ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Review of Various Approaches for Securing Cloud Storage

Kranti M. Chaudhari, Prof. Vilas S. Gaikwad

PG Scholar, Dept. of Computer Engineering, JSPM NTC, Rajarshi Shahu School of Engineering and Research, Narhe, Pune, India

Assistant Professor, Dept. of Computer Engineering, JSPM NTC, Rajarshi Shahu School of Engineering and Research, Narhe, Pune, India

ABSTRACT: Achieving security is the major task considered while sending messages over the network. The science of sending encoded messages or data is known as cryptography. By using cryptography, we can make the message unreadable and thus providing security, privacy and reliability to the confidential data. A system using this technique is called as cryptographic system or cryptosystem which are the only way which allows the user to access the encrypted data and decrypt it for making the data readable. The authorized users can share the authenticated messages with each other. But while working on cloud computing, security has been the major issue and topic of concern. Thus, in this paper we discuss the different security aspects related to the various encryption methods used for data sharing in secure cloud storage.

KEYWORDS: Cloud storage, data sharing, Encryption, Secret keys, Decryption

I. INTRODUCTION

In the upcoming years, the field of cloud computing has gained immense popularity. The method of data outsourcing has been increased these days. The management of corporate data must be assisted with data outsourcing technique. Data outsourcing is been a basic technology used in almost every online services and applications. This technology is easily applied to applications like mails, photographs, file sharing, etc. User around the world can access their files, directories, emails from anywhere, anytime with the use of wireless technology equipped in devices.

Maintaining privacy of the data stored in cloud is very important. Many traditional approaches used for ensuring data privacy depended upon the server to enforce the security policies. The servers would apply access control mechanism after authentication process. The security requirement in a shared-lease cloud computing environment becomes more deficient. Data from diverse users can be organized on separate virtual machines (VMs) but reside on a sole physical machine. The data in a target virtual machine can be compromised and stolen by instantiating other virtual machine that is co-occupant with the target one.

Many cryptographic techniques are proposed for providing availability and security to the shred files. These techniques make use of third-party auditor for checking the availability of files. The third-party auditor carries out the task on behalf of the data owner without compromising the owner’s identity and without leaking the information [1].

The cloud users don’t hold strong belief on the cloud servers providing quality privacy preserving services. A cryptographic solution has found to be more appealing in terms of providing security. When the user is unable to trust the security of the virtual machine and honesty of the technical workforce, they encrypt their data with a set of keys before uploading the data on the cloud storage.

The principal functionality in cloud storage is data sharing. For example, users of blogs can share their pictures with their friends, and an enterprise may allow his employees to access important portion of data. But the

DOI: 10.15680/IJIRCCE.2015. 0309078

demanding problem arises here is how to efficiently share the encrypted data. If we allow the users to download the encrypted data, decrypt it and then again share it with other users, than the cloud storage may lose the basic value. The users can also provide access rights of sharing the data with other people so as the other people can access the data directly from the server openly. It is not trivial for finding an efficient and secure way for sharing the partial data in cloud storage [1].

II. TECHNIQUES FOR SECURE CLOUD STORAGE

1. Cryptographic Keys for a Predefined Hierarchy

The cryptographic key assignment scheme uses tree structure [2] and reduces the expense incurred in storing and managing secret keys as in conventional method. Key provided for a given branch can be used to get the keys of the descendant nodes by using hierarchical tree structure. The issue can be partially solved when one single key can be used for sharing files under same branch. But the other part still remains, when number of keys increases with the number of branches increase. Therefore, it is challenging to create a hierarchy and save number of keys to be given to all individuals simultaneously.

2. Symmetric-Key Encryption with Compact Key

The author Benaloh et al. [3] proposed an encryption scheme that was used for transmitting a large number of keys in a broadcast manner [4]. The erection of this scheme is simple and the process of key derivation of this

