ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(42), DOI: 10.17485/ijst/2016/v9i42/97522, November 2016* ISSN (Online) : 0974-5645

Improved Searchable Encryption via Conglomerate Keys in Federated Cloud Storage

G. Kavitha* and R. Priya

School of Computing Sciences, Vels University, Pallavaram, Chennai - 600117, Tamil Nadu, India;
giridharan.kavitha@gmail.com priyaa.research@gmail.com

Abstract

Objectives: Cloud computing is the sort of computing process that shares the data and its resources in the Internet. Data Leakage is the main challenge prevails in the federated cloud storage service. This challenge is overcome by proposing an efficient searchable encryption system. **Methodology:** An improved searchable encryption is designed to apportion the data among the multi-users. An efficient key management is the required phase of the encryption schemes. Owing to adversaries, a promising approach using conglomerate keys invents as a better searchable encryption schemes in multi-owner applications. **Findings:** By reducing the count of trapdoor function to cloud data from the multi-user, an effective search over the encrypted data is performed. In compare to existing models, tree based approach and one to one function, the proposed, improved SE-CK works efficient in terms of lessened delegation ratio and conglomerate keys. **Applications/ Improvements:** This method can also be extended to the hybrid architecture like Indexing schemes, Re-encryption schemes etc.

Keywords: Data Sharing, Data Leakage and Multi-Owner Applications, Federate Cloud Storage, Searchable Encryption, Trapdoor Functions

1. Introduction

Due to rapid technologies evolution in data sharing, the need to keep the secret data is an essential task. Presently, cloud computing is the novel technology widely used by the people, to access their data from any remote settings. Relied upon the data demands, the data is approached in pay per use service[1]. In the domain of Cloud computing, the main characteristic is the cloud storage application. It is widely adopted by most part of the business sectors. It supports the organization people by offering a massive amount of storage space at down expenses. The need of data storage and high performance computation is emancipated by Cloud Service Provider. Some real providers are Amazon, Drop box, Google app engine etc. The main practices of the cloud computing is to free from the data maintenance at the local machines[2]. Though it offers a fruitful services for its user, it also poses a significant risks like confidentiality, privacy, integrity etc. of those saved files.

Concerning about the security issues, the data outflow and data secrecy is the most issues prevail in cloud storage system. It is resolved by some encryption schemes. Each cloud data is secured from the intruders by enforcing encryption schemes[3]. The most renowned schemes are the Attribute Based Encryption, Ciphertext policy based Attribute Based Encryption, Key Policy based Attribute Based Encryption, Proxy Re-encryption etc. The above all processes take attributes as input, for both encryption and decryption schemes. Proxy re-encryption is the fundamental cryptographic schemes that transform ciphertexts into double-refined encryption keys. It employs re-encryption protocols that work independently over the private keys of sender and the receiver.

Group key management [4] is the enhanced concept developed from the basic encryption methodologies. It is widely employed in the group communication process. A shared key is generated and it's shared among

* *Author for correspondence*

the group members. It is mainly deployed during the mid –communication process of its group members. Each member in the group should take roles of creating, distributing and deleting the keys. The session group key management [5] is obtained from two anonyms: 1. Group controller and 2. Key Server. Group Controller (GC) takes account of creation, appropriation and resending the keys among the members in the group whereas Key Server (KS)[6] take account of key maintenance. The Figure 1 illustrates the group communication process in cloud settings.

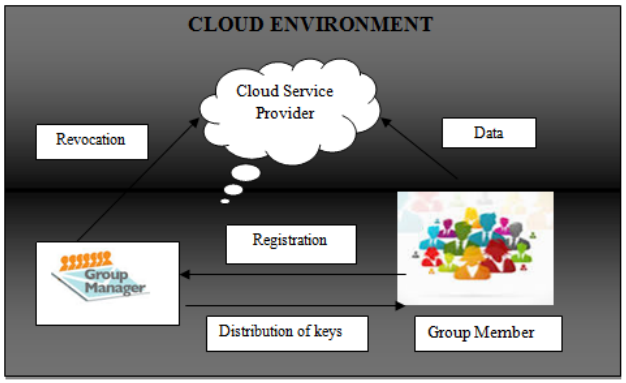

Figure 1. Data sharing in group communication process.

