SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE, BY USING CRYPTCLOUD+

K.Ravi Raju[1]

[1]Assistant Professor, Department of Computer Science & Engineering,

Raghu Engineering College, Visakhapatnam.

ABSTRACT

An emerging form of cloud administration, secure distributed storage looks to protect sensitive data while still making it easily accessible to users regardless of where their data resides. A promising method that could be used to confirm the administration's credibility is Encryption Using Ciphertext-Policy Attributes (CP- ABE). However, due to the "win or bust" decoding feature of CP-ABE, its use may result in an inevitable security breach known as the abuse of access certification (for example, unscrambling rights). On the one hand, side of the semi-believed specialist, the other is in, and favour of the an online client; both are studied in this paper. We propose CryptCloud+, a CP-ABE-based distributed storage framework with white-box recognizability and reviewing, to help curb abuse. We also detail the security analysis and provide experimental evidence of our framework value.

INDEX TERMS: Attribute-based Ciphertext-Policy Encryption (CP- ABE), Inevitable Security Breach, win or bust, curb abuse

I INTRODUCTION:

The popularity may be distributed computing indirectly lead to shortcomings in the privacy of redistributed Data protection and cloud security customers. One of the challenges here is figuring out how to give previously restricted users access to data stored on the cloud at their convenience [3]. Protecting data with encryption before uploading it to the cloud is a simple and secure option. However, it is important to continue exchanging information and getting ready as much as possible. For one thing, in order to share encrypted data, a data owner must first get it Suddenly, from the cloud reencode assuming the information owner doesn't have any neighbourhood information that is repeated). There is a lot of appeal in cloud registering due to the possibility of access control with fine granularity for encrypted data [51]. In this case, Encryption using Ciphertext-Policy Attribute (CPABE) [15] could be a workable solution for certifying the privacy of information and providing granular permissions. For instance, in a CPABE based distributed storage system, organizations (such as the University of Texas at San Antonio) and people (such as pupils, teachers, and guest researchers) can first signal interest in reaching an agreement over characteristics of a prospective cloud client. Authorized users of the cloud then granted access information (i.e., decoding keys) that specific from their trait sets (such as student (job, employee job, or visitor job) and can be used to retrieve the stolen data. Because of its strong one-to -numerous encryption component, CP-ABE not only provides a solid technique for protecting cloud-stored data, but also enables granular the power to decide who has access to that data. Unfortunately, the possibility of abused access accreditation is rarely taken into account by the pre-existing CP-ABE based cloud capacity frameworks. As an illustration, a university may implement based on CPABE distributed storage framework to redistribute encrypting student information the cloud in accordance with certain entry approaches that are compatible with the applicable information sharing and protection enactment (such as the federal family rights to education Protection (FERPA) Act and the Health Insurance Portability and Accountability Act (HIPAA), which was passed in 1992. The organization top dog (say, the head of security at a university) lays out the ground rules for the system and provides users with access credentials (e.g., understudies, employees, and visiting researchers). It common practise to assign a number of traits to each employee (e.g. director, ranking director, monetary official, tenured staff, residency track personnel, non- residency trace workforce, educators, extra, guest, as well as understudies).

Student data stored in the cloud can only be accessed by staff members whose attributes match the unmasking strategy of the appropriated data (for example understudy confirmation materials). Any delicate student information kept in the cloud as we may have known, might have far- reaching consequences for the organization and the people who

use it (e.g, prosecution, loss of advantage, criminal allegations). Using We may benefit from the CP-ABE prevent a security lapse caused by external assailants. Nevertheless, when a member of the organization is accused the act the wrong doings associated with the transfer that decodes rights both the transit of student plain text data configuration for illegal monetary advantages, how may we be able to definitively demonstrate that the insider is liable? Can we also ignore the access gains we gave up? In addition to the aforementioned concerns, we also have a question about a important age expert. In most cases, a semi-trusted expert issues the access qualification (i.e., decoding key) for a cloud client based on the characteristics of the client. How can we prevent this professional from (re- distributing) the newly created access credentials to other parties?

II. RELATED WORKS

2.1 Keyword search for public key encryption.

Authors include:G. Persiano, R. Ostrovsky, G. Di Crescenzo, and D. Boneh.

We investigate the challenge of indexing information that has been encrypted with an open key. Take the example of Bob sending an encrypted email to Alice using Alices public key. Because of this, an email gateway may look for the word in an incoming message before deciding how to handle it. Instead, Alice would prefer to keep her communications private and not give the gateway decryption keys. We define and build a system where Alice can give the gateway a key that checks if in the email, the term is used as a keyword without the gateway learning any other information regarding the email. Key Search for Public Key Encryption is the name given to this system.

Let's say that there is a mail server that stores a bunch of messages that were all public encrypted for Alice. With our system, Alice provide mailing server with a key which allows it to identify all messages containing a specific keyword while gaining no other information about the messages. We provide a conceptualization of Public-key cryptography using keyword-based searches, and then provide several implementations.