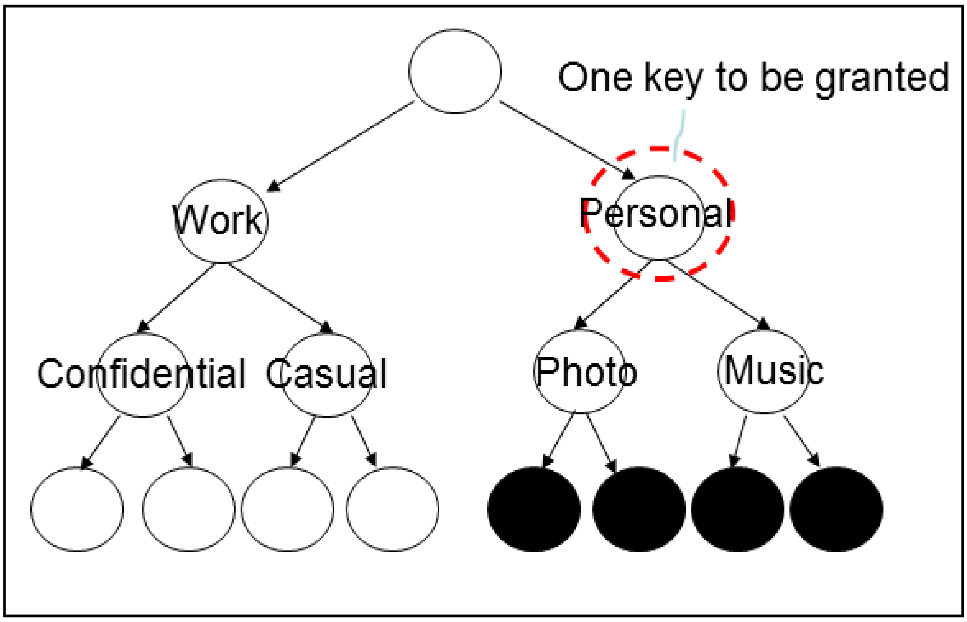

Figure 1.a :Compact key is not always possible for a fixed hierarchy (One key to be granted)

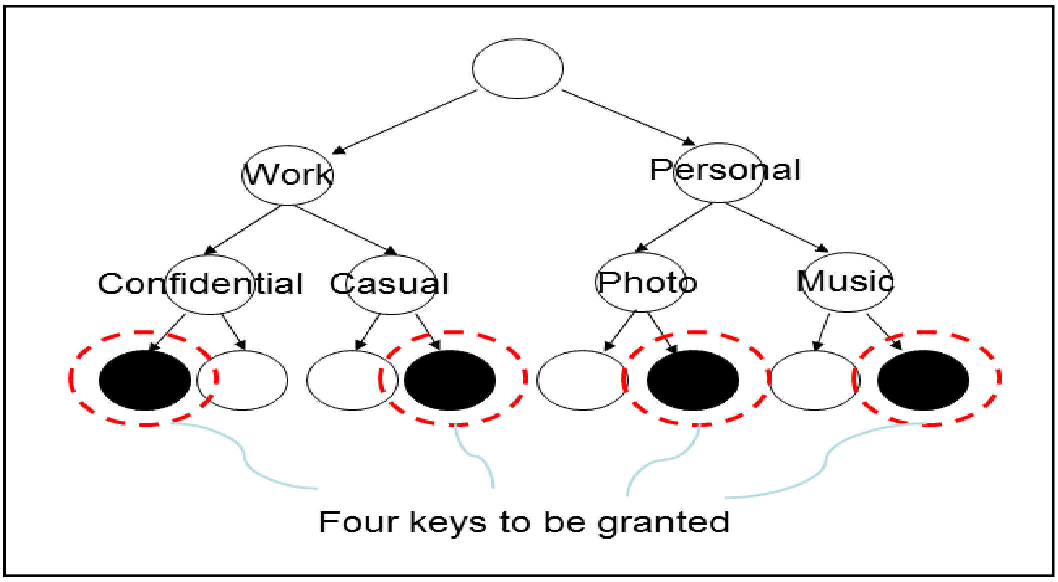

Figure 1.b :Compact key is not always possible for a fixed hierarchy (Four keys to be granted)

scheme is used for creating desirable functionalities we want to achieve. The process of inferring of the key for a certain set of classes is described as follows: A complex modulus is chosen with the values of p and q, where p and q are two large primes. The selection of master secret key is also done randomly. Each and every class is correlated with a distinct prime, and all these prime numbers can be places into the public system parameter. The generation of constant-size key is formed for a set for those who have been delegated the access rights for S'. Instead this design is for the symmetric-key setting. The user that provides the contents also needs to get the corresponding secret keys for encrypting the data, which is not suitable for many applications. This method aims at generating a secret value rather than a pair of public/secret keys. But, the process of applying this idea to public-key encryption scheme is uncertain. Finally, we note that there are schemes trying to reduce the key size for achieving authentication in symmetric-key encryption, e.g., [5]. However, this scheme is not concerned with the process of sharing decryption powers.

