Data Security using KAC for Sharing Scalable Data

Mr.Sunil S.khatal[1], Mr. B.S. Chunchore[2] , Mr. K.S.Kahate[3]

[1] *ME 2nd year ,Computer Engineering,SPCOE ,Dumberwadi,Otur*
[2] *Assistant Profecer,Computer Engineering ,SPCOE,Dumberwadi,Otur*
[3]*ME Co-Ordinator,Computer Engineering,Dumberwadi,Otur*

ABSTRACT

Sharing any information is an important function in cloud storage. This system prove how to share data securely, e_ciently, and exibly with others in cloud storage. And access the private information in cloud with the help of secrete key.They describe new technique i.e. public-key cryptosystems for secure communication between data owner and third party user also .Public key cryptosystem produce constant-size cipher texts such that e_cient delegation of decryption rights for any set of ciphertexts are possible. In the key aggregate cryptosystem 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. This compact aggregate key can be kindly sent to others for data access it increase data personally and security. In innovation cryptographic key generation techniques, this technique possesses unique cryptographic key aggregate cryptosystem which is helpful for secure data and privacy preserving key generation process.And propose access level policy structure such as Public and Private Access level to improve the data access mechanism in the data sharing mechanism process. Governments, military, business and Private Citizens all over the world now use stegnography and cryptography for security and privacy purpose to secure sharing information in the cloud storage . Computer forensics and another forensic methods such as digital forensics ,alternate data storage forensic etc. are used more popular in recently world due to advantages in computer systems and Authentication as well as investigation purpose in computer communication.

Keyword: - Cloud storage, data sharing, key-aggregate cryptosystem, Encryption,Decription

1. INTRODUCTION

A] Cloud Storage:

Cloud computing is widely increasing technology; data can be saved on cloud remotely and can have access to huge applications with quality services which are shared among customers. As increase in outsourcing of data the cloud computing serves does the management of data [1].

Its exible and cost optimizing characteristic motivates the end user as well as enterprises to store the data on cloud. The insider attack is one of security concern which needs to be focused. Cloud Service provider need to make sure whether audits are held for users who have physical access to the server. As cloud service provider stores the data of different users on same server it is possible that users private data is leaked to others.The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol [2].

It is necessary to make sure that the data integrity without compromising the anonymity of the data user. To ensure the integrity the user can verify meta data on their data, upload and verify [3].

2. PROPOSED WORK

In key-aggregate cryptosystem (KAC), users encrypt a message not only under a public-key, but also under an identifier of cipher text called class. That means the cipher texts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used 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 power of many such keys, i.e., the decryption power for any subset of cipher text classes. example, Alice can send Bob a single aggregate key through a secure e-mail. Bob can download the

encrypted photos from Alices Box.com space and then use this aggregate key to decrypt these encrypted data. The sizes of cipher text, public-key, master-secret key and aggregate key in KAC schemes are all of constant size.

3. SYSTEM FRAMEWORK

In this system to make data sharing secure and leak resilient. Decryption key is made more and more powerful so that it can decrypt multiple cipher texts. At the same time an Intrusion detection system monitors data exchange between two hosts and ensures that these are trusted hosts.

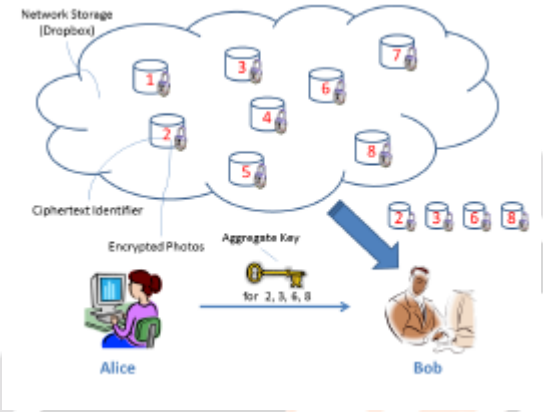

Fig 1.Data Sharing

Specifically, the problem statement is to generate a constant size decryption key by data owner. This decryption key should have power to decrypt multiple cipher text. The decryption key is aggregate key which encompasses the power of all secret keys. Aggregate decryption key will prevent leakage of unwanted data. While sharing aggregate decryption key all the hosts in communication work in collaboration to find out the suspicious activity in their re spective sub-networks. The solution proposed is to use a public-key encryption technique which is called as Key Aggregate Encryption (KAE).

Key Aggregate Cryptosystem (KAC)[1], data owner encrypts a message using public-key, as well as under cipher text identifiers. Cipher texts are categorized into different classes. The key owner generates public/master key pair. Master-secret is used to extract secret keys for different cipher text classes. The
extracted aggregate key is as compact as a secret key for a single cipher text class, but combines the power of many such keys, i.e., the decryption power for multiple cipher texts which are subset of a single cipher text classes.

