Review on: Multiple Data Sharing Using Key Aggregate Cryptosystem in Cloud Storage

Neha Pawar[1], Saad Meer Ali[2], Sayali Jaid[3], Priyanka Sengar[4]
[1, 2, 3, 4] BE-GHRIET, Pune University

Abstract- *As the development of new wireless technology is growing data sharing becomes a vital part in cloud storage. Sharing of data efficiently and in secured manner is of great importance. In this article, a cryptographic technique having secret keys can be aggregated to a compact single key by encompassing the power of all keys. This enables the secret key holder to release a fixed size aggregate key for any choices of cipher text set in cloud storage. A less secured smart card can be used to store the generated compact single key.*

Keywords- cloud storage, cryptographic technique, data sharing, cipher text, aggregate key

I. INTRODUCTION

With the rapid development in technology, the use of cloud storage (CS) has grown in recent times. Each and every organization, company has a CS to backup the data for security reasons. The information is stored in cloud so that it can be accessed directly by the employee/company as and whenever required. However the crucial or important data stored on cloud has the chance of leakage. Innovation and administrations in CS, is standard for clients to influence CS administrations to exchange data to others in a companion circle, e.g., Dropbox, Google Drive and Ali Cloud.

In order to share this information it should be securely transmitted. To avoid leakage of data while sharing various methods are available such as: security mediator, oruta etc. They all use third party auditor to handle cloud data.

Cryptography is the content's scrambling of the data, e.g. content, image, sound, feature to make the information indistinguishable irrespective of transmission or capacity is known as Encryption. Furthermore, primary part of cryptography is to deal with information security from intruders. The inverse technique of obtaining back the original information from scrambled data is known as Decryption, which restores the first information. Scrambling of information at CS uses both symmetric-key and unbalanced key for calculations. Cloud computing is developing as a huge stage for putting away, keeping up and sharing information. Interest for keeping data secured as well as its storage capacity is expanding in all sphere, whether clients are from corporate, military, IT associations etc.

Information protection has turned into a vital affinity towards the CS clients. Clients don't compromise their privacy.

Security is a noteworthy concern, while sharing the information. Considering an example of clinic administration framework where specialists and patients are getting to the cloud for information sharing about illness and medicines. The patient information is transferred by specialist on the cloud, yet he is unhappy with the security principles of cloud. Therefore, the specialist chose to encode all his data and later transfer the records unto the cloud. Following three days one of the patients asked for the data applicable to him. The unscrambling key will be appointed to the patient do effectively obtain the original information

To overcome above obstacles while sharing the information, a technique is used to "Encode all information with disparate encryption key and send just single decoding key. This single unscrambling key has the capacity to decode the right content. The promising element of decoding key is that, it is total of the whole unscrambling key yet it stays minimal in size as a single key. The hosts included in correspondence ought to have the capacity to screen the security breaks, henceforth an interruption location framework ought to be given".

The unscrambling key is assigned safely on a secured channel. Little size of decoding key is coveted, as we can utilize it for advanced cells, remote sensors, and savvy cards and so on.

II. LITERATURE REVIEW

Table 1. Literature survey

PAPER	DESCRIPTION	ADVANTAGES	DISADVANTAGES
Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage (2014)	Introduction to Key Aggregation Cryptosystem.	1.It is more secure. 2.Decryption key is sent via a secure channel and kept secret	The predefined bound of the number of maximum cipher-text classes.
"Privacy-Preserving Public Auditing for Secure Cloud Storage(2013)	It is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA).It checks the correctness of the outsourced data.	1.Public audit-ability, 2.Storage 3.Correctness, 4.Privacy preserving,	1.No guarantee of data integrity. 2.No guarantee of availability
"Storing Shared Data on the Cloud via Security-Mediator" (2013)	Security mediator (SEM) is approach allows the user to preserve the anonymity.	1.Public Verifiability 2.Anonymity. 3.Data Privacy.	1.Does not provide the high security. 2.Unable to preserve identity of data owners to public verifiers
"SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment" (2012)	Preserving the privacy and also maintaining users identity	1.Digital Identity Management, 2.Interoperability, 3.Delegation, 4.Privacy, 5.Unlinkability	1. To create a fuzzy-IBE where the attributes come from multiple authorities
"Shared and Search able encrypted data for untrusted servers" (2011)	To securely encrypt keywords, keyword encryption scheme is also obtained by proxy encryption scheme and proxy cryptography.	1.Does not require a trusted data server. 2.System has a unique set of keys.	1. It Track unnecessary network. 2.The number of user increase then difficulty may arise in key management process
"Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing" (2010)	This system provides the solution for the problem of fine-grainedness, scalability, and data confidentiality of access control in cloud storage. Attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption techniques.	1.User access privilege confidentiality. 2.User secret key accountability.	1.Exchanging the key. 2.Third party can attack the key easily.
"Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing" (2010)	SP scheme is used provide security and trusted evidences for data forensics in cloud computing. Provable security techniques are used to check the validity of the security.	1.Information confidentiality 2.Anonymous authentication 3.Provenance tracking.	1.Lack of control 2.Security and privacy. 3.Higher operational cost. 4.Reliability
"Improving Privacy and Security in Multi-Authority Attribute-Based Encryption" (2009)	Multi-authority attribute-based encryption allows real time deployment of attribute based privileges as different attributes are issued by different authorities.	1.Removes the trusted central authority. 2.Protects the users' privacy	1.Difficult handling for bulky users due to load n PKG. 2.Central Authority is required.