Consider the example in tree format in Figure 1, Each node in a tree presents a secret key, where leaf node represents individual cipher text classes. Filled circles represent the keys for the classes to be delegated and circles circumvented by dotted lines represent the keys to be granted. Note that every key of the non-leaf node can derive the keys of its descendant nodes.

3. Compact Key in Identity-Based Encryption (IBE)

In the Identity-Base encryption scheme, there is a party i.e. a trusted party called private key generator used. This trusted party is responsible for holding a master-secret key and distributing a secret key to each and every user according to their identity. In order to encrypt the data, the encryption algorithm takes the public parameter and user's identity for the process of encryption of message [6]. On the other hand at the receiver side, the decryption of the message is done by the secret key owned by the receiver. Some researchers tried to assemble IBW with key aggregation method. But this attempt resulted with the size of O(n) where n stands for the number of secret keys. This expense of O(n) results for both, ciphertext and for the public parameter and hence, increases the cost of storing and transmitting the ciphertext.

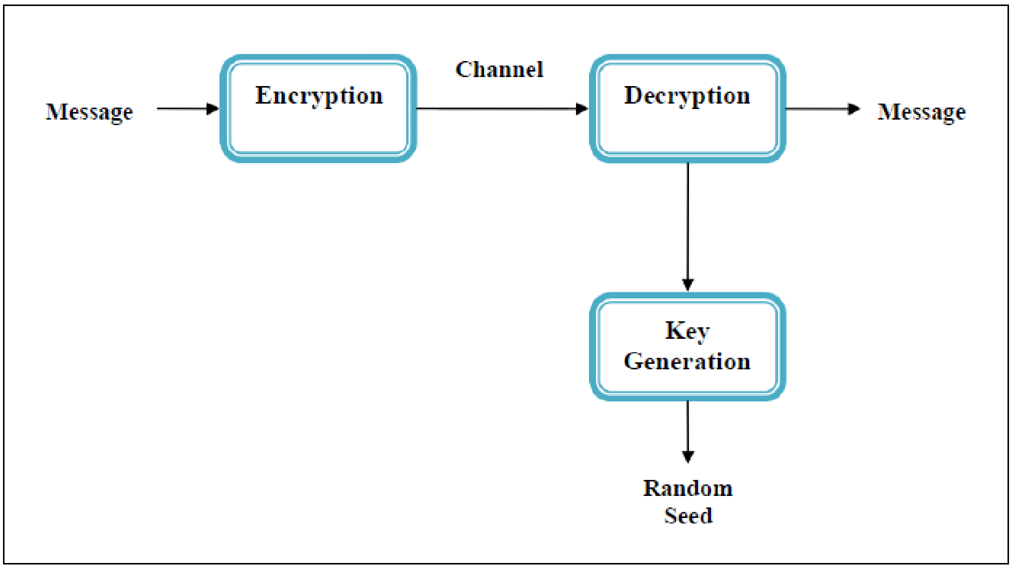

Figure 2: Identity based Cryptosystem (Identity-based cryptosystems and signature schemes)

4. Attribute-based encryption (ABE)

The ciphertext in Attribute-based encryption (ABE) scheme is always associated with an attribute [7] [8]. The holder of the master-secret key can pull out a secret key from a policy associated with an attribute so that the ciphertext can be decrypted by the secret key if the associated attribute keeps to the policy. For example, if the secret key for the policy is given as (1 ∨ 3 ∨ 6 ∨ 8), then it is possible to decrypt the ciphertext tagged with class 1, 3, 6 or 8. But there are certain concerns related to this ABE scheme. The major concern is the collision-resistance without the compactness of the secret keys. But indeed, the size of the key often increases along with the number of attributes it encompasses, or when the size of the ciphertext is not constant [9].

