Expressive and Secure Cloud Storage Controlling Data Access to Protect Data

MALAPATI NARESH[1],DANDU INDRASENA REDDY[2]

#1Associative Professor,DEPT OF CSE, Newton's Institute of Engineering, Macherla, Andhra Pradesh, India.

#1PG Scholar,DEPT OF CSE, Newton's Institute of Engineering, Macherla, Andhra Pradesh, India.

ABSTRACT_ In order to ensure the classification of reappropriated information while also providing adaptable information access to cloud clients whose information is not under their physical control, secure distributed storage is a growing cloud administration trend. One of the most promising methods for verifying the administration's certification is cypher text-policy attribute-based encryption (CP-ABE). Due to the inherent "win big or bust" unscrambling feature of CP-ABE, the adoption of CP-ABE may result in an inescapable security breach known as the abuse of access accreditation (for example, decoding privileges). Here, we focus on two key cases in which a cloud client's access qualification is abused by a semi-believed specialist. CryptCloud+, a distributed storage platform with white-box discernibility and review, is proposed as a way to limit the exploitation of the system. Additionally, we demonstrate the framework's usefulness by conducting studies.

1.INTRODUCTION

Cloud processing is the critical parts of PC world. It empowers adaptable, on-request, and ease of figuring assets. In any case, the data is outsourced to some cloud servers, and different protection concerns rise up out of it. The one of the basic services of cloud processing is the putting away limit of cloud which empowers clients (data proprietor) to have their data in cloud by methods for cloud server. It gives the data access to data shoppers. It can likewise give on request assets to storage which can help specialist organizations to lessen their support costs [1]. Ordinarily clients store his/her data in confided in servers. These data are controlled by a trustable chairman [2]. The cloud storage can gives the authorization to clients

to get to their data from anyplace on any gadget in proficient way. The client's secret key is put away in their PC [10]. In cloud registering there are a few outlines is proposed to secure the cloud storage. The attribute based encryption approach is the one among sorts of encryption framework [6]. In this sort of framework, every client has the client secret key is issued by the authority. This encryption strategy is the effective adaptable approach which executes attribute-based access control (ABAC) by utilizing data or subjects' attributes as data get to strategies and also public keys [10]. AttributeBased Encryption (ABE) is a promising methodology for cloud storage that offers finegrained get to control approach over encoded data [2]. Attribute-based Encryption (ABE) is viewed as a standout amongst the most reasonable plans to lead data get to control in public clouds for it can ensure data proprietors' immediate control over their data and give a fine-grained get to control benefit. It manages confirmed access on scrambled data in cloud storage benefit [8].There are numerous ABE plans proposed, which can be partitioned into two classes: Key Policy Attribute based Encryption (KP-ABE), Cipher content Policy Attribute-based Encryption (CPABE) [2]. In the KP-ABE, a figure content is related with an arrangement of attributes, and a private key is related with a monotonic access structure [3] [1]. Contrasted and KP-ABE, CP-ABE is a favored decision for planning access control for public cloud storage. The CPABE is utilized for data proprietors and based on get to arrangements, to give adaptable, fine-grained and secure access control for cloud storage frameworks [3]. In CPABE plot, there is an authority that is in charge of attribute administration and key appropriation. There are two sorts of CP-ABE frameworks: single-authority CP-ABE where all attributes are overseen by a solitary authority, and multiauthority CP-ABE [4]. CP-ABE is utilized to data get to control for cloud storage, some multiauthority CP-ABE plans, has proposed. Exceptionally, in DAC-MACS [1], other than proposing a multi authority CP-ABE plot for cloud storage, the creators asserted that the attribute renouncement component [5]. The client's entrance authorization relies upon the attributes the client holds in the CP-ABE based access control framework, and each attribute might be controlled by numerous data clients [7]. CP-ABE plot was proposed to totally conceal the entrance strategy. In any case, the plan just bolstered the straightforward 'AND' door get to structure [9].In request to enhance the framework security, ensure client protection and spare the storage overhead of figure content, for cloud storage [8].

2.LITERATURE SURVEY

2.1 Privacy-Preserving Public Auditing for Secure Cloud Storage

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

2.2 Certificateless public auditing for data integrity in the cloud

Due to the existence of security threats in the cloud, many mechanisms have been proposed to allow a user to audit data integrity with the public key of the data owner before utilizing cloud data. The correctness of choosing the right public key in previous mechanisms depends on the security of Public Key Infrastructure (PKI) and certificates. Although traditional PKI has been widely used in the construction of public key cryptography, it still faces many security risks, especially in the aspect of managing certificates. In this paper, we design a certificateless public auditing mechanism to eliminate the security risks introduced by PKI in previous solutions. Specifically, with our mechanism, a public verifier does not need to manage certificates to choose the right public key for the auditing. Instead, the auditing can be operated with the assistance of the data owner's identity, such as her name or email address, which can ensure the right public key is used. Meanwhile, this public verifier is still able to audit data integrity without retrieving the entire data from the

cloud as previous solutions. To the best of our knowledge, it is the first certificateless public auditing mechanism for verifying data integrity in the cloud. Our theoretical analyses prove that our mechanism is correct and secure, and our experimental results show that our mechanism is able to audit the integrity of data in the cloud efficiently.

