A Survey on Cloud Group Data sharing using Key-Aggregate Searchable Encryption (KASE) Scheme

S.Saikrishna[1] & S.Vineela Krishna[2]

[1]M-Tech Dept. C.S.E Gudlavalleru Engineering College Gudlavalleru, Andhra Pradesh 521356, India Mail Id: - saikrish205@gmail.com

[2]Assistant professor Dept. C.S.E Gudlavalleru Engineering College Gudlavalleru, Andhra Pradesh 521356, India Mail Id: - vineela.suri@gmail.com

Abstract

Cloud computing technology is widely used so that the data can be outsourced on cloud can accessed facilely. Different users can apportion that data through different virtual machines which present on single physical machine. But the thing is utilizer don't have control over the outsourced data. The main purport is to apportion data securely among users. The cloud accommodation provider and users Authentication is compulsory to ascertain no loss or leak of user's data in cloud. Privacy preserving in cloud is consequential. Cryptography avails the data owner to apportion the data to the requested utilizer in safe way. For that the data owner encrypts the data and uploads on server. The encryption and decryption keys may be different or same for different set of data. For decrypting the required data only the set of decryption keys are shared. Here a public key cryptosystems which engenders a ciphertext which is of constant size. The difference is one can amass a set of secret keys and make them as minuscule size as a single key with holding the same ability of all the keys that are composed in a group as aggregate key.

Keywords: Cloud Provider, Authentication, Privacy in Cloud, Cryptography, Encrypt, Cyphertext, Aggregate Key.

1. Introduction

Nowadays, many immensely colossal scale and diminutive scale organizations outsource their astronomically immense-scale data storage to the cloud for preserving the cost in maintaining their storage. With cloud storage accommodation, the members of an organization can apportion data with other members facilely by uploading their data to the cloud. Examples of organizations which may benefit from this cloud storage and sharing accommodation are numerous, such as international enterprises with many employees around the world, collaborative web application providers with a sizably voluminous utilizer base, or institutions dealing with sizably voluminous data, healthcare researchers, patients, etc. While the economic benefits brought by outsourcing data can be captivating, security is one of the most consequential factors that obstruct its wide development. Since data operations in the cloud are not transparent to users, and security breaches or inopportune practices are prevalent and inevitably ineluctable, users still have an immensely colossal concern about the security of their data on the cloud, especially on data integrity.

Cloud is gaining popularity recently. In professional settings, we optically discern the hike in demand for data outsourcing, which avail in the strategic management of utilizable data. It is withal utilized as a main technology abaft many online accommodations for personal applications and some other applications.

Nowadays, it is very facile to apply for free accounts for email, file sharing and/or remote access, with storage size more than 25GB (or a few dollars for more than 1TB). Together with the modern technology, users can access virtually all of their files and emails by a mobile phone in any corner of the world. Storing data in cloud reduce the jeopardy.

Cryptography is the method of storing and transmitting data in a form that only those intended for it can read and process the required data. It is technique of for fending information by encrypting the data it into an unreadable format utilizing some encryption algorithm. Cryptography is an efficacious way of bulwarking sensitive information that is to be stored on media or transmitted through network communication paths. The main goal of cryptography is that to obnubilate information from unauthorized individuals like intruders or hackers. Hackers now a day can hack most of the cryptography algorithms and the information can be revealed if the assailant has enough time and resources to hack the data. So a more authentic goal of cryptography is to decrypting the data to be arduous. Considering data privacy, rely on the server to enforce the access control after authentication, if there is any unexpected privilege escalation will expose all data which is sensitive. In a shared- cloud computing environment, things become even worse because Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Regarding availability of files, there is lot of cryptographic schemes which sanctions a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owner's anonymity. Likewise, cloud users probably will not hold the vigorous notion that the cloud server is doing a good job in terms of confidentiality.

2. Related Work

Sharing data or information among users is a paramount functionality in cloud storage. In [1] author Proposed incipient public-key cryptosystems that engender constant-size ciphertexts such that efficient delegations of decryption rights for any set of ciphertexts are possible. The one can aggregate any set of secret keys and make them as compact as a single key, but the puissance of all the keys being aggregated. This compact aggregate key can be conveniently sent to others or be stored in a keenly intellective card with very inhibited secure storage. How to a decryption key more potent in the sense that it sanctions decryption of multiple ciphertexts, without incrementing its size. A variant of public key encryption "key aggregate cryptosystem" in which the users inscribe a data utilizing an identifier of ciphertext called class which denotes the ciphertexts are further categorized into different classes. The key data owner of the data holds a master-secret key, to extract secret keys for different classes of the ciphertext from the cloud. More consequential is that the extracted key can be an aggregate key which is as condense as a secret key for a single class, but amalgamates the puissance of many such keys that is the decryption power for any subset of ciphertext classes. Implementation of the KAC system in C with the pairing-predicated cryptography (PBC) Library.