"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data" (2006)	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.	1.Supports delegation of private keys	1.Key escrow problem.
"Practical techniques for searches on encrypted data" (2000)	The proofs of security with the help proposed cryptographic scheme. It supports searching functionality without losing the confidentiality of the data.	1.They are provably secure; 2.They support controlled and hidden search and query isolation. 3.They are simple and fast	1. No space and communication over- using an index is that storing and updating the index can be of substantial overhead.

III. SCOPE OF WORK

Data sharing in cloud storage is of great importance as it allows bloggers to let their friends view a part of their personal images; an organization may grant access to a portion of sensitive information to their employees. The major problem is to effectively share the encrypted data. However, users can download the encrypted information from the CS, decrypt them, and then send them to others for sharing. Users should be able to confine the access rights of the sharing data to others so that they can access these data from the server directly. However, finding an efficient and secure way to share partial data in CS is not important.

IV. PROPOSED SYSTEM

To eliminate the leakage/conning/ hacking of information, more secured method is used for encryption and decryption. Here Alice encrypts files with distinct public-keys, but only sends Bob a single (fixed-size) decryption key. As the decryption key should be sent via a secured channel and kept secret, small key size is always desirable. For example, we cannot use large storage for decryption keys in the resource-constraint devices like smart phones, smart cards or wireless sensor nodes.

Especially, these secret keys are usually stored in the tamper-proof memory, which is relatively expensive. The present research efforts mainly focus on minimizing the communication requirements (such as bandwidth, rounds of communication) like aggregate signature. However, not much has been done about the key itself.

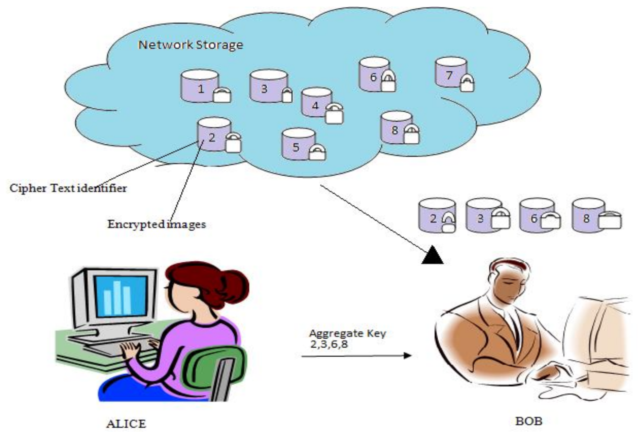

Figure1. System Architecture

Advantages of Proposed System:

- It is more secure
- Decryption key is sent via a secure channel and kept secret
- It is an efficient public-key encryption scheme which supports flexible delegation

1. MODULE:

A key aggregate encryption has five polynomial-time algorithms: Setup Phase, Key Gen Phase, Encrypt Phase, Extract Phase, Decrypt Phase.

A. Setup Phase

The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

B. Encrypt Phase

Encrypt (PK,M, A). The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a cipher-text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

C. Key Gen Phase

Key Generation (MK,S). The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK

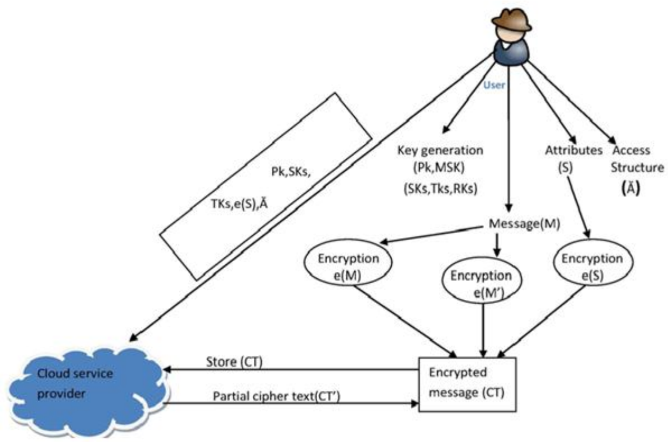

Figure2.

D. Extract Phase

This is executed by the data owner for delegating the decrypting power for a certain set of cipher-text 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

E. Decrypt Phase

Decrypt (PK, CT, SK). The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private-key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

V. CONCLUSIONS

Protection of user's data privacy is a key-concern of CS. With the help of mathematical tools, cryptographic schemes becomes more flexible. In this article, we consider how to "aggregate" secret keys in public-key cryptosystems (single key). This helps assignment of secret keys to different ciphertext classes in CS. The representative to whom aggregate key is handed over always gets an aggregate key of fized size. Intrusion detection system is unified with the aggregated key which has the potential to improve detection accuracy, to the problem of how to effectively share information between users.

ACKNOWLEDGMENT

This is an opportunity to express my gratitude towards everyone who suggested and helped us in this Review paper. I wish devote my sincere thanks to our guide Prof. Shubhangi Suryawanshi, and also provide gratitude to GHRIET, Pune for providing framework to accomplish our work.

REFERENCES

[1] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member, Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[2] 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.

[3] 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.

[4] 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

[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 Dedicatedto Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.8.

[6] 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.

[7] 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.

[8] 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.

[9] 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. 89–9

[10] 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.