Secure sharing of personal data on cloud Using key aggregation and Cryptography

Amulya Sulake V[1], Ashwini J V[2], Kavya N Kumar[3], Rakshitha M[4]

[1,2,3,4] *B.E Dept of CSE ,NIE, Mysuru, Karnataka, India*

Abstract - *Cloud innovation is exceptionally productive and helpful in display new mechanical time, where a man utilizes the web and the remote servers to give and keep up information and in addition applications. Such applications thusly can be utilized by the end clients through the cloud correspondences with no establishment. Distributed storage is getting astoundingly popular these days. The two significant workplaces that cloud give are data amassing and data sharing. An ensured data sharing in cloud is a basic issue. This paper goes with an idea of making the data sharing secure and discharge adaptable. Distributed storage ought to have the capacity to store and offer information safely, proficiently, and adaptably with others in distributed storage.*

We propose a basic, proficient, and freely irrefutable way to deal with guarantee cloud information security while sharing between various clients. The flow work centers around decreasing key-estimate by creating a solitary total key, however does not give accessible encryption, which is required for adaptable information sharing. Our proposed plot tends to this issue by empowering a owner to circulate a solitary consistent size total key to an information client for sharing an expansive number of records and afterward client presents a solitary total trapdoor to the cloud for seeking over approved encoded archives.

Key Words: **Personal data, secure data sharing, key-aggregate encryption, searchable, cloud storage.**

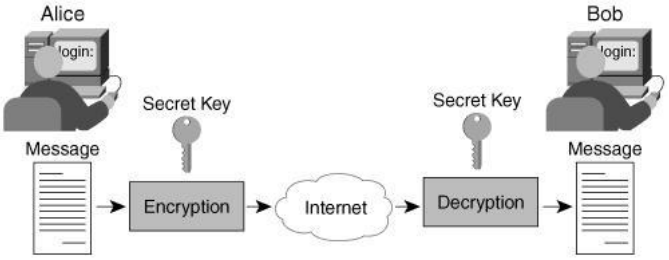
1. INTRODUCTION

Cloud systems can be used for providing data sharing functionality because of its ubiquity, convenient and on demand access facilities. So, it is used by owners to store their data on the cloud. The cloud, because of its data outsourcing feature has many privacy and security issues. So owners encrypt their sensitive data before outsourcing it to the cloud and hence the data remains secure against the cloud provider and other malicious users. But data encryption makes searching and retrieving only the selected data containing given keywords a challenging task.

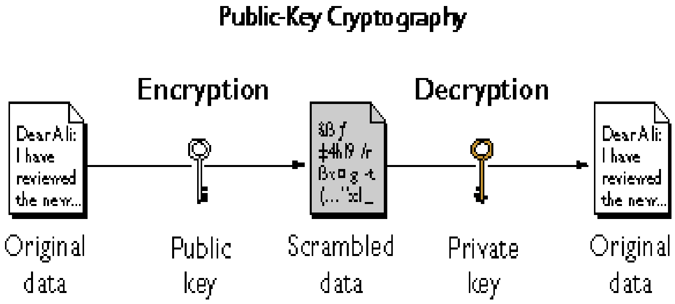
The common information in cloud servers, in any case, generally contains users‟ delicate data, for example, individual profile, monetary information, wellbeing records, and so forth and should be very much secured. As the responsibility for information is isolated from the organization of them, the cloud servers may move users‟ information to other cloud servers in outsourcing or offer them in cloud seeking. Along these lines, it turns into a major test to secure the protection of those mutual information in cloud, particularly in cross-cloud and huge information condition. Keeping in mind the end goal to address this difficulty, it is important to outline an extensive answer for help client characterized approval period and to give fine-grained get to control amid this period.

While sharing data, security is an important concern. Usually we put stock in pariah server for giving security. Requesting is sent to the server for approval, has getting to fogs are constrained to trust the pariah for their security.

Cryptography of information is fundamentally the mistake the substance of the information, for example, content, picture, sound, video et cetera to make the information unintelligible, imperceptible or useless amid transmission of information. It is known as named Encryption. Fundamental point of cryptography framework is to secure information from assailant. In the meantime decoding is correct inverse procedure of getting back the first information from scrambled information, which restore the first information. To encode information at distributed storage, both symmetric and unbalanced key age calculations are utilized. Symmetric-key calculations are calculations for cryptography that utilization the same cryptographic keys for both encryption of plaintext and unscrambling of ciphertext. The keys might be indistinguishable or there might be a straightforward change to go between the two keys. The keys, practically speaking, speak to a common mystery between at least two gatherings that can be utilized to keep up a private data interface.



Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used for encryption. This prerequisite that the two gatherings approach the mystery key is one of the principle disadvantages of symmetric key encryption, in contrast with open key encryption.



2. RELATED WORK

As data privacy and security is the biggest obstacle in the wide adoption of cloud services in a modern health care environment [4], [5], many researchers have contributed to this area. This section reviews several categories of existing literature works.