The review articles analyze based on two concepts: 1. Data sharing, 2. Cloud security. The five divisions of security aspects are Confidentiality, Integrity, Availability, Accountability and Privacy. The advent of backtracking algorithm[7]. The study contributes to reduce the consequences of virtual migrations in a lessened time[8]. Implements new framework which helps to improve the integrity verification for remote data stored in cloud[9]. The security concerns in the federated cloud storage[10]. Their aggregate key schemes lessened the file uploading time with efficient security systems. The regression tree concept in the federated cloud settings[11]. The trust system ensures that the ranking model yields better results than the other systems. In[12] enhanced the HABE concept by the re-encryption process. The keys are regenerated to cut down the computational overhead process exists in mobile users.

In[13] studies about those previous aspects and the threat models related to security. The prerequisites for better data privacy and cloud security suggests by in[14]. Furthermore, it incorporates to define security mechanisms for securing personal's data by[15]. The factors that mislead the security concern are studied by[16]. They combined with the business sectors to know about the information security in the cloud, and this is further extended by [16] with some software security enforcements. From his study, explores that SaaS is widely adopted rather than IaaS and PaaS[17]. They depicted about the user's experiences about sharing data in cloud system and the survey is conducted by[18]. In his survey, he states that "Even though the researchers define numerous cloud security models, the act of defending from the malevolent users is still a significant study. It is declared from the study that the analysis over security and privacy issues is essential, in the cloud.

The study concerning to data apportioning is also discussed by several authors. The apportioning of the data in the business sectors is studied by[19]. The information is acquired from the business sectors like government agencies. Before apportioning the data across the cloud, the data dissemination process takes place. They effectively classify the data and then shared to cloud server[20]. The data sharing along with the revealing of user's personal data issues. His study makes a great development towards the organizations to be aware of their personal data. Thus, the data shared via public channel to the cloud server cause greater effects on the confidentiality of the users. Then the study on banking applications is done by[21]. This further enhanced in view of public health information, educational development etc. is studied by[22,23].

Several studies are relevant to both data sharing and cloud security. In that approach, the advent of access control mechanisms is widely explored. It employs access right permission of the cloud data. In[24] framed the most effective technique, Attribute Based Encryption approach. Each data of an entity is encrypted based on fine grained access policy. The users mentioned in the Access Control Lists (ACLs) are not permitted to access the cloud services. And this is finalized as the coarse grained access to data. The Ciphertext is obtained by encrypting the data using the public key. The use of ciphertext is merged with ABE and it's known as Ciphertext policy based Attribute Based Encryption. The Secret key is defined with set of attributes for the group of users and it is shared among the group of users. The users are permitted to access the data if they satisfy the access policy with cloud service provider. It is only applicable to the Ciphertext chosen attacks. The data computation incurs heavy time and space complexity as serious drawbacks. The study is further enhanced in focus to the Certificate management. A Certificate Less Proxy Re-encryption (CL-PRE) is framed by[25]. The study targets to recover from Key Agreement Problem (KAP). The CSP

doesn't make use of public keys to authorize the users. It offers greater benefits towards large scale systems.

From the reviews, we infer that the analysis on data apportioning in the cloud doesn't meet the user's requirements. Still, cloud security and data sharing are challenging task in the cloud settings. The major drawbacks are the:

- The design model of the shared data is not an impeccable one.
- In group communication, the multi-owner application is not enhanced.
- Some unexpected data privilege will expose the data to the malevolent users.
- User's control over the multi-document incurs high number of shared keys.
- The Trapdoor functions are not employed properly.

2. Improved Searchable Encryption via Conglomerate Keys

In this section, we propose an improved Searchable encryption via conglomerate keys. It works in five steps. They are: 1. Data Owner 2. Network storage 3. Encrypted Conglomerate key and Searchable Encryption 4. Generation of Trapdoors 5. File users. These are explained as follows:

- **Data Owner:** In first process, the data owner enrolls with the cloud server. He/ She do not know whether they choose the emancipated servers. The setup step uses security parameter and the classes of ciphertextas the inputs. The class of Ciphertext includes the class index of the file that ranges from 1 to n. A public parameter param is obtained as the output.
- **Network Storage:** A sample Drop box, Gmail, Send space etc. are used as the Cloud storage. In the group communication process, any users can access any kinds of data with the shared secret key.

