International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

Aggregate Key Based Data Sharing in Cloud Storage

PEDDIREDDY SRI SATYA LAKSHMI SUJAYA [#1] and CH.SUBHASH [*2]

[#] PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science and Engineering, JNTUK,A.P, India

[*] Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA

***Abstract*— Presently, the cloud storage attracts several users due to its widespread usage. Data sharing plays a vital role in the cloud storage. In this paper, we make a study about the efficient data processing in the cloud storage system. We propose an enhanced Aggregate key based cryptosystem in the cloud storage. This approach reduced the number of key generation in the public cloud storage system i.e users can generate several secret keys and at last, it gets aggregated. The main idea of this study is to reduce the no. of keys generation and also aggregate the large no.of keys. By giving different privileges, the users can differentiate the data access privileges. Experimental results prove the effectiveness of the system.**

***Index Terms*— Cloud storage, cryptosystem, key generation, Aggregation and secret keys.**

I. Introduction

Presently, the cloud storage spaces have created a great attraction towards the cloud user as well as the Cloud Service Provider. A massive amount of data has been generated over the internet. The data may be in audio, video etc. Most of the business user’s relied upon the cloud storage space due to its lower cost, better agility and improved resource utilization [1]. The user might share their private data over the cloud server. In some scenario, the users worried about the data loss that may occur in any accidental cases. The data loss occurs by any malicious users ie. Unauthorized users. In order to prevent attackers from data stealing, the encryption schemes are used. Rather than storing the information to the hard drive or some other neighborhood stockpiling [2], we spare the information to the remote stockpiling which is available from anyplace and at whatever time. It decreases endeavors of conveying physical capacity to all over the place. By utilizing cloud capacity, we can get to data from any PC through web which discarded confinement of getting to data from same PC where it is stored [3].

The solution is to encode information before transferring to the server [4] with client's secret key. Information sharing is again vital system of distributed storage, since client can share information from anyplace furthermore, at whatever time to anybody. In any case, the challenging is that how to share the scrambled information. Cryptography technique can be applied in a two major ways: i) symmetric key encryption and ii) asymmetric key encryption. In symmetric key encryption, same keys are used for encryption and decryption [5]. By contrast, in asymmetric key encryption different keys are used, public key for encryption and private key for decryption. By the use of asymmetric key encryption is more flexible for our approach.

The rest of the paper is organized as follows: Section II describes the related work studied by other researchers. Section III describes about the proposed scheme to solve the challenging issue. Section IV describes the experimental analysis of the research study. At last, concluded in Section V.

II. RELATED WORK

There exist a few expressive Attribute based encryptions strategies where the unscrambling calculation just requires a consistent number of pairing calculations. As of late, *Green et al.* proposed a solution for this issue by presenting the idea of ABE with outsourced unscrambling, which to a great extent takes out the unscrambling overhead for clients. In view of the current ABE plans, Green et al. additionally exhibited concrete ABE plans with outsourced unscrambling issues.

In these current plans, a client gives an untrusted server, by the use of proxy server, cloud service provider. By the use of transformation key, TK that permits to decipher any ABE ciphertext CT fulfilled by that client's traits or access approach into a direct ciphertext CT', and it just acquires a little overhead for the client to recuperate the plaintext from the transformed ciphertext CT'. The security property of the ABE plan with outsourced unscrambling ensures that intruders can steal the information; in any case, the plan gives no certification on the accuracy of the transformation done by the cloud server. In the cloud processing setting, cloud administration suppliers may have financial related services, to return erroneous answers.

There are a progression of cryptographic plans which go similarly as permitting a third party verifier, to check the accessibility of documents for the benefit of the information proprietor without leakage anything about the information, or without trading off the information proprietors secrecy. Benaloh et al. [2] introduced an encryption plan which is initially proposed for transmitting the broadcast scenario.

Since the key construction is simple, the derivation process is quite harder. Each class is associated with prime generation, which insists the efficient secured form. Identity based encryption (IBE) (e.g., [5], [6], [7]) is a public key encryption in which the general population key of a client can be set as a identity string of the client (e.g., an email address, contact number). There is a private key generator (PKG) in IBE which holds an expert mystery key and issues a mystery key to every client as for the client personality. Guo et al. [8], [9] attempted to assemble IBE with key conglomeration. In their plans, key collection is compelled as in all keys to be totaled must originate from various ―identity divisions. Attribute based encryption (ABE) [11], [12] permits each ciphertext to be connected with a characteristic, and the master secret key holder can remove a mystery key for an approach of these properties, so that a ciphertext can be unscrambled by this key, if its related to ascribe the approach.