Existing System:

Surmise that Alice puts all her private files on Dropbox(cloud), and she does not optate to expose her files to everyone. Due to sundry data leakage possibility Alice cannot feel assuaged by just relying on the privacy aegis mechanisms provided by Dropbox, so she encrypts all the files utilizing her own keys afore uploading. One day, Alice's friend, Bob, asks her to apportion the files surmounted all these years which Bob appeared in. Alice can then utilize the portion function of Dropbox, but the quandary now is how to delegate the decryption rights for these files to Bob. A possible option Alice can optate is to securely send Bob the secret keys involved. Naturally, there are two extreme ways for her under the traditional encryption paradigm:

- Alice encrypts all files with a single encryption key and gives Bob the corresponding secret key directly.
- Alice encrypts files with distinct keys and sends Bob the corresponding secret keys.

Conspicuously, the first method is inadequate since all un-culled data may be withal leaked to Bob. For the second method; there are practical concerns on efficiency. The number of such keys is as many as the number of the shared files, verbally express, a thousand. Transferring these secret keys inherently requires a secure channel, and storing these keys requires rather expensive secure storage. The costs and involutions involved generally increase with the number of the decryption keys to be shared. In short, it is very heftily ponderous and costly to do that.

Proposed System:

We solve this quandary by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but additionally under an identifier of cipher text called class. That signifies the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be habituated to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the potency of many such keys, i.e., the decryption power for any subset of ciphertext classes.

With our solution, Alice can simply send Bob a single aggregate key via a secure e-mail. Bob can download the encrypted files from Alice's Dropbox space and then utilize this aggregate key to decrypt these encrypted files.

3. Implementation

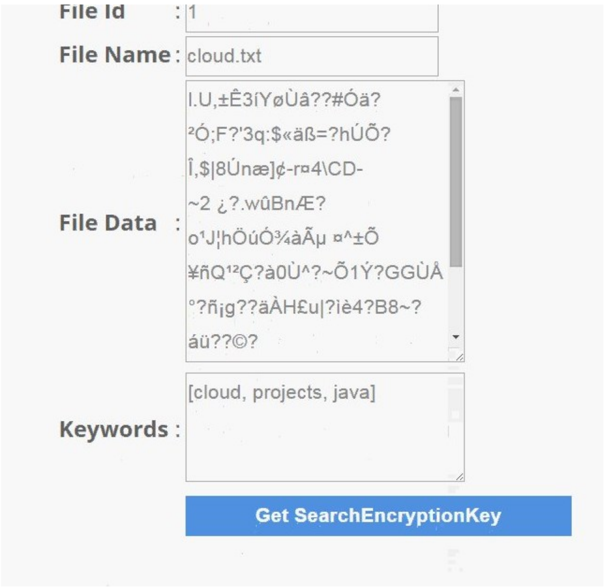
a) **Key Gen:** executed by the data owner to randomly generate a public/master-secret key pair(pk; msk).

b) **Encrypt (pk; i;m):** executed by anyone who wants to encrypt data. On input a public-key pk, an index i denoting the ciphertext class, and a message m, it outputs a ciphertext C.

c) **Extract (msk; S):** executed by the data owner for delegating the decrypting power for a certain set of ciphertext classes to a delegatee. On input the mastersecret key msk and a set S of indices corresponding to different classes, it outputs the aggregate key for set S denoted by KS.