2.1 Encrypted Conglomerate Keys and Searchable Encryption

The searchable encryption works in four phases:

- Key generation- It generates public and master key as (p_k, ms_k),
- Encryption- With the help of p_k, ms_k and index i of ciphertext classes, the Ciphertext C is obtained.
- Extract- In the group communication, some members may need of other member's files. It executes by the data owner. By employing of master key ms_k and ciphertext class i, the conglomerate keys for the set of ciphertext class S_i.
- Decryption- It is executed by the Group members who possess conglomerate keys from the Extract step. Using conglomerate keys CK, Group of users S, Ciphertext class C_i as the input, the decrypted output D_m.
- **Generation of Trapdoors:** Trapdoor algorithm is run by the user who holds the conglomerate keys. With the use of conglomerate keys CK, the search operation is initialized. The output trapdoor Tr is predicted from CK and keyword K.
- **File user:** The computed key is transferred to its group member via any security devices like email, etc. At last, the user who possess function Tr can decrypt the data. By doing so, the data shared among the group proves the confidentiality.

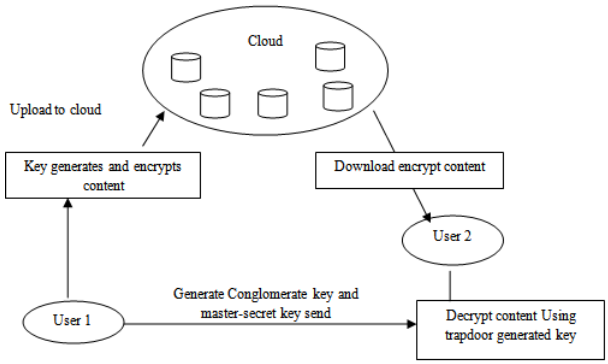

Figure 2. Proposed workflow.

The proposed workflow is described in Figure 2. Consider two users U1 and U2. Both inclusively share the data over cloud settings. By using Improved Searchable encryption via conglomerate keys, the data is efficiently secured. The features of the proposed approach are the:

- The user can remind of the keys.
- Since the group manager works as cloud service, the trapdoor can get from anywhere.
- The trapdoor keys are fully secured with efficient encryption approach.

3. Performance Analysis

In this section, the performance analysis is expressed 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 count 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

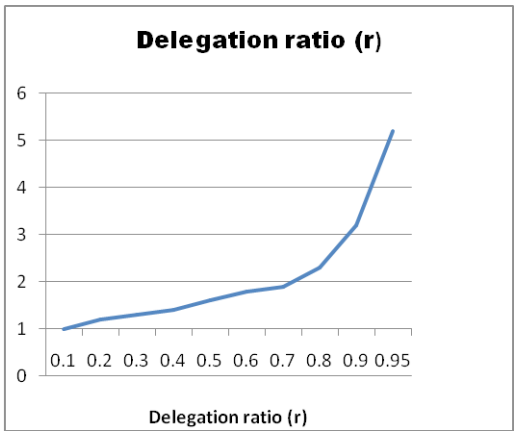

Figure 3. Delegation ratio (r) under tree-based approach.

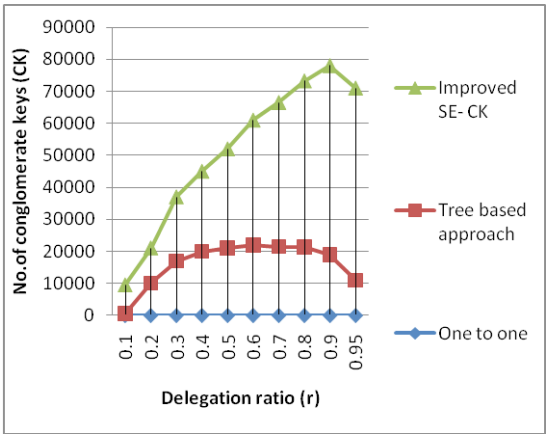

Figure 4. Comparison graph for variant approaches like Improved SE –CK, Tree based system and One-to-one.

From the Figure 3 and 4, our proposed approach, improved SE-CK works efficiently in terms of delegation ratio and no. of conglomerate keys.

4. Conclusion

Data privacy is a vital research concept of storage systems. Nowadays, Federated Cloud environment usage is growing vast. To develop the privacy of the stored data, the user encrypts the data before uploading into cloud. In the multi-owner perspectives, the files are shared among the users available in the group. Thus, these data may encounter some unexpected events like byzantine faults, delay response to the requests, malevolent users etc. In order to prevent from these sorts of events in the federated cloud scenario, an efficient key management system is the best solution. We propose an improved Searchable Encryption via Conglomerate keys systems that aims to reduce the usage of number of trapdoor functions in the federated environment. Concurrently, it also reduces the key computational complexities. Performance analysis is carried out in binary tree-based key agreement structure in terms of estimating the delegation ratio and number of conglomerate keys generation. It is evident from the results that our proposed approach works effectively in federated cloud environment. As future work, we shall study about the hybrid architecture of both data and key conglomeration systems.

