International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 4th Aug 2021. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-08

DOI: 10.48047/IJIEMR/V10/I08/04

Title EFFICIENT SECURITY OF CLOUD BASED DATA BY DUAL ACCESS VERIFICATION MECHANISM

Volume 10, Issue 08, Pages: 23-28

Paper Authors
Mr M. MAHARSHI

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

EFFICIENT SECURITY OF CLOUD BASED DATA BY DUAL ACCESS VERIFICATION MECHANISM

Mr M. MAHARSHI, VIth semester, Dept of MCA, SVIM - Sree Vidyanikethan Institute of Management, Tirupati. Email.id maharshimanubrolu23@gmail.com

ABSTRACT

Due to its effective and low-cost administration, cloud-based data storage services have piqued the interest of both academia and business in recent years. Service providers must utilise secure data storage and sharing mechanisms to protect data confidentiality and service user privacy since they deliver services via an open network. Encryption is the most frequently used way for protecting sensitive data from being hacked. However, just encrypting data (for example, using AES) is insufficient to meet the actual need for data management. Furthermore, an effective access control on download requests must be addressed in order to prevent Economic Denial of Service (EDoS) attacks from preventing users from using the service. We examine dual access control in the context of cloud-based storage in this work, in the sense that we propose a control mechanism that can handle both data access and download requests without sacrificing security or efficiency. In this work, two dual access control systems are built, each for a different intended context. The systems' security and experimental analysis are also discussed.

KEYWORDS ***Cloud-based data sharing, access control, cloud storage service, Intel SGX, attribute-based encryption.***

I INRODUCTION

Cloud-based storage services have gotten a lot of interest from academics and industry in recent decades. It might be widely utilised in a variety of Internet-based commercial applications (e.g., Apple iCould) due to a lengthy number of advantages, including access flexibility and the elimination of local data administration. Nowadays, an increasing number of people and businesses want to outsource their data to a remote cloud in order to save money on modernising their local data management facilities/devices. The fear of a security breach involving outsourced data, on the other hand, may be one of the primary barriers preventing Internet users from making widespread use of cloud-based storage services. Outsourced data may need to be shared with others in a variety of situations. Alice, a Dropbox user, may, for example, exchange photographs with her pals.

Without utilising data encryption, Alice must create a sharing link and then share it

with others before sharing the photographs. The sharing link may be displayed inside the Dropbox management level, although ensuring some level of access restriction for unauthorised users (e.g., those who are not Alice's friends) (e.g., administrator could reach the link). Because the cloud (which is based on an open network) cannot be completely trusted, it is generally advised that data be encrypted before being uploaded to the cloud to protect data security and privacy. One of the relevant options is to apply an encryption technique (e.g., AES) on the outsourced data before uploading to the cloud, so that only a specific cloud user (with a valid decryption key) may decode the data. A simple approach to prevent shared photographs from being viewed by system "insiders" is to identify a set of approved data users before encrypting the data. Nonetheless, Alice may have no clue who the photo receivers/users will be in such situations.

It's possible that Alice just knows about picture receivers' characteristics. Traditional public key encryption (e.g., Paillier Encryption) cannot be used in this scenario because it needs the encryptor to know who the data recipient is ahead of time. It is also desired to provide a policy-based encryption method over the outsourced photographs, so that Alice may use the mechanism to set access policies over the encrypted photos, ensuring that only a limited number of authorised people have access to the photos.

II RELATED WORK

TMACS is a threshold multi-authority CP-ABE access control system for public cloud storage that allows several authorities to administer a consistent attribute set together. In TMACS, the master key can be shared across many authorities via (t; n) threshold secret sharing, and a lawful user can create their or her secret key by interacting with any t authority. The findings of the security and performance analyses demonstrate that TMACS is not only verifiably safe when fewer than t authorities are compromised, but also resilient while all t authorities are active. Furthermore, create a hybrid scheme that fulfils the situation of characteristics originating from multiple authorities while also providing security and system-level resiliency [1] by efficiently integrating the standard multi-authority scheme with TMACS. The technique for dealing with attribute revocation in multi-authority data access control for cloud storage systems was proposed in a security study of attribute revocation in multi-authority data access control for cloud storage systems. The work uses a bidirectional re-encryption approach in ciphertext updating, resulting in a security vulnerability, according to analysis and research. Also demonstrated is that a revoked user may decode new ciphertexts that are stated to require the new version secret keys to decipher [2].

