International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-5, May 2015

"Key Aggregate Cryptosystem for Data Sharing In Cloud"

Shilpa V Chavan, Sharada G Kulkarni

***Abstract*— In its most simple description, cloud computing is taking services ("cloudservices") and sending them to the customer outside an organization firewall on shared systems. Instead of your hard drive like pendrive applications and services are accessed via the internet. This article shows how to securely, efficiently, and flexibly store data with others in cloud storage,because Securely Storing data in cloud has become security concern. This can achieved using Cryptography, it is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. A public-key cryptosystem is described which generate a constant or fixed size ciphertext so that to transfer the decryption rules for number of ciphertext. The new thing is that one can merge any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. The compact aggregated key can be easily sent to others or be stored in any storage device or smart card with very limited secure storage.**

***Index Terms*— Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.**

I. INTRODUCTION

Cloud Storage:

Cloud computing is acquiring popularity, now a days we see there is a rise in demand for data out sourcing in enterprise setting ,it renders companies to devour computer resources to use just like electricity, pay per use that is there is no need to build and maintain computing infrastructures . Several attractive services are provided for the welfare of businesses and end users by cloud computing. Self serving provision, elasticity and pay per use, no installation, no cost of purchasing hardware and software are some of the main benefits of cloud computing. Cloud computing services can be private, public or hybrid. Cloud service providers are like , IBM, Google, Amazon, Microsoft etc. Cloud storage is used as a core technology of many online services for personal applications like gmail. Recently it has become easy to apply for free account creation for file transfer, photo album, remote access and facebook. The major issue in cloud are privacy of data and cloud security.

The users divulge data with a secure authorization and authentication in the cloud. It is required to divulge the data in order to share the sensible information in a gauranteed and secured environment. Imparting data airs several problems such as data misuse, privacy and uncontrolled propagation of data. The data in cloud is saved as a shared pool and ruptures in data are the major development to security. One of the most used techniques to securely storage data on confided servers is cryptography access control, where sensitive data is encrypted before sending to the authorized use along with decryption keys. Without the decryption keys no one can decrypt the encrypted data.

Cryptography schemes for data storage

A proven cryptographic solution, is more attractive and relies on number-theoretic assumptions,. When the user is not satisfied with trusting the security of the VM or the honesty of the technical staff. Such users are encouraged and motivated to encrypt their data using their own keys before uploading the data into the server. Cryptography is the way of storing and sharing the data in the form of scrambled information,which can only be accessed by the authenticated user . It is the process of securing the message by encoding it into a scambled data which will be in an unreadable format. The basic goal of cryptography is the ability to send the information to the receiver in a way that prevents attackers from accessing it. This information is stored on cloud through the internet.

Encryption is a technique of converting original message called clear text or plaintext, into a unreadable format that cannot be understood by an attacker, which is called as ciphertext. The user can't access the original message until the ciphertext is decrypted. Similarly Decryption is the reverse technique of encryption which includes converting the ciphertext into plaintext or original message

Types of Encryption keys

Encryption keys are of two types — symmetric key(single key encryption) and asymmetric (public) key.

•Symmetric Key Encryption

In symmetric encryption, only one key is used for both encryption and decryption process; obviously, this is not always desirable.

Asymmetric Key Encryption

By contrast, in public-key encryption the encryption key and decryption key are different. For example,every employee can upload encrypted data on the cloud storage server without the knowing the company's master-secret key. Especially, these secret keys are usually stored in the tamper-proof memory, which is relatively expensive.

II. LITERATURE SURVEY

Cloud computing is visualized as architecture for succeeding generation. It has many facilities though have a risk 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 [1]

Shilpa V chavan, Mtech in computer science and engineering ,KLS Gogte Institute of technology.

Sharada G Kulkarni, Asst. Prof at KLS Gogte Institute of technology

The flexible use of cloud storage for user is a need as it is seams accessing data locally though that is present at remote side. It is important to inspect the data set on the cloud. So it is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA). TPA is also beneficial for cloud service provider. It checks the correctness of the outsourced data. TPA should be able to do public auditability, storage correctness, privacy preserving, Batch auditing with minimum communication and computation overhead [2].

There are many cloud users who wants to upload there data without providing much personal details to other users. The anonymity of the user is to be preserved so that not to reveal the identity of data owner. Provable data possession (PDP) uses similar demonstrating marks to reduce computation on server, and network traffic. PDA ensures the data present on cloud which is un-trusted is original without accessing it. Security mediator (SEM) is approach allows the user to preserve the anonymity. Users are meant to upload all their data to SEM so that the SEM is not able to understand the data although it's going to generate the verification on data. As the users are signed at SEM it should not know the identity of uploader [3].

Another way for sharing encrypted data is Attribute-Based Encryption (ABE). It is likely to encrypt the data with attributes which are equivalent to users attribute rather than only encrypting each part of data. In ABE attributes description is considered as set so that only a particular key which is matched with attribute can decrypt the ciphertext. The user key and the attribute are matched if it matches it can decrypt a particular ciphertext. When there are k attributes are overlay among the ciphertext and a private key the decryption is granted [5].

A multi group key management accomplishes a hierarchical access control by applying an integrated key graph also handling the group keys for different users with multiple access authorities. Centralized key management plan uses tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it. It accomplishes an integrated key graph for every user [6].