III. PROPOSED SCHEME- ENHANCED AGGREGATE KEY GENERATION SYSTEMS

In this section, we explain about the enhanced cryptosystem in the cloud storage. In order to share the data to the server, a public key and secret key is generated by the servers. In the cloud scenario, anyone can encrypt and outsource the data to the cloud server. But only, an authorized user can decrypt the data. The system architecture is presented in Fig.1.

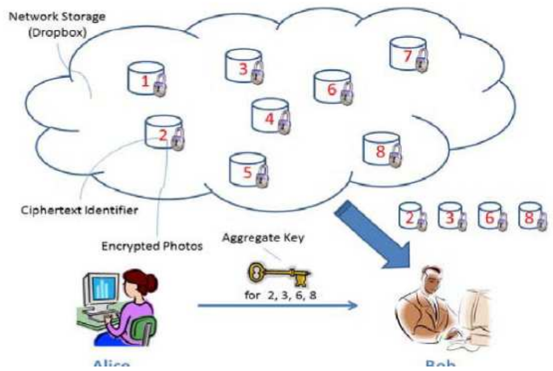

Fig.1. System Architecture

Based on the aggregate key send to the bob, he can decrypt the data. It is executed in four phases:

a) Setup Phase: It takes an implicit security parameter. The set up phase is executed at an untrusted server.
b) KeyGen Phase: This phase is initiated by the data owner that generates the public key and master key as (pk, mk).
c) Encrypt Phase: It is executed by anyone, who needs transmit the data to be encrypted. It takes the input as public parameter pk, data d, and ciphertext class i. Here, the message m is encrypted by the data owner and creates ciphertext C. Input: public key pk, index i and message m and the output is generated ciphertext C.
d) Extract Phase: It is processed by the data owner, that the delegates the decrypting cipher classes.
e) Decrypt phase: Only the authorized user can decrypt the data. It takes the input, public parameters pk, ciphertext C, set of attributes that contain ciphertext class i. The overall working process of the system is presented in fig.2.

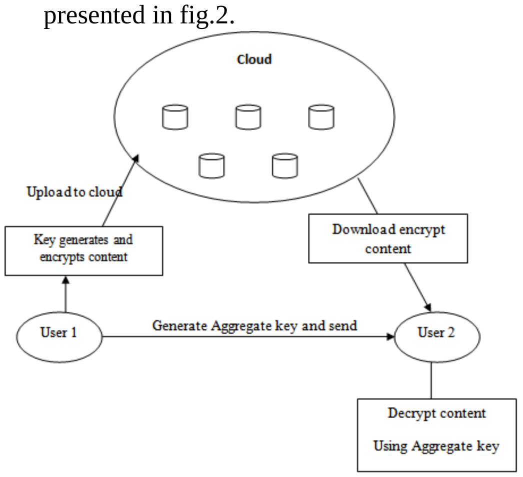

Fig.2. Overall working process of the system

IV. EXPERIMENTAL ANALYSIS

In this section, the performance analysis is carried out in the multi-owner application of the federated cloud storage. It deploys in tree- based key agreement structure. A logic key hierarchy is engrossed with the binary tree of height h=3 with 2h ciphertext classes for the authorized user. The delegation ratio r is derived from the ratio of current ciphertext class C_i to the ratio of total number of ciphertext classes. A random delegation pattern is adopted. The computation of combinatorial function of r and h, we obtained 104 combinations of the delegated classes. The parameter settings for h=16 with variant delegation ratio r is shown in table 1.

TABLE 1. PARAMETER SETTINGS

r	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95
Setup	8.4									
Extract	2	4	5	7	8	9	10	10	11	11
Decrypt	4	6	9	12	14	15	16	18	20	20