2.3 Data Storage Auditing Service in Cloud Computing: Challenges, Methods And Opportunities

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is moving data into the cloud: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. In this paper, we investigate this kind of problem and give an extensive survey of storage auditing methods in the literature. First, we give a set of requirements of the auditing protocol for data storage in cloud computing. Then, we introduce some existing auditing schemes and analyze them in terms of security and performance. Finally, some challenging issues are introduced in the design of efficient auditing protocol for data storage in cloud computing

3.PROPOSED SYSTEM

An accountable authority and revocable Crypt Cloud+ (referred to as Crypt Cloud+) has been designed to address the issue of credential leakage in CP-ABE based cloud storage systems. White-box traceability, accountable authority, auditing, and effective revocation are all supported together for the first time in a cloud storage system built on the CP-ABE protocol with this technology. Our ability to track down and ban rogue cloud users is greatly enhanced by Crypt Cloud+ (leaking credentials). When the semi-trusted authority redistributes the user's credentials, our approach can also be used.

3.1 IMPLEMENTATION

1. **Data owner:**

Is an entity who encrypts its documents under an arbitrary access control policy and outsources them to the cloud. He/She considers the time of encrypting in generating the cipher texts. We should highlight that the data owner also encrypts his/her documents under his/her arbitrary access control policy. However, in this paper we concentrate on the encryption of the extracted keywords from documents.

2. **Data user:**

Is an entity who is looking for documents which contains an intended keyword, and are encrypted in a determined time interval. The time interval is arbitrarily selected by the data user.

3. **Cloud Server :**

Is an entity with powerful computation and storage resources. CS stores a massive amount of encrypted data, and owner will monitor all file detaills

4. **TPA**

In this TPA will login by using valid user name and password after login tpa will give permission to user for login and then TPA will trace data and provide results to data owner.

5. STA

In this module STA login by using valid user name and password after STA will provide permission to user for data access.