5. References

1. Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable and fine-grained data access control in cloud computing. Proceedings of IEEE INFOCOM; San Diego, CA. 2010. p. 15–9.
2. Goh EJ, Shacham H, Modadugu N, Boneh D. SiRiUS: Securing remote untrusted storage. NDSS. 2003; 1-15.
3. Ateniese G, Fu K, Green M, Hohenberger S. Improved proxy re-encryption schemes with applications to secure distributed storage. NDSS. 2005; 9(1):1-30.
4. Bethencourt J, Sahai A, Waters B. Ciphertext policy attribute-based encryption. 28th IEEE Symposium on Security and Privacy; Berkeley, CA. 2007. p. 321–34.
5. Kamara S, Lauter K. Cryptographic Cloud Storage. Financial Cryptography and Data Security. Vol. 6054. 2010; p. 136–49.
6. Rocha F, Abreu S, Correia M. The final frontier: Confidentiality and privacy in the cloud. Computer. 2011; 44(9):44–50.
7. Huang R, Gui X, Yu S, Zhuang W. Research on privacy-pre-

serving cloud storage framework supporting ciphertext retrieval. International Conference on Network Computing and Information Security; Guilin. 2011. p. 93–7.
8. Suja TL, Savithri V. Backtracking algorithm for virtual cluster migration in cloud computing. Indian Journal of Science and Technology. 2015 Jul; 8(15):1-6.
9. Kalpana V, Meena V. Study on data storage correctness methods in mobile cloud computing. Indian Journal of Science and Technology. 2015 Mar; 8(6):1-6.
10. Reddy VK, Sushmitha Y, Rao KT. Distributed authentication for federated clouds in secure cloud data storage. Indian Journal of Science and Technology. 2016 May; 9(19):1-7.
11. Mourougan S, Aramudhan M. Regression tree based ranking model in federated cloud. Indian Journal of Science and Technology. 2016 Jun; 9(22):1-7.
12. Devi BS, Shruthi S, Rajeswari ST, Shanthi P, Umamakeswari A. secure data sharing in scalable mobile cloud environment using HABE with re-encryption. Indian Journal of Science and Technology. 2015 May; 8(S9):1-6.
13. Xiao Z, Xiao Y. Security and privacy in cloud computing. IEEE Commun Surveys Tutorials. 2012; 15(99):1–17.
14. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. International Conference on Computer Science and Electronics Engineering; Hangzhou. 2012. p. 647–51.
15. Zhou M. Security and privacy in the cloud: a survey. 6th International Conference on Semantics Knowledge and Grid (SKG); Beijing. 2010. p. 105–12.
16. Wang J, Liu C, Lin L. How to manage information security in cloud, computing anchorage. AK. 2011; 1405–10.
17. Wang Y. The role of SaaS privacy and security compliance for continued SaaS use. International Conference on Networked Computing and Advanced Information Management (NCM); Gyeongju. 2011. p. 303–6.
18. Oza N, Karppinen K, Savola R. User experience and security in the cloud - An empirical study in the finish cloud consortium. IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom); 2010. p. 621–8.
19. Sarathy R, Muralidhar K. Secure and useful data sharing. Decis Support System. 2006; 42(1):204–20.
20. Butler D. Data Sharing Threatens Privacy. Nature Publishing, Group; 2007. 449(7163):644–5.
21. Mitchley M. Data sharing: Progress or not? Credit, Manage. 2006; p. 10–1.
22. Feldman L, Patel D, Ortmann L, Robinson K, Popovic T. Educating for the future: Another important benefit of data sharing. Lancet. 2012; 1877–8.
23. Geoghegan S. The latest on data sharing and secure cloud computing. Law. San Diego, CA. 2011. p. 1-9.
24. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y. Fine-grained data access control systems with user accountability in cloud computing. IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom); Indianapolis, IN. 2010. p. 89–96.
25. Xu L, Wu X, Zhang X. CL-PRE: A Certificate less proxy re-encryption scheme for secure data sharing with public cloud. ASIACCS; 2012. p. 1-10.