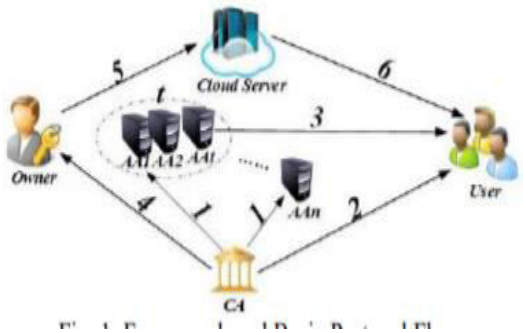
Because it offers data owners more direct control over access regulations, Ciphertext-Policy Attribute-based Encryption (CP-ABE) is recognised as one of the most suited technologies for data access control in cloud storage. Due to the attribute revocation problem, it is difficult to directly adapt existing CP-ABE methods to data access control for cloud

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

storage systems. For this, we developed an expressive, efficient, and reversible data access control method for multi-authority cloud storage systems, in which several authorities coexist and each authority can issue attributes independently. It presented a revocable multiauthority CP-ABE approach and used it to construct the data access control scheme [4]. Due to the frequent change of membership, sharing data in a multi-owner way while protecting data and identity privacy from an untrusted cloud is a difficult challenge. For this, he offers Mona, a secure multiowner data sharing system for dynamic cloud groups. Any cloud user can anonymously exchange data with others by utilising group signature and dynamic broadcast encryption methods. In the meanwhile, the scheme's storage overhead and encryption calculation cost remain unaffected by the number of revoked users [5].

III METHEDOLOGY

Figure 1 depicts the TMACS scheme structure. In order to obtain the necessary identity and certificate in TMACS, AAs must first register with the CA (aid, aid.cert). The AAs will thereafter be involved in the system's creation, aiding CA with the finalisation of system parameters. CA accepts user registration and provides each lawful user a certificate (uid, uid.cert). The user can use the certificate to negotiate with any of the t AAs one by one to obtain his or her secret key (SK). CA can provide the public key (PK) to owners who wish to share their data in the cloud. The owner can then encrypt his or her data according to a set of access policies and upload the ciphertext (CT) to the cloud server. The ciphertexts (CT) that the user is interested in can be freely downloaded from the cloud server. However, he/she won't be able to decode the ciphertext (CT) unless he/she has the appropriate characteristics.



Protocol flow

N Attribute Authorities, Cloud Server, Data Owners, and Data Consumers are the four categories of entities in this system. A user can be both a Data Owner and Data Consumer at the same time. Because some attributes partially include users' personally identifying information, authorities are considered to have significant computing abilities and are controlled by government agencies. Because the entire attribute collection is split into N discrete sets and managed by each authority, each authority only knows about a fraction of the attributes. The entity that intends to outsource encrypted data files to Cloud Servers is known as a Data Owner. The Cloud Server, which is presumed to have sufficient storage space, just stores them. Data Consumers who are new to the system seek private keys from all authorities, and they have no idea which authorities control certain characteristics. When Data Consumers ask the authorities for their private keys, the authorities create a matching private key and deliver it to them. All Data Consumers

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

can download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can perform the privilege p action.

If and only if the user's credentials are confirmed through the privilege tree Tp, the server is delegated to perform an operation p. [3]. The author proposes a new revocable multi-authority CP-ABE protocol based on Lewko and Waters' single-authority CPABE protocol. That is, the author makes it revocable and extends it to a multi-authority scenario. The authors employ techniques from Chase's multi-authority CP-ABE protocol to link secret keys issued by various authorities for the same user and avoid collusion. The author divides the authority's capabilities into two types: a global certificate authority (CA) and numerous attribute authorities (AAs). The CA is in charge of setting up the system and accepting user and AA registrations. Each user is given a global user identity uid, and each attribute authority is given a global authority identity aid. Secret keys generated by various AAs for the same uid can be linked together for decryption since the uid is globally unique in the system. Furthermore, because each AA is linked to an assistance, each attribute is distinct, even if multiple AAs issue the same attribute. Instead of utilising the system's unique public key to encrypt data, the author's approach requires all attribute authorities to produce their own public keys and utilises them to encrypt data along with the global public parameters to address the security issue in MultiAuthority Attribute Based Encryption.

This prohibits the ciphertexts from being decrypted by the certificate authority in the scheme. The author gives a version number to each attribute to address the attribute revocation problem. To enhance performance, the author uses the proxy reencryption technique to delegate the ciphertext update burden to the server, allowing the newly joined user to decode previously published material encrypted with the prior public keys if they contain appropriate characteristics [4]. The authors plan to integrate group signature and dynamic broadcast encryption approaches to provide safe data sharing for dynamic groups in the cloud. Users may utilise cloud resources anonymously thanks to this group signature system, and data owners can safely share their data files with others, including new users, thanks to the dynamic broadcast encryption technology.