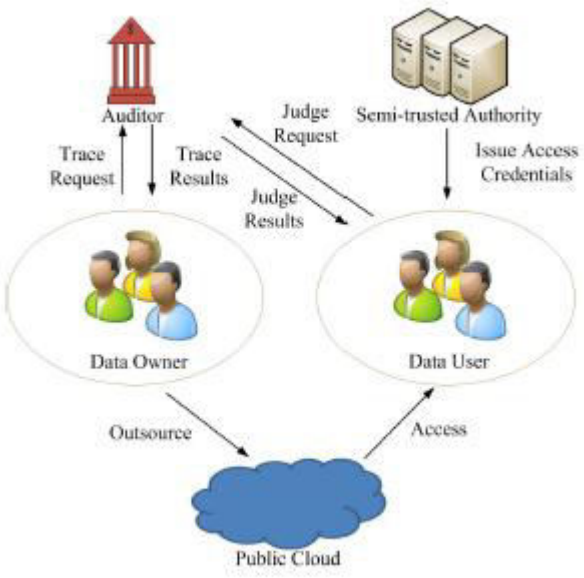

Fig 1:Architecture

4.RESULTS AND DISCUSSION

Fig 2: Home Page of Crypt cloud

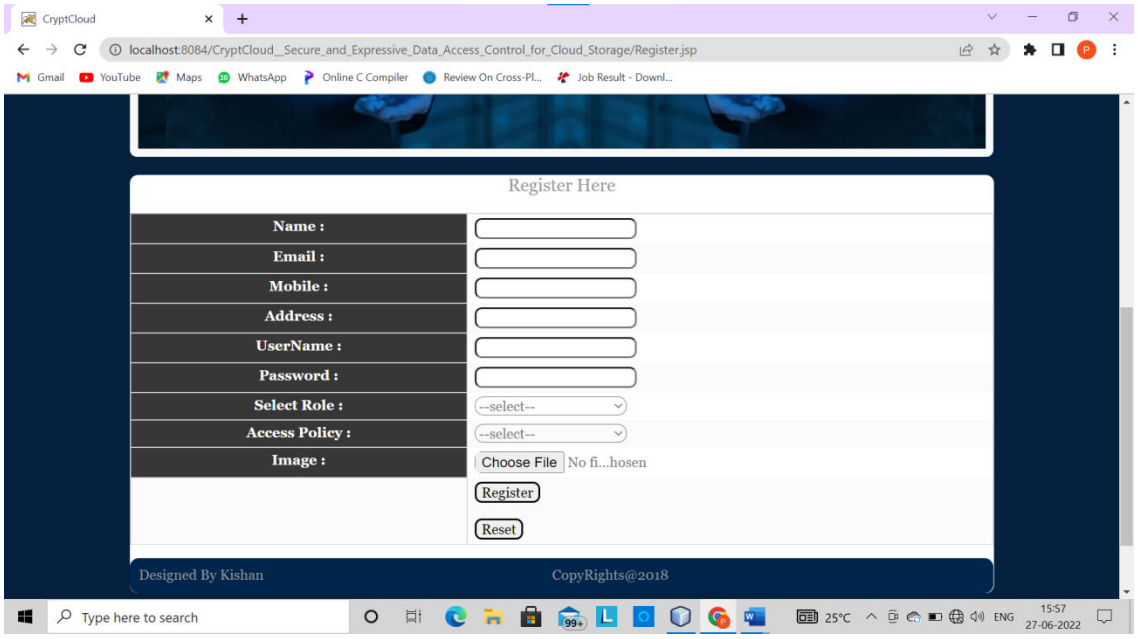

Fig 3: Showing the data user's registration page

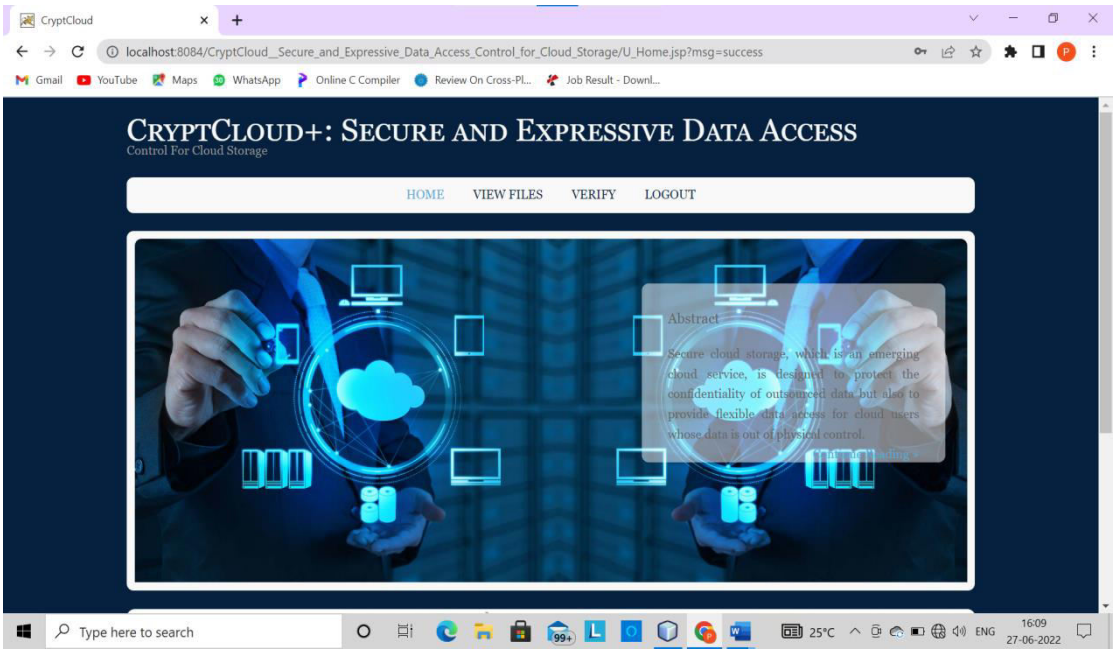

Fig 4: Data user's home page after login of data user

5.CONCLUSION

CryptCloud+, a responsible expert and revocable CryptCloud that provides white-box discernibility and examination, has been used in this work to verify certification spillage in CP/ABE based distributed storage frameworks. First CP-ABE based distributed storage architecture that provides white-box detection, responsible

expert, inspection and successful repudiation all at the same time The CryptCloud+ feature, in example, enables us to track and block spiteful cloud customers (spilling accreditations). Our solution can also be used in the case where the semi-confided in power redistribute the qualifications of the clients. As a more grounded concept (as opposed to white-box recognizability), we believe that in CryptCloud, we may require discovery detect ability. One of our upcoming projects will be to consider and examine the finding detect capabilities.

REFERENCES

[1] KaipingXue ”RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage”, IEEE2016.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, “Towards efficient content-aware search over encrypted outsourced data in cloud,” in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, “A dynamic secure group sharing framework in public cloud computing,” IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[5] Y. Wu, Z. Wei, and H. Deng, “Attributebased access to scalable media in cloudassisted content sharing,” IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[6] J. Hur, “Improving security and efficiency in attributebased data sharing,” IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271– 2282, 2013.

[7] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, “TAFC: Time and attribute factors combined access control on timesensitive data in public cloud,” in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, “LABAC: A location-aware attributebased access control scheme for cloud storage,” in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.

[10] A. Lewko and B. Waters, “Decentralizing attribute based encryption,” in Advances in Cryptology– EUROCRYPT 2011. Springer, 2011, pp. 568–588