TWOFOLD ACCESS CONTROL MECHANISM FOR SECURE DATA STORAGE AND SHARING

[1]Dr. NAVEEN KUMAR. S, [2]G.SIVA SANKAR

[1]Assoc. Professor, Dept. of CSE, Audisankara College of Engineering and Technology, Gudur, Tirupati(Dt), Andhra Pradesh, India

[2]PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology, Gudur, Tirupati(Dt), Andhra Pradesh, India

Abstract – Cloud based data limit organization has drawn extending interests from both scholarly and industry in the new years due to its useful and insignificant cost the board. Since it offers sorts of help with an open association, it is squeezing for expert communities to use secure data storing and sharing part to ensure data mystery and organization client insurance. To shield delicate data from being compromised, the most by and large used technique is encryption. Regardless, simply encoding data can't totally address the practical need of data the chiefs. Besides, a strong access control over download request moreover ought to be contemplated so Economic Denial of Sustainability attacks can't be shipped off to demolish clients from valuing organization. In this paper, we consider the twofold access control, concerning cloud-based limit, as in we plan a control framework over the two data access and download request without loss of security and capability. Two twofold access control systems are arranged in this paper, where all of them are for an undeniable arranged setting.

Index Terms – Daniel of Service Attacks, Cloud Computing, CP-ABE.

I. INTRODUCTION

In the new many years, cloud-based capacity administration has drawn in impressive consideration from both scholarly world and enterprises. It could be broadly utilized in numerous Internet-based business applications (e.g., Apple iCould) because of its extensive rundown benefits including access adaptability and liberated from nearby information the executives. Expanding number of people and organizations these days like to re-appropriate their information to remote cloud so that they might diminish the expense of updating their nearby information the board offices/gadgets. In any case, the concern of safety break over reevaluated information might be one of the fundamental deterrents frustrating Internet clients from generally utilizing cloud-based

capacity administration. In numerous functional applications, reevaluated information might should be additionally imparted to other people. For instance, a Dropbox client Alice might share photographs with her companions.

Without utilizing information encryption, before sharing the photographs, Alice needs to create a sharing connection and further offer the connection with companions. Despite the fact that promising some degree of access command over unapproved clients (e.g., those are not Alice's companions), the sharing connection might be noticeable inside the Dropbox organization level (e.g., director could arrive at the connection).

Since the cloud (which is sent in an open organization) isn't be completely trusted, it is for the most part prescribed to encode the information before being transferred to the cloud to guarantee information security and protection. One of the comparing arrangements is to straightforwardly utilize an encryption method (e.g., AES) on the re-appropriated information prior to transferring to cloud, so that main indicated cloud client (with substantial decoding key) can get sufficiently close to the information through legitimate unscrambling. To forestall shared photographs being gotten to by the "insiders" of the framework, a clear way is to assign the gathering of approved information clients before encoding the information. Sometimes, regardless, Alice might have no clue about who the photograph recipients/clients will be. It is conceivable that Alice just knows about ascribes w.r.t. photograph recipients. For this situation, conventional public key encryption (e.g., Paillier Encryption), which requires the encryptor to know who the information collector is ahead of time, can't be utilized. Giving approach based encryption component over the rethought photographs is subsequently alluring, so Alice utilizes the instrument to characterize access strategy over the scrambled photographs to ensure just a gathering of approved clients can get to the photographs.

In a cloud-based capacity administration, there exists a typical assault that is notable as asset depletion assault. Since a (public) cloud might not have any command over download demand (to be specific, an assistance client might send limitless quantities of download solicitation to cloud server), a pernicious help client might send off the refusal of-administration (DoS)/conveyed forswearing of-administration (DDoS) assaults to consume the asset of distributed storage administration server so the cloud administration couldn't have the option to answer legitimate clients' administration demands. Accordingly, in the

"pay-more only as costs arise" model, financial perspectives could be upset because of higher asset utilization. The expenses of cloud administration clients will rise decisively as the assaults increase. This has been known as Economic Denial of Sustainability (EDoS) assault, which focuses to the cloud adopter's financial assets. Aside from monetary misfortune, limitless download itself could open a window for network aggressors to notice the encoded download information that might prompt some potential data spillage (e.g., record size). Thusly, a viable command over download demand for re-appropriated (encoded) information is additionally required. In this paper, we propose another component, named double access control, to handle the above previously mentioned two issues. To get information in cloud-based capacity administration, trait based encryption (ABE) is one of the promising up-and-comers that empowers the classification of rethought da ta as well as fine-grained command over the reevaluated information.

Specifically, Ciphertext-Policy ABE (CP-ABE) gives a viable method of information encryption to such an extent that entrance arrangements, characterizing the entrance honor of potential information recipients, can be determined over encoded information. Note that we think about the utilization of CP-ABE in our system in this paper. In any case, just utilizing CP-ABE procedure isn't adequate to plan a rich instrument ensuring the control of the two information access and download demand.

