IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 1, Ver. III (Jan.-Feb. 2017), PP 37-41
www.iosrjournals.org

Secure Data Sharing and Search in Cloud Based Data Using Authoritywise Dynamically Generated Aggregate Key

Chetna Waykole[1], Prof.D.D.Patil[2]
ME Student, Shri Sant Gadge Baba college of Engineering & Technology, Bhusawal, North Maharashtra University, India
Assistant Professor & Head of the Computer Department, Shri Sant Gadge Baba college of Engineering & Technology, Bhusawal, North Maharashtra University, India

Abstract: *The Data sharing is an important functionality in cloud storage. We describe new public key crypto systems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. Ensuring the security of cloud computing is second major factor and dealing with because of service availability failure the single cloud providers demonstrated less famous failure and possibility malicious insiders in the single cloud. A movement towards Multi-Clouds, In other words "Inter-Clouds" or "Cloud-Of-Clouds" as emerged recently. This works aim to reduce security risk and better flexibility and efficiency to the user. Multi-cloud environment has ability to reduce the security risks as well as it can ensure the security and reliability.*

Keywords: *Cloud Storage, Data Sharing, Key Aggregate Encryption, Multi-cloud infrastructure.*

I. Introduction

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, with storage size more than 25GB (or a few dollars for more than 1TB). Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any corner of the world. Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Data in a target VM could be stolen by instantiating another VM co-resident with the target one. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing 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 owners anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality. A cryptographic solution, with proven security re-lied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff. These users are motivated to encrypt their data with their own keys before uploading them to the server. Data sharing is an important functionality in cloud storage. For example, bloggers can let their friends view a subset of their private pictures; an enterprise may grant her employees access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server.

II. Related Work

We proposed Multi-cloud strategy. Multi-cloud strategy is the use of two or more cloud to store the data. Cloud computing is becoming an important thing to deal with, in many organizations around the world. It provides many benefits like 1. cost, 2.Reliability and 3.Ease in retrieval of data. Security in cloud computing is gaining more and more importance as organizations often store sensitive data and important data on the cloud. Security of data in cloud is an issue which should be focused carefully. Customers do not want to lose their sensitive data due to malicious insiders and hackers in the cloud. In addition, the loss of service availability has caused many problems for a large number of recently. Data intrusion technique create many problems for the users of cloud computing. The other issues such as data theft, data lost should be overcome to provide better services to the customers. It is observed that the research into the use of inter cloud providers to maintain security has received less attention from the research community than has the use of single clouds. Multi-cloud

environment has ability to reduce the security risks as well as it can ensure the security and reliability. Multi-cloud strategy minimize the risk of:-

1. service availability failure
2. Loss and corruption of data
3. loss of privacy
4. vender lock-in
5. the possibility of malicious insiders in the single cloud.

III. Proposed Approach

The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) Finally, any user with an aggregate key can decrypt any ciphertext provided that the ciphertexts class is contained in the aggregate key via Decrypt.

The key aggregation property is especially useful when we expect the delegation to be efficient and flexible. The schemes enable a content provider to share her data in a confidential and selective way, with a fixed and small ciphertext expansion, by distributing to each authorized user a single and small aggregate key. Here, we describe the main idea of data sharing in cloud storage using KAC, illustrated in Fig. Suppose Suhas wants to share her data m1;m2;.....;m on the server. He first performs Setup1; n to get param and execute KeyGen to get the public/mastersecret key pair pk; msk. The system parameter param and public-key pk can be made public and master-secret key msk should be kept secret by Suhas. Anyone (including Suhas herself) can then encrypt each mi by Ci Encrypt pk; i; mi. The encrypted data are uploaded to the server. With param and pk, people who cooperate with Suhas can update Suhass data on the server. Once Suhas is willing to share a set S of her data with a friend Pritam, He can compute the aggregate key KS for Pritam by performing Extract msk; S. Since KS is just a constant-size key, it is easy to be sent to Pritam via a secure e-mail. After obtaining the aggregate key, Pritam can download the data he is authorized to access. That is, for each i 2 S, Pritam downloads Ci (and some needed values in param) from the server. With the aggregate key KS, Pritam can decrypt each Ci by Decrypt KS; S; i; Ci for each i 2 S.