In this, Alice can send Bob a single aggregate key via a secure e-mail or chats. Bob downloads the encrypted photos from Alices picasa space and then use this aggregate key to decrypt these encrypted photos. The sizes of cipher text, public-key, master-secret key and aggregate key in KAC schemes are all of constant size. While key exchange process each host works as intrusion detection system. Distributed hash table is maintained by each host which records the IP addresses of their sub-network. If some suspicious activity happens all other hosts are notified about this and key exchange is stopped.

A] Symmetric-Key Encryption with Compact Key

An encryption scheme which is originally proposed for concisely transmitting large number of keys in broadcast scenario. The construction is simple and brifly review its key derivation process here for a concrete description of what are the desirable properties to achieve. The derivation of the key for a set of classes (which is a subset of all possible cipher text classes) is as follows. A composite modulus is chosen where p and q are two large random primes. A master secret key is chosen at random. Each class is associated with a distinct prime. All these prime numbers can be put in the public system parameter. A constant-size key for set can be generated. For those who have been delegated the access rights for Scan be generated.

However, it is designed for the symmetric-key setting instead. The content provider needs to get the corresponding secret keys to encrypt data, which is not suitable for many applications. Because method is used to generate a secret value rather than a pair of public/secret keys, it is unclear how to apply this idea for public-key

encryption scheme. Finally, note that there are schemes which try to reduce the key size for achieving authentication in symmetric-key encryption. However, sharing of decryption power is not a concern in these schemes.

B]Attribute-Based Encryption

Attribute-based encryption (ABE) allows each cipher text to be associated with an attribute, and the master-secret key holder can extract a secret key for a policy of these attributes so that a cipher text can be decrypted by this key if its associated attribute conforms to the policy. For example, with the
secret key for the policy (1 3 6 8),one can decrypt cipher text tagged with class 1, 3, 6 or 8. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys. Indeed, the size of the key often increases linearly with the number of attributes it encompasses, or the cipher text-size is
not constant. In this system every cipher text is labeled by the encrypt or with a group of de- scriptive attributes. Every non public secret is related to AN access structure that species which sort of cipher texts the key will decode. And tend to decision such a theme a Key-Policy Attribute-Based secret writing (KP-ABE), since the access structure is per the non-public key, whereas the cipher texts area unit
merely labeled with a group of descriptive attributes. Cloud computing is visualized as architecture for succeeding generation. It has many facilities though have risks of attacker who can access the data or leak the users identity. While setting a cloud users and service providers authentication is necessary. The issue arises whether loud service provider or user is not compromised. The data will leak if any one of them in compromised. The cloud should be simple, preserving the privacy and also maintaining users identity.

4. CONCLUSIONS

Steganography is the method of hiding any secret information or any personal information like password, unique key text and image, audio behind original cover file in cloud storage. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio- video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, and select any frame of video and audio for hiding our secret
data. Suitable algorithm such as LSB is used for image steganography suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. This system focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

5. ACKNOWLEDGEMENT

We thankful to Teacher, Friends and Department of Computer Engineering for their constant guidelines and support. We also thankful college staff for providing the required infrastructure and support.

6. REFERENCES

[1]Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng,, Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage, in Proceedings of IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014
[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.
[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Trans.Computers, vol. 62, no. 2, pp. 362375, 2013.
[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, Storing Shared Dataon the Cloud via Security-Mediator, in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
[5] G. C. Chick and S. E. Tavares, Flexible Access Control with Master Keys, in Proceedings of Advances in Cryptology - CRYPTO 89, ser. LNCS, vol. 435. Springer, 1989, pp. 316322.

[6] 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. 8998.
[7] Y. Sun and K. J. R. Liu, Scalable Hierarchical Access Control in Secure Group Communications, in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM 04). IEEE, 2004.
[8] 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. 213229.
[9] M. Chase and S. S. M. Chow, Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, in CM Conference on Computer and Communications Security, 2009, pp. 121130.
[10] CERT Coordination Center, Module 2 - Internet Security Overview, 2003.
[11] M. E. Locasto, J. J. Parekh, A. D. Keromytis, S. J. Stolfo, Towards Collaborative Security and P2P Intrusion Detection, 2005 IEEE Workshop on IAS, June 2005.
[12] B. Y. Zhao, J. D. Kubiatowicz, and A. D. Joseph, Tapestry: An infrastructure for faulttolerant wide-area location and routing, Technical Report CSD-01-1141, University of California, Berkeley, 2000.