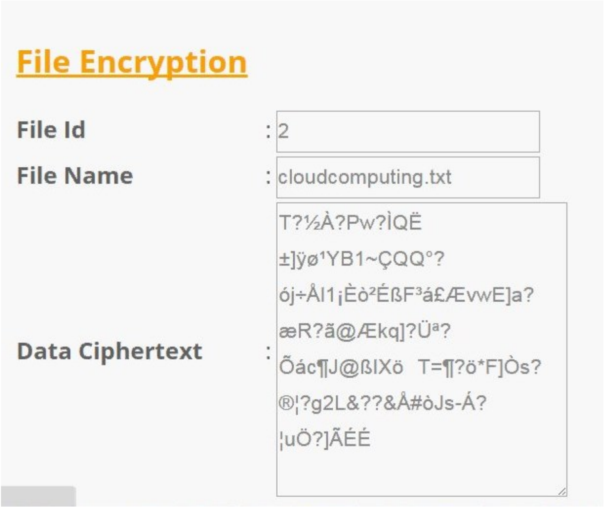
d) **Decrypt (KS; S; i; C):** executed by a delegatee who received an aggregate key KS generated by Extract. On input KS, the set S, an index i denoting the

4. Experimental results



```
File Id   : 1
File Name : cloud.txt
File Data :
I.U,±Ê3íYøÙâ??#Óä?
²Ó;F?'3q:$«äß=?hÚÕ?
Î,$|8Únæ]¢-r¤4\CD-
~2 ¿?.wûBnÆ?
o¹J¦hÖúÓ¾àÃµ ¤^±Õ
¥ñQ¹²Ç?à0Ù^?~Õ1Ý?GGÙÅ
°?ñ¡g??äÀH£u|?ìè4?B8~?
áü??©?
Keywords  :
[cloud, projects, java]
```

Fig 1: File Upload with Encryption Format.



File Encryption

```
File Id         : 2
File Name       : cloudcomputing.txt
Data Ciphertext :
T?½À?Pw?ÌQË
±]ÿø¹YB1~ÇQQ°?
ój÷ÅI1¡Èò²ÉßF³á£ÆvwE]a?
æR?ã@Ækq]?Üª?
Õác¶J@ßIXö  T=¶?ö*F]Òs?
®¦?g2L&??&Å#òJs-Á?
¦uÖ?]ÃÉÉ
```

Fig 2: File Encryption with Cipher text.

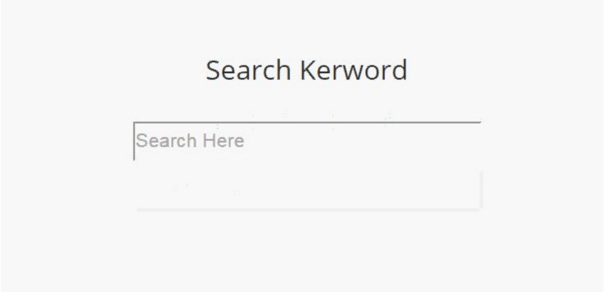


Fig 3: Search for Keywords.

5. Conclusion

In this paper, literature survey on key aggregate cryptosystem was auxiliary to grasp the technique and the way the techniques area unit developed to apportion cognizance among users in cloud. To apportion erudition flexibly is paramount factor in cloud computing. Users relish to transfer their cognizance on cloud and among consummately different users. Outsourcing of erudition to server could lead to leak the personal erudition of utilizer to everybody. Coding could be a one solution that provides to apportion culled erudition with desired candidate. Sharing of cryptography keys in secure method plays vital role. Public -key cryptosystems provides delegation of secret keys for plenarily different ciphertext categories in cloud storage. The delegate gets firmly associate amalgamation key of constant size. It'sneeded to keep enough range of cipher texts categories as they increment expeditious and the ciphertext categories area unitfinite that's the circumscription.

6. References

1. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" ,IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.

2. Cloud Storage "IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.

3. Reza Curtmola and Osama Khan Randal Burns, "Robust Remote Data Checking" ,Proceedings of the 4th ACM international workshop on Storage security and survivability PAGES63-68 ACM 978-1-60558-299-3.

4. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps",Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.

5. Melissa Chase and Sherman S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption",Pages 121-130 ACM New York, NY, USA ©2009 978-1-60558-894-0. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage",ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

6. Qian Wang ,Kui Ren, Wenjing Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", Parallel and Distributed Systems, IEEE Transactions on Volume:22 , Issue: 5 Page(s):847 – 859.

7. Giuseppe Ateniese , Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner ,Zachary Peterson and Dawn Song, "Provable Data Possession at Untrusted Stores",Proceeding CCS '07 Proceedings of the 14th ACM conference on Computer and communications security Pages 598-609.

8. Mehul A. Shah Ram Swaminathan and Mary Baker, " Privacy-Preserving Audit and Extraction of Digital Contents",HP Labs Technical Report No. HPL-2008-32.

9. Ari Juels1 and Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files" , Proceeding CCS '07 Proceedings of the 14th ACM conference on Computer and communications security Pages 584-597.