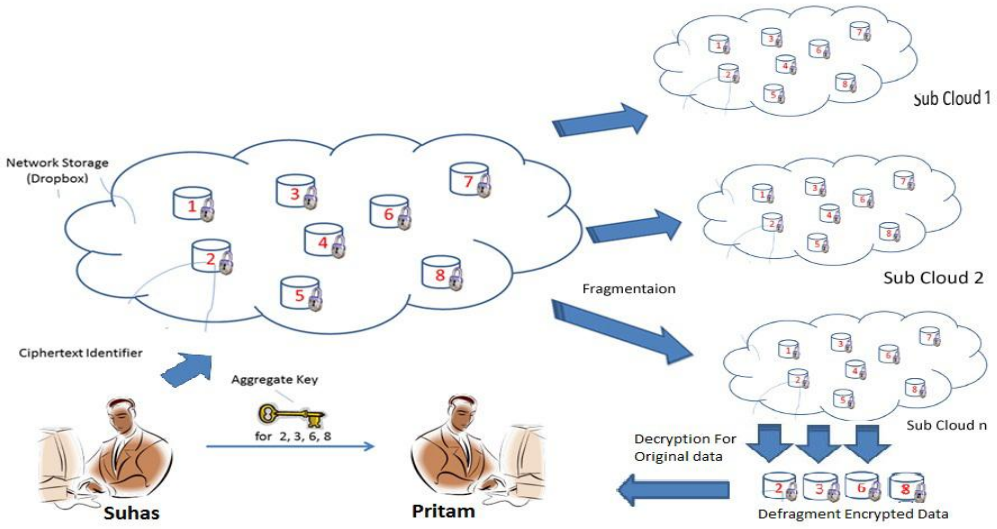

Fig.1 System Architecture

3.1 Algorithm:

1. Setup (1, n) The data owner establishes public system parameter via Setup. On input of a security level parameter 1 and number of cipher text classs n, it outputs the public system parameter param
2. KeyGen It is for generation of public or master key secret pair.
3. Encrypt (pk, i, m) It is executed by data owner and for message m and index i, it computes the cipher text as C.
4. Extract (msk, S) It is executed by data owner for delegating the decrypting power for a certain set of ciphertext classes and it outputs the aggregate key for set S denoted by Ks.
5. Decrypt (Ks,S,i,C)) When an appointee receives aggregate key Ks as exhibited by the previous step, it can execute Decrypt. The decrypted original message m is displayed on entering Ks, S, i, and C, if and only if I belongs to the set S

3.2 Aggregate Key Generation Algorithm

1. First Setup Data
2. All the key like k1,k2 ,k3 are in string format then it will converted into bytes using Byte Encoder.
3. Then every string converted in string to number like, K1=12356, K2=56423, K3=35641
4. All set key combine then it can give separator for that different key like,12356 0 56423 0 35641 here no value consider as separator.
5. secrete key i.e, S.
6. key convolution : we are use the quadratic equation, f(x)=(n1x + n2x + S)/n1=94,n2/66 here the x is consider as 2 or any number.
7. Then it calculation getting the number like 254631 then that no again converted in String.
8. Display String format of key.

3.3 Implementation Details:

AES Encryption Algorithm:

- After Files will be uploaded by a registered user will encrypted by using Improved AES Encryption technique then file will be stored on cloud.
- First we process file using base64 encoder to convert it in byte array.
- Then this byte array will be encrypted using AES technique.