Identity-based encryption (IBE) is a vital primary thing of identity bases cryptography. The public key of user contains distinct information of user's identity. The key can be textual value or domain name, etc. IDE is used to deploy the public key infrastructure. The identity of the user is used as identity string for public key encryption. A trusted party called private key generator (PKG) in IBE which has the master secret key and gives secret key to users according to the user identity. The data owner collaborate the public value and the identity of user to encrypt the data. The ciphertext is decrypted using secret key [7].

In a multi attribute-authorities numbers of attributes are analyzed regarding the decryption key and the user must get a particular key related to the attribute while decrypting a message. The decryption keys are allocated independently to users those who have attribute identity without interaction between each other. Multi-authority attribute-based encryption allows real time deployment of attribute based privileges as different attributes are issued by different authorities. The attribute authorities ensure the honesty of the user privilege so the confidentiality is maintained by central authority [8]

III. KEY-AGGREGATE ENCRYPTION

The proposed system design an efficient public-key encryption scheme which supports flexible allocation. In this scheme any subset of the cipher texts (produced by the encryption scheme) is decrypt by a constant-size decryption key (generated by the proprietor of the master-secret key). We solve this problem by introducing a special type of public-key encryption called key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher text called **class**. Such that cipher texts are further categorized into different classes. The owner of the key holds a master-secret called Master secret key [5].

The master-secret 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, such that the decryption power for any subset of cipher text classes. By this solution, Alice can simply send Bob a single aggregate key via a secure channel like email. Bob can download the encrypted photos from Alice's Drop box space and then use this aggregate key to decrypt these encrypted photographs. The scenario is depicted in Figure 1.

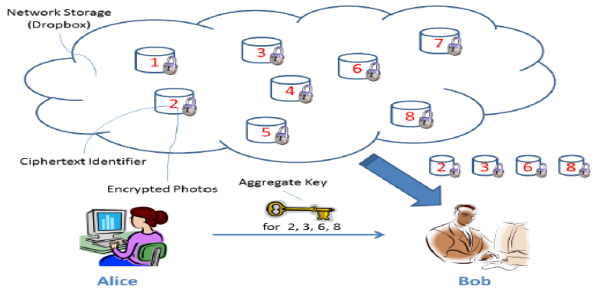

Fig. 1. Alice shares files with identifiers 2, 3, 6 and 8 with Bob by sending him a single aggregate key.

A key aggregate encryption has five polynomial-time algorithms as

Setup Phase

The data owner executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter.

KeyGen Phase

This phase is executed by data owner to generate the public or the master key pair (pk, msk).

Encrypt Phase

This phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m, i), the encryption algorithm takes input as public parameters pk, a message m, and i denoting ciphertext class. The algorithm encrypts message m and produces a ciphertext C such that only a user that has a set of attributes that satisfies the access structure is able to decrypt the message.

- Input= public key pk, an index i, and message m
- Output = ciphertext C.

Extract Phase

This is executed by the data owner for delegating the decrypting power for a certain set of ciphertext classes to a delegate.

 Input = master-secret key mk and a set S of indices corresponding to different classes
 Outputs = aggregate key for set S denoted by kS.

Decrypt Phase

This is executed by the candidate who has the decryption authorities. Decrypt (kS, S, i, C), the decryption algorithm takes input as public parameters pk, a ciphertext C, i denoting ciphertext classes for a set S of attributes.
 Input = kS and the set S, where index i = ciphertext class
 Outputs = m if i element of S.

Advantages:-

- A single decryption key is more powerful it allows decryption of multiple cipher texts, without increasing its size.
- The size of cipher text, master-secret key, aggregate key and public-key in KAC schemes are all kept constant.
- KAC scheme is flexible there is no special relation is required between the classes.
- Efficient data sharing scheme is a "canonical application of KAC ".
- The aggregate key is secure ,efficient and flexible.
- The schemes enables a content provider to share the data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing a single ,compact, small,constant sized aggregate key to each authorized user.
- With the aggregate key the delegacy of decryption can be implemented efficiently.
- Number of cipher text classes is large.
- It is easy to manage key
- Authorised Member can view their messages.

Extensive performance and rigorous security analysis, can be provided.

	Decryption key size	Ciphertext size	Encryption type
Key assignment schemes for a predefined hierarchy (e.g., [7])	most likely non-constant (depends on the hierarchy)	constant	symmetric or public-key
Symmetric-key encryption with Compact Key (e.g., [8])	constant	constant	symmetric-key
IBE with Compact Key (e.g., [9])	constant	non-constant	public-key
Attribute-Based Encryption (e.g., [10])	non-constant	constant	public-key
KAC	constant	constant	public-key

TABLE 1
Comparisons between our basic KAC scheme and other related schemes

IV. Conclusion

Overall an "aggregate key Cryptosystem" which produces secured and effective constant size private key is produced by means of derivations of different cipher text classes. Proposed approach proves to be more secure and efficient cryptographic scheme in which we have an effective derivation of secret key generation and key management for the outsourced Cloud data.

REFERENCES

[1] 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. 526–543.

[2] L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.

[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. 362–375, 2013.

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[5] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

[7] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[8] 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.

[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[10] 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.

Shilpa V chavan, Mtech in computer science and engineering ,KLS Gogte Institute of technology
Sharada G Kulkarni, Asst. Prof at KLS Gogte Institute of technology