II. LITERATURE SURVEY

To apply fine-grained approach based control over mixed data, ABE has been introduced in the composition. Positively, ABE has two chief examination branches: one is CP-ABE, and the other is KP-ABE which insinuates as key game plan ABE. This paper essentially deals with the past. In a CP-ABE, unscrambling key is connected with quality set and ciphertext is embedded with access system. This component makes CP-ABE exceptionally fitting for secure cloud data sharing stood out from KP-ABE). Note this is so considering the way that KP-ABE

requires unscrambling key to be connected with access pol cold which yields profound limit cost for cloud client. Beginning from the introduction of unique CP-ABE [9], many works have been proposed to use CP-ABE in various applications, e.g., dependable and perceptible CP-ABE multi-authority reconsidered CP-ABE and extendable varieties.

Regardless of the way that having the choice to assist fine-grained data with getting to, CP-ABE, going probably as a single plan, is far from helpful and practical to hold against EDoS attack which is what is happening of DDoS in the cloud setting. A couple of counter measures to the attack have been proposed in the composition. Notwithstanding, Xue et al. communicated that the previous works couldn't totally safeguard the EDoS attack in the algorithmic (or show) level, and they further proposed a response for secure cloud data sharing from the attack. Regardless, encounters two downsides. In the first place, the data owner is supposed to create a lot of challenge ciphertexts to go against the attack, which works on its computational weight. Second, a data client is supposed to unscramble one of the test ciphertexts as a test, which costs a great deal of exorbitant assignments (e.g., coordinating). Here the computational unpredictability of the two players is most certainly extended and meanwhile, high association bandwidth is normal for the transport of ciphertexts. The huge computational power of cloud isn't totally considered. In this paper, we will present another plan that requires less estimation and correspondence cost to stop before the EDoS attack. Lately, Antonis Michalas proposed a data sharing show that joins symmetric open encryption and ABE, which licenses clients to directly investigate encoded data. To execute the handiness of key forswearing in ABE, the show utilizes SGX to have a renouncement authority. Bakas and Michalas later extended the show and proposed a hybrid encryption contrive that reduces the issue of multi-client data sharing to that of a single client.

In particular, the symmetric key used for data encryption is taken care of in a SGX region, which is mixed with an ABE plot. It deals with the disavowal issue concerning ABE by using the SGX region. In this work, we use SGX to enable the control of the download request (so much that the DDoS/EDoS attacks can be prevented). In this sense, the explanation and the technique of our own are interesting comparable to that of the shows.

III. PROPOSED WORK

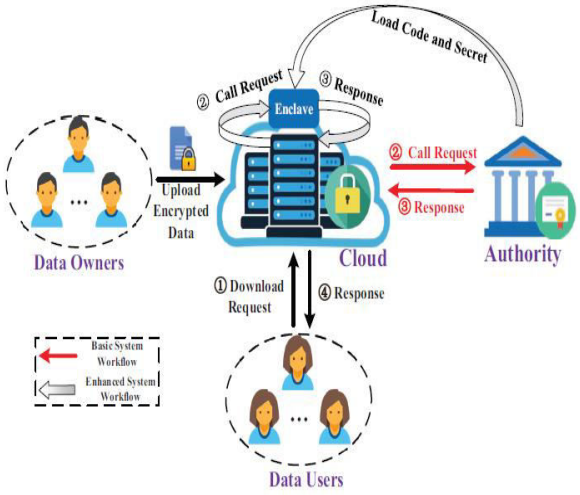

Fig. 1: System Architecture

The architectures of our dual access control systems for cloud data sharing are shown in Fig. 1. Concretely, the systems consist of the following entities:

- 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.
- 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., professors or associate professors). They will be offline once their data have been uploaded to the cloud.
- 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.
- 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.
- Enclave handles the call request from the cloud (used in the second system).

The description of workflow is introduced as follows. Data owners encrypt their data under the access policies chosen by themselves and upload the encrypted data to the cloud. Authorized data users can download the shared data by sending a download request to the cloud.

We employ the use of a hybrid system to protect the data, which combines the efficiency of a symmetric-key system with the convenience of a public-key system. In particular, the proposed dual access control systems are both in Key/Data Encapsulation Mechanism (KEM/DEM) setting. The message is encrypted by an efficient symmetric-key encryption scheme, while the inefficient public-key scheme (i.e., the CP-ABE) is used only to encrypt/decrypt a short key value.

To achieve the security requirements of anonymous data sharing, confidentiality of shared data and access control on shared data, we employ the CP-ABE technique as the basic building block. Specifically, we present the construction based on the CP-ABE scheme due to its efficiency and elegant construction. To achieve the security requirements of anonymous download request and access control on download request, we design an effective mechanism that the cloud can judge whether a data user is authorized or not without revealing any sensitive information

(including he identity of the data user, the plaintext of the outsourced data) to it.

