlos V.Rozas, HishamShafi, VedvyasShanbhogue, and Uday R. Savagaonkar.Innovative instructions and software model for isolatedexecution. In HASP@ISCA 2013, page 10, 2013.

[20] AntonisMichalas. The lord of the shares: combining attributebasedencryption and searchable encryption for flexible data sharing.In SAC 2019, pages 146–155, 2019.

[21] JiantingNing, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma,and Lifei Wei. Auditable -time outsourced attribute-based encryptionfor access control in cloud computing. IEEE Transactionson Information Forensics and Security, 13(1):94–105, 2018.

[22] JiantingNing, Zhenfu Cao, Xiaolei Dong, and LifeiWei. White-boxtraceable CP-ABE for cloud storage service: How to catch peopleleaking their access credentials effectively. IEEE Transactions onDependable and Secure Computing, 15(5):883–897, 2018.

[23] JiantingNing, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and XiaodongLin. Large universe ciphertext-policy attribute-based encryptionwith white-box traceability. In Computer Security-ESORICS 2014,pages 55–72. Springer, 2014.

[24] JiantingNing, Xiaolei Dong, Zhenfu Cao, and Lifei Wei.Accountableauthority ciphertext-policy attribute-based encryptionwith white-box traceability and public auditing in the cloud. InComputer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[25] JiantingNing, Xiaolei Dong, Zhenfu Cao, Lifei Wei, and XiaodongLin. White-box traceable ciphertext-policy attribute-based encryptionsupporting flexible attributes. IEEE Transactions on InformationForensics and Security, 10(6):1274–1288, 2015.