IV SYSTEM DESIGN

ARCHITECTURE DIAGRAM

Our dual access control solutions for cloud data sharing include the following designs. The systems are made up of the following components:

• The authority is in charge of setting up system specifications and registering data users. In the initial suggested architecture, it also processes the call request from the cloud.

• The data owner owns the data and want to move it to the cloud. Data owners, in particular, wish to share their data (only) with people who meet specific criteria (e.g., professors or associate professors). Once their data has been transferred to the cloud, they will be disconnected.

• The data user want to download and decode the cloud-based encrypted data. Those who have been granted access can download the encrypted file and decode it to obtain the plaintext.

• Cloud storage is handy for both data owners and data users. It specifically saves data users' outsourced data and responds to data users' download requests.

• Enclave is in charge of cloud-based call requests (used in the second system). The following is a description of the workflow. Data owners encrypt their data according to their own access restrictions and upload the encrypted data to the cloud. By sending a download request to the cloud, authorised data users can download the shared data.

When the cloud receives a download request from an authorised data user, it conducts the following.

(a) For our basic system, the cloud makes a call request to the authority in charge of the cloud and the authority in charge of the authority in charge of the authority in charge of the authority in charge of the authority in charge of the authority in charge

The cloud delivers a response to the data user after receiving a response from the authority between the cloud and the authority in 1.

(b) For our improved system, the cloud initiates a call to the enclave above it. The cloud responds to the data user after getting a response from the enclave.

V CONCLUSION

We proposed two dual access control methods to solve an intriguing and long-standing challenge in cloud-based data sharing. DDoS/EDoS assaults are not a problem for the suggested solutions. The approach utilised to accomplish the control on download request feature is “transplantable” to different CP-ABE designs, according to the authors. The suggested systems do not incur any substantial computational or communication overhead, according to our results (compared to its underlying CP-ABE building block). We use the fact that the private information placed into the enclave cannot be retrieved in our improved system. Recent research suggests, however, that enclave may leak some of its secret(s) to a hostile host via memory access patterns or other side-channel assaults. As a result, the transparent enclave execution model is introduced. Constructing a dual access control system from a transparent enclave for cloud data sharing is an intriguing challenge. We will consider the problem's corresponding solution in our future work.

VI REFERENCES

[1] M. Healey. Why IT needs to push data sharing efforts. Information Week, 2010. URL http://www.informationweek.com/services /integration/why-itneeds-to-push-data-sharing-effort/225700544. Accessed: 15-10-2012.

[2] A. Mohamed. A history of cloud computing. ComputerWeekly, 2009. URL http:// www.computerweekly.com/feature/A-history-of-cloud-computing. Accessed: 18-05-2015

[3] P. Mell and T. Grance. The nist definition of cloud computing. NIST Special Publication 800-145. National Institute of Standards and Technology, U.S. Department of Commerce. URL http://csrc.nist.gov/publications/nistpubs/800-145/ SP800-145.pdf. Accessed: 15-10-2012.

[4] E. J. Giniat. Cloud computing: Innovating the business of health care. Healthcare Financial Management, 2011.

[5] ISO/IEC 17788:2014. Information technology – cloud computing – overview and vocabulary. ISO Catalogue. URL http://www.iso.org/iso/home/store/ catalogue tc/catalogue detail.htm?csnumber=60544. Accessed: 09-05-2016.

[6] S. M. Shariati, Abouzarjomehri, and M. H. Ahmadzadegan. Challenges and security issues in cloud computing from two perspectives: Data security and privacy 194 Bibliography 195 protection. 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pages 1078–1082, 2015. doi: 10.1109/KBEI.2015.7436196.

[7] NIH Website. Nih data sharing policy and implementation guidance. National Institute of Health (NIH). URL http://grants.nih.gov/grants/policy/ data sharing/data sharing guidance.htm. Accessed: 08-05-2016.

[8] R. Soni. How to get users to share social data with you. Kissmetrics Blog. URL https://blog.kissmetrics.com/get-users-to-share/. Accessed: 08-05-2016.

[9] C. Brooks. 8 benefits of online data storage. Business News Daily. URL http://www.businessnewsdaily.com/6294-benefits-of-onlinedata-storage.html. Accessed: 01-05-2016.

[10] A. Gellin. Facebook's benefits make it worthwhile. Buffalo News, 2012.

AUTHOR PROFILE:

Mr M. MAHARSHI, VIth semester, Dept of MCA, SVIM
Sree Vidyanikethan Institute of Management, Tirupati.
Email.idmaharshimanubrolu23@gmail.com

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org