IV. RESULTS

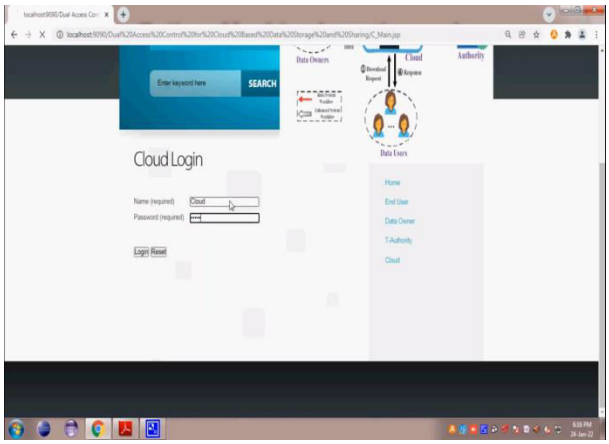

Fig. 2: Cloud Page

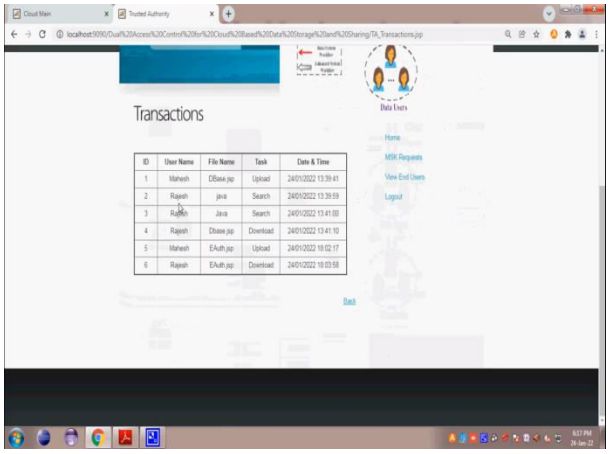

Fig. 3: View Transactions

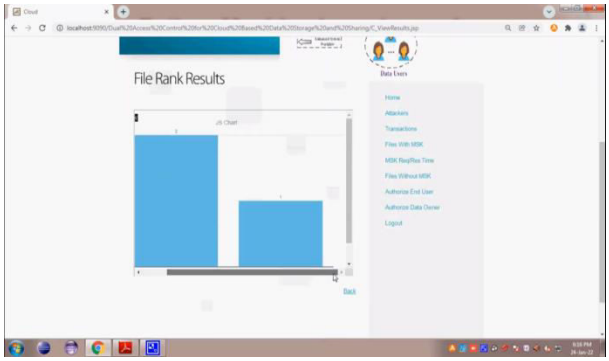

Fig. 4: File Rank Results

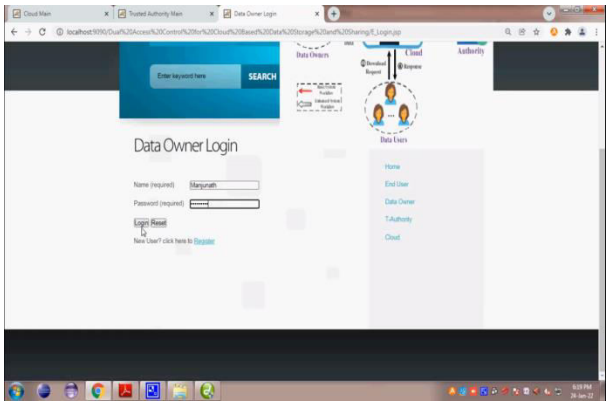

Fig. 5: Data Owner Login Page

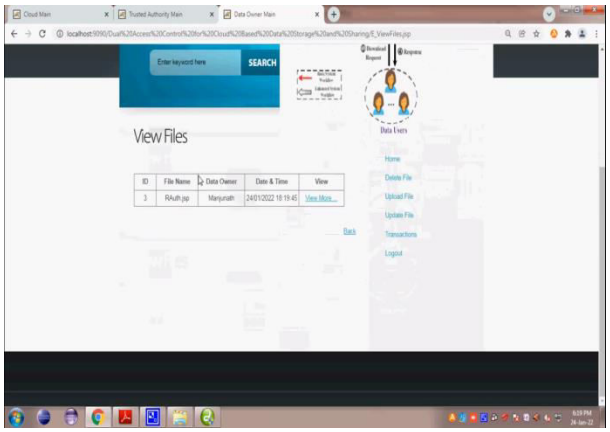

Fig. 6: View Uploaded Data Owners Files

V. 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 to DDoS/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).

REFRENCES

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

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

[3] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, 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, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

[6] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.

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

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

[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.

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

AUTHORS

Dr. Naveen Kumar. S has received him M.Tech degree in CSE from Sri Venkateswara University in 2014, Tirupati and PhD in CSE from Annamalai University in 2019 respectively. He is dedicated to teaching field from the last2 years. He has guided P.G and U.G students. Him research areas included Artificial Intelligence, Network Security and Machine Learning. At present he is working as Associate Professor in Audisankara College of Engineering and Technology, Gudur, Tirupati(Dt), Andhra Pradesh, India

G.Siva Sankar has Pursuing his MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, affiliated to JNTUA in 2022. Andhra Pradesh, India.