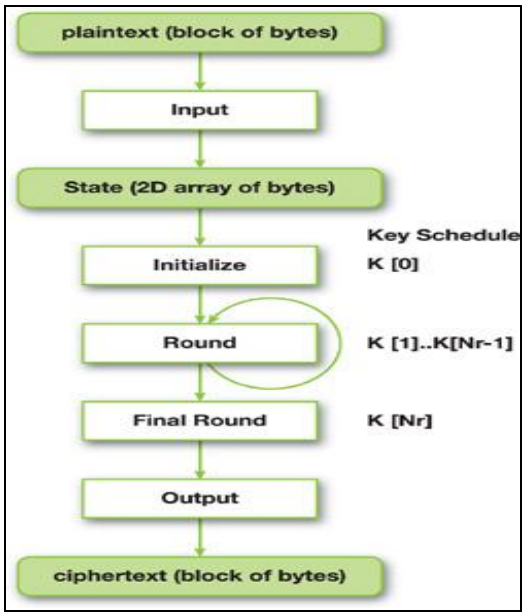

Fig. 2 AES Encryption Algorithm

IV. Result

	Userid	Nasme	Contactno	Email	City	State	Country
☑	19	Ksb Prit	7249494489	ksb.prit@gmail.com	Nashik	Maharashatra	India
☑	18	pise sagar	8793160748	pise.sagar1@gmail.com	Kopargaon	MH	India
☑	17	yogesh khalkar	7350128284	yogeshwarkhalkar01@gmail.com	yeola	Maharashatra	India
☐	16	Nik Shinde	9423571557	suhya25@gmail.com	Nashik	Maharashatra	India