2.2 (Without random oracles) Anonymous hierarchical identity- based encryption

Authors: B. Waters and X. Boyen. We introduce a cryptosystem based on the concept of identities, which allows for completely private ciphertexts and a decentralised system of key distribution. Using the relatively relaxed complexity assumption of Decision Linear groups in bilinear systems, we provide a proof of security for the canonical model. This system is effective and useful because ciphertexts are linear in size relative to the level of the hierarchy they represent. Uses for encrypted data include searching, private communication, and other uses. As the initial scheme to provide verifiable anonymity in the conventional model and the initial to realise fully anonymous all levels of HIBE in the hierarchy, our results solve two outstanding issues in the field of anonymous identity-based encryption.

III. METHODOLOGY

In this work, we have designed a revocable Crypt Cloud with an accountable authority that allows for White-box auditing and traceability (we call it Crypt Cloud+) to solve the problem of credential leakage in Cloud storage based on CP-ABE systems. Black-box traceability, accountable authority, auditing, and efficient revocation are all supported in this first cloud storage solution based on CP- ABE.In particular, Cloud Crypt+ permits us to track down and delete negative cloud users (leaking credentials). When the semi-trusted authority redistributes user credentials, our method can be used as well.

A. IMPLEMENTATION:

i. DATA OWNER MODULE:

Is a company or organisation that sends sensitive files to the cloud where they are encrypted using a policy of unpredictable access. When creating cypher texts, he or she takes into account the encrypting time. To emphasise, the data owner encrypts records filed under his or her own Unpredictable access control rules. This paper, however, is focused on the protection of document keyword extracts.

ii. END-USER MODULE FOR DATA:

Refers to a person or thing searching for encrypted files within a given time frame that contain a specific keyword. The user of the data chooses the time period at will.

iii. MODULE FOR A CLOUD SERVER:

Is something that can perform complex calculations and store huge volumes of information In CS, a lot of encrypted information is stored, the search tokens, and are used to locate the requested files on the data users behalf. The cloud searches for the appropriate files and returns them to the data consumer.

iv. RELIABLE THIRD-PARTY SERVICE PROVIDER:

Is a completely reliable party that receives the access trees of all users and creates private keys for them based on the sets of attributes they have specified. After confirming the authenticity of the user, the TTP will return their credentials over an encrypted and verified connection.

IV. EXPERIMENT, RESULTS AND ANALYSIS

Fig 1: In the above screen the user can using fields

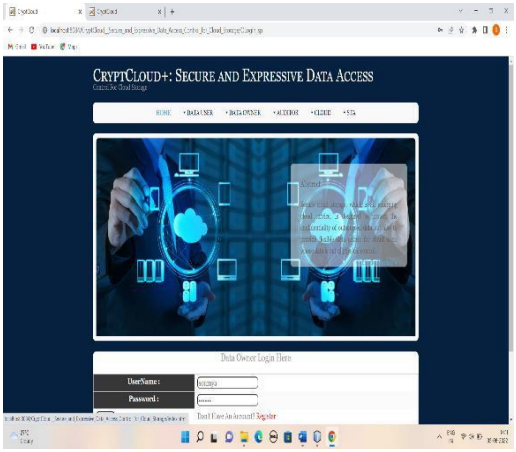

Fig 2: In the above screen the user can login by using user name and password.

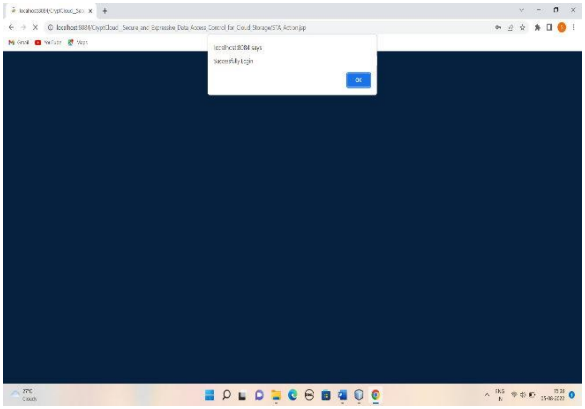

Fig 3: In the above screen user can login successfully

Fig 4: In above screen user can used file

Fig 5: In the above screen user can file register

V. CONCLUSION AND FUTURE WORK

This work includes devised a CryptCloud+ with revocable credentials and an accountable authority that enables white-box traceability and auditing, which we call CryptCloud+, to combat leakage of credentials in CP-ABE-based cloud storage is a problem systems. White- box auditing, responsible authorities, traceability, and efficient revocation are all supported in this the first cloud storage system based on CP-ABE. In particular, CryptCloud+ enables us to monitor and terminate potentially harmful cloud users (leaking credentials). To extend the applicability of our method, it can be used when a semi-trusted authority is responsible for redistributing user credentials.

Black-box traceability, a more robust concept than white-box traceability, is something we should keep in mind for CryptCloud+.Our plans include investigating methods of providing auditable and transparent black-box traceability.

References:

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc:

Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

[2] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4] NuttapongAttrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[5] Amos Beimel. Secure schemes for secret sharing and key distribution.

PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[6] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge.

In Advances in Cryptology- CRYPTO'92, pages 390–420.
Springer, 1993.

[7] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing:

Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.

[9] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system

ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.

[11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching my cloud. In Computer Security-

ESORICS 2014, pages 362–379.
Springer, 2014.

[12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.