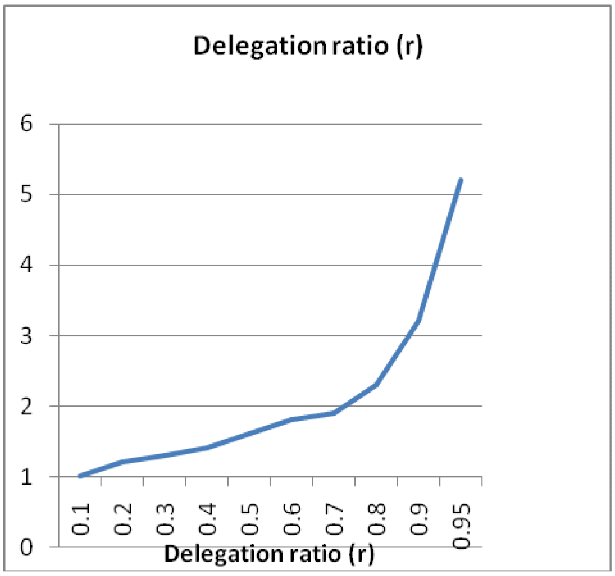

Fig.3. Delegation ratio (r) under tree-based approach

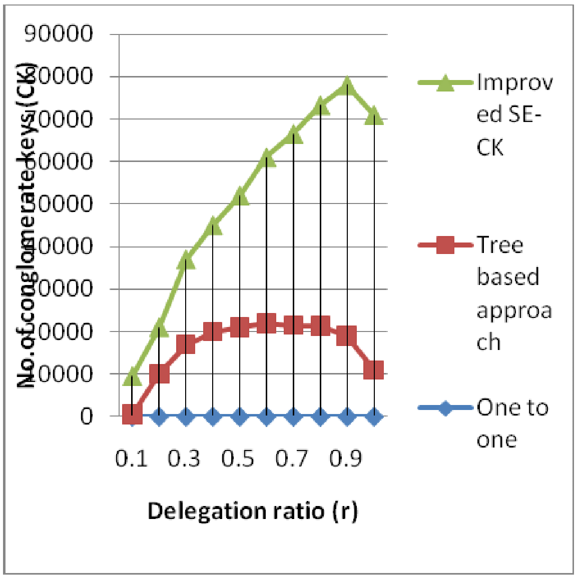

Fig.4. Comparison graph for variant approaches like Improved SE –CK, Tree based system and One-to-one

V. CONCLUSION

Data sharing is an important phase in the cloud storage systems. In order to ensure the integrity and privacy of the data in the cloud systems, the data sharing process should be well-defined. Cryptographic schemes are getting more versatile and involve multiple keys for a single application. Our approach was considered in all these aspects and generated a novel approach to “compress” secret keys in public-key cryptosystems which support delegation of different cipher text classes in a cloud storage. The delegate can decrypt the encrypted data by obtaining the aggregate key and need not worry about to which class the data belong to. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. In addition to this, we can provide different access rights to different users, to maintain the integrity of the data.

REFERENCES

[1] Cheng-Kang Chu ,Chow, S.S.M, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , —Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage‖, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[2] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, —Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ in Proceedings of ACM Workshop on Cloud Computing Security (CCSW ’09). ACM, 2009, pp. 103–114. 886

[3] J. Benaloh, —Key Compression and Its Application to Digital Fingerprinting,‖ Microsoft Research, Tech. Rep., 2009.

[4] B. Alomair and R. Poovendran, —Information Theoretically Secure Encryption with Almost Free Authentication,‖ J. UCS, vol. 15, no. 15, pp. 2937–2956, 2009.

[5] D. Boneh and M. K. Franklin, —Identity-Based Encryption from the Weil Pairing,‖ in Proceedings of Advances in Cryptology – CRYPTO ’01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.

[6] A. Sahai and B. Waters, —Fuzzy Identity-Based Encryption,‖ in Proceedings of Advances in Cryptology - EUROCRYPT ’05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457–473.

[7] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, —Practical Leakage-Resilient IdentityBased Encryption from Simple Assumptions,‖ in ACM Conference on Computer and Communications Security, 2010, pp. 152–161.

[8] F. Guo, Y. Mu, and Z. Chen, —Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key,‖ in Proceedings of Pairing-Based Cryptography (Pairing ’07), ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.

[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, —MultiIdentity Single-Key Decryption without Random Oracles,‖ in Proceedings of Information Security and Cryptology (Inscrypt ’07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[10] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, —Practical Leakage-Resilient IdentityBased Encryption from Simple Assumptions,‖ in ACM Conference on Computer and Communications Security, 2010, pp. 152–161.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, —Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,‖ in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06). ACM, 2006, pp. 89–98.

[12] M. Chase and S. S. M. Chow, —Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,‖ in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

[13] T. Okamoto and K. Takashima, —Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption,‖ in Cryptology and Network Security (CANS ’11), 2011, pp. 138–159.

AUTHOR PROFILE

SRI SATYA LAKSHMI SUJAYA is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Computer Science) Her Area of interest includes Cloud Computing and its objectives in all current trends and techniques in Computer Science.

CH.SUBHASH **M.TECH** is Working as M.Tech Assistant Professor, Department of Computer Science & Engineering of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada, A.P, India.