5. Proxy re-encryption (PRE)

The scheme is useful to emissary the unscrambling control of some ciphertexts without sending the secret key to the delegatee, is known as proxy re-encryption (PRE) [10]. A PRE plan permits Alice to delegate to the proxy server the capacity to change over the ciphertexts encoded under her open key into ones for Bob. PRE is surely understood to have various applications including cryptographic record framework. By and by, Alice needs to believe the proxy that it just changes over ciphertexts as per her guideline, which is the thing that we need to keep away from at the primary spot. Far more atrocious, if the proxy plots with Bob, some type of Alice's secret key can be recovered which can unscramble Alice's (convertible) ciphertexts without Bob's further offer assistance. That likewise implies that the change key of proxy ought to be very much secured. Utilizing PRE just moves the secure key stockpiling requirement from the delegatee to the proxy. It is accordingly undesirable to let the proxy reside in the capacity server. That will likewise be awkward since each decoding requires separate association with the proxy.

6. Key Aggregate Cryptosystem (KAC)

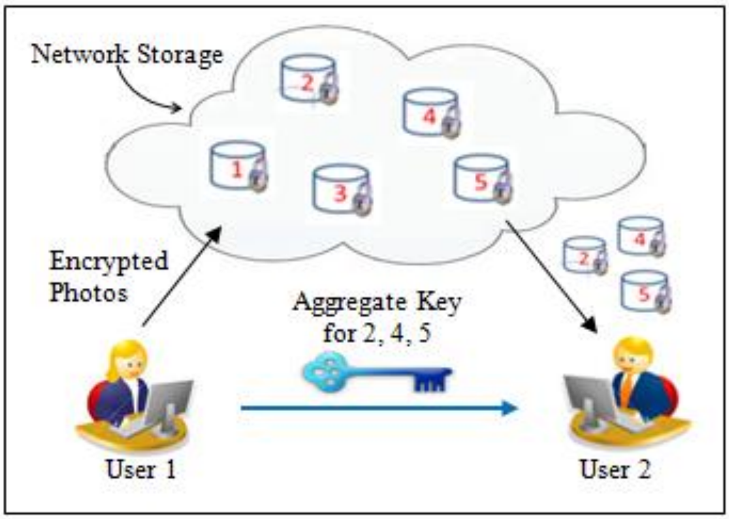

Figure 3: User1 shares files 2,4,5 with User2 by sending him a single aggregate key

In KAC[11] author proposed a new public encryption cryptosystem in which user can encrypt the message with public key and classes. In this system classes categorized according to the subject. Instead of sending separate decryption key for each file user send the aggregate key. Aggregate key is similar to the single key but aggregate power of many keys. However the aggregate key is depend on the maximum number of cyphertext classes. In cloud environment , the number of ciphertexts usually raises swiftly. A limitation is handled by the system –Aggregate Key Expansion (AKE) [12]. In AKE system the Cyphertext classes created dynamically. The system create aggregate key, is independent of number of cyphertext classes. The size of Decryption key ,Aggregate key is constant.

Table 1: Techniques for secure cloud storage

Different Schemes	**Cipher text Size**	**Decryption Key Size**	**Encryption type**
Key assignment schemes[2]	Constant	Non-constant	Symmetric or public-key
Symmetric-key encryption with compact key [3]	Constant	Constant	Symmetric key
IBE with compact key[6]	Non-constant	Constant	Public key
Attribute based encryption[7]	Constant	Non-constant	Public key
KAC[10]	Constant	Constant	Public Key

III. CONCLUSION

Providing privacy to the user’s data is the major task carried out in cloud storage systems. Assigning the secret keys to several cipher text classes is done in the process of public-key cryptosystem where the secret keys are compressed. The compression of the secret keys makes a aggregate key with constant size. Generally the number of cipher texts grows rapidly in cloud storage with no restrictions, thus, we need to accumulate enough cipher text classes or make the aggregate key which is not dependent on the number of cypher text classes, is more practical.

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] S.G. Akl and P.D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans.Computer Systems,vol. 1, no. 3, pp. 239-248, 1983.

[3] 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.

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

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

[6] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption:How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575,pp. 392-406, 2007.

[7] 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.

[8] 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.

[9] 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.

[10]G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1–30, 2006.

[11] Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEETransactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[12] Kranti M. Chaudhari, Prof. Vilas S. Gaikwad, "Compliant Data Sharing With Aggregate Key Development in Cloud Environment" in IJIRCCE, Volume 3, Issue 7, July 2015.