Fig. 3 User Selection

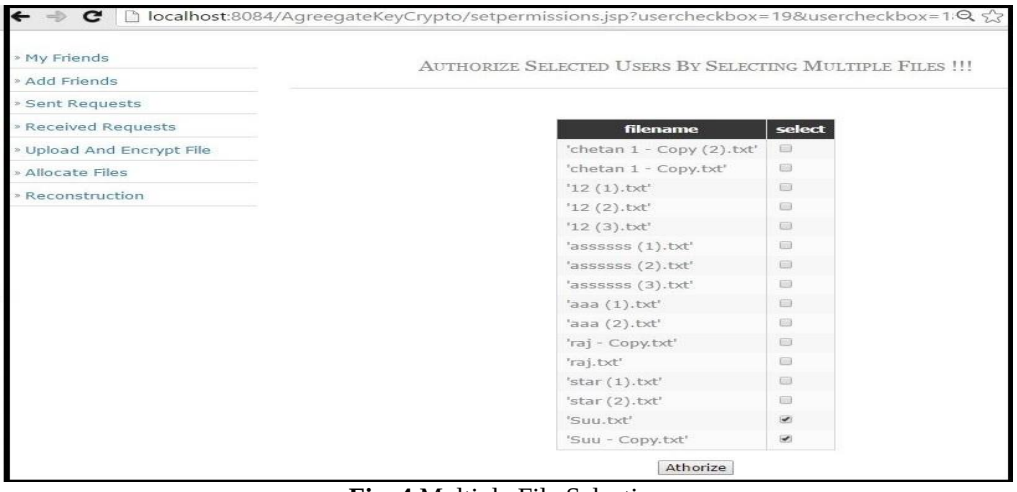

Fig. 4 Multiple File Selection

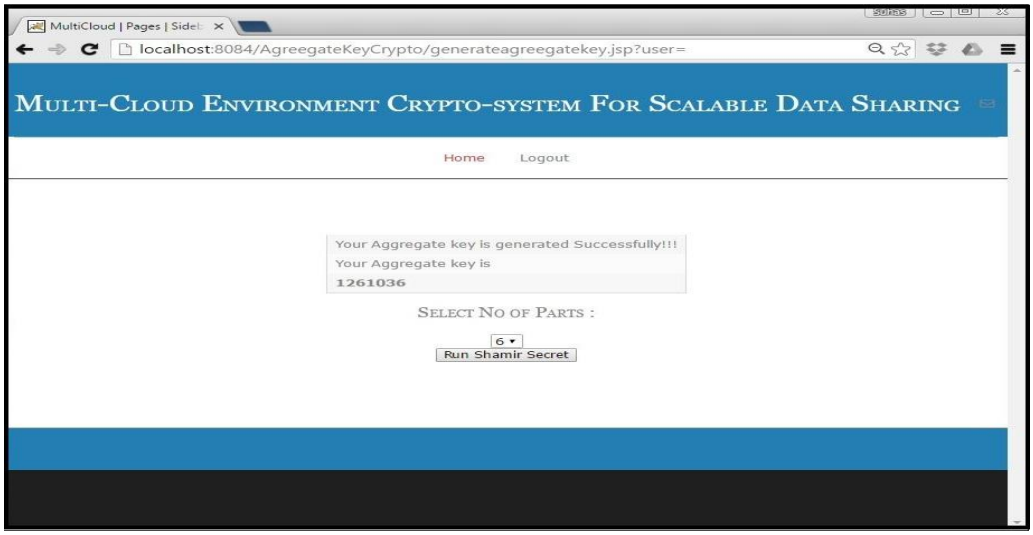

Fig. 5 Aggregate Key Generation

V. Conclusion

In this work we have reviewed three authentication techniques: Attribute based encryption (ABE), Identity Based Encryption (IBE) and Key Aggregate Cryptosystem (KAC). The major concern in ABE is collusion resistance but not compression of secret keys. Definitely, the ciphertext size is not constant. In IBE, random set of identities are not match with our design of key aggregation. Key Aggregate Cryptosystem protects users data privacy by compressing the secret key in public key cryptosystem which supports delegation of secret key for different cipher text classes. For future extension it is necessary to reserve enough cipher texts classes because in cloud cipher texts grows rapidly and the limitation is that bound of the number of maximum cipher text classes. To share data exibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for different ciphertext classes in cloud storage.

VI. Future Work

There are some limitation to the existing system like predefined bound of the number of maximum ciphertext classes and system is prompt to leakage of key. In cloud storage, the number of cipher texts usually grows rapidly. So we have to reserve enough cipher text classes forces the future extension. Otherwise, we need to expand the public-key. Although the parameter can be downloaded with cipher texts, it would be better if its size is independent of the maximum number of ciphertext classes. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

References

[1] F. C. Chang and H. C. Huang, \Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," Inf. Sci., vol. 192, no. 1, pp. 3949, Jun. 2012.
[2] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, \SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security .,ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526543. pp. 173184, 2011.
[3] L. Hardesty, Secure computers arent so secure, \MIT press,"2009,http://www.physorg.com/news176107396.html..
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, \Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,Proc ," 13th ACM Conf. Computer and Comm. Security (CCS 06),pp. 89-98, 2006.
[5] S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, \Practical Leakage- Resilient Identity-Based Encryption from Simple Assumptions ," in Proc. ACM Conf. Com-puter and Comm. Security,pp. 152-161, 2010.
[6] G. Ateniese, A.D. Santis, A.L. Ferrara, and B. Masucci, \Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, ,"J. Cryptology.,vol. 25, no. 2, pp. 243-270, 2012.
[7] F. Guo, Y. Mu, Z. Chen, and L. Xug, \Multi-Identity Single-Key Decryption without Random Oraclesl,",in Proceedings of Information Security and Cryptology (Inscrypt 07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384398.
[8] Vigneshwaran.K 1, Sumithra.S2, Janani.R3 "An Intelligent Tracking System Based on GSM and GPS Using Smartphones" Vol. 4, Issue 5, May 2015.

Biography

Ms. Chetna Waykole is a student in Computer Science Department, college of ShriSant Gadge Baba college of Engineering &Technology, Bhusawal, North Maharashtra University, India. She received Bachelor of Engineering degree in 2012 from JTM college of Engineering, Faizpur, North Maharashtra University, India. Her research interests are in Cloud Computing