A PRE scheme allows data owners to delegate to the proxy the ability to convert the cipher texts encrypted under his public-key into ones for data users. But this scheme requires the data owner to trust the proxy that it only converts cipher texts according to his instruction. If the proxy colludes with data users, some form of the data owner's secret key can be recovered which can decrypt data owner's cipher texts. In addition to this, proxy suffers from too many encryption and decryption operations, which increase computational overhead [1].

Chu et al. [1] developed a scheme to allow encrypting a set of documents with different keys, but be decrypted with a single aggregate key. This scheme is based on a public key cryptosystem and takes into account cipher text class during encryption. The scheme [1] enables efficient delegation of decryption rights for any set of cipher texts using a single aggregate key and is the main inspiration of our work. But it does not support keyword search over the encrypted data which is required to achieve secure and selective data sharing in the cloud.

Leng et al. [4] proposed a solution that enables patients to enforce fine-grained access control. Patients use Conditional Proxy Re-encryption to provide data users with write privileges for PHRs. When data users finished updating the authorized PHRs, they signed the PHRs with the signature key of the PHR owner and it is therefore difficult to correctly verify who signed the PHRs.

Cipher Cloud provides a unified cloud encryption gateway with award-winning technology to encrypt sensitive data in real time before it„s sent to the cloud. It also protects enterprise data by using operations-preserving encryption and tokenization in both private and public cloud communication without affecting functionality, usability, or performance.

3. IMPROVED KEY AGGREGATION

Proposed system :

Ensured information partaking in the cloud utilizing the total key for Data proposed work points in sharing the information without exchanging keys for every last record. The deviated encryption standard is utilized for scrambling every one of the information took after by open key encryption. The end client can get to their information utilizing their private key and the Global mystery key which is exchanged amid the validation procedure. Despite the fact that the Global mystery key is hacked amid transmission, malignant assailant can't get the information since it can be decoded just by utilizing a private key. Keys require not be exchanged for every single document, information will be encoded utilizing a Global mystery key. So the information will be sheltered at remote place. The customers who require the information will get to the information utilizing their private key.

Architecture:

Presenting an extraordinary kind of open key encryption which we call key-total cryptosystem (KAC). In KAC, clients scramble a message under an open key, as well as under an identifier of ciphertext called class. The key proprietor holds an ace mystery called master secret key, which can be utilized to extricate mystery keys for various classes. More importantly, the extract key can be an aggregate key which is 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 ciphertext classes.

Implementation modules:

1. Data Owners & Data User Registration Module:

Owner & Data Users (Doctor/Nurse/Insurance Broker) gets registered to our storage service (With personal information's – Id, Name, Location, Contact, Login Password, etc..)

Generate Master Key for each patient (Generate Asymmetric Keys for Data Users). Store registration information's and key in Amazon Simple DB

2. data Upload Module:

Build Index file for the health record. Index file holds all those keywords provide along with the number of occurrence of each keyword in that health record (Based on Binary Representation). Generate Symmetric File/Document Encryption Key for Health Record (Unique Key for every record derived from Patients Master Key) (Basic Polynomial Equation). Perform Symmetric Key Encryption on the Health Record (AES - Rijndael Algorithm). Upload Encrypted data Record & its associated Index File to Cloud using Amazon S3 Service
Update Amazon Simple DB with Upload Information's

3. Record Sharing Module:

Owner are allowed to selectively share their personal records to respective Data Users (Doctor/Nurse/Insurance Broker). Aggregated Key gets generated for selected records [Lagrange Interpolating Polynomial]. Encrypt Aggregate key with Data Users Public Key, File sharing information & its respective enc. aggregate key are stored at Amazon Simple DB

4. Document Retrieval Module:

Download Enc. Aggregated Key at Data User (Doctor/Nurse/Insurance Broker) Machine based on the selected sharing. Decrypt Enc. Agg. Key with Users Private Key. Data Users are allowed to provide Search Query – Keywords (Single or Multiple) on selected health records sharing. Generate Query Trapdoor. Generated Query Trapdoor is sent to cloud for searching. Calculate Documents Relevance Score using Cosine Similarity Search [Euclidean Dot Product Formula]. Download Records from Amazon S3 Storage. Generate File/Record Decryption Keys from Aggregate Key. Decrypt all encrypted health records using Symmetric Key Algorithm (AES - Rijndael Algorithm)

4.RESULT ANALYSIS

The Initial outcomes acquired for the given security display is broke down thinking about Various Situation. Different encryption procedures are contrasted and their handling time for different document sizes. The chart demonstrates the general assessment of the encryption systems. It unmistakably demonstrates that the proposed calculation works more productively than the other encryption guidelines being looked at.

5.CONCLUSION

Proposed subject secured information sharing utilizing a total key is Involve for preparing vital information. The Data can be safely relieved in Cloud stockpiling utilizing these Aggregate key procedures. Key Asymmetric Encryption Protocol are more Protected than the Key Symmetric Encryption Protocol which utilizes a solitary key on the two sides for transmission of information. Utilizing a solitary Global Secret key is an imperative element of the proposed calculation. This lessens the utilization of different keys sharing between the buyers and consequently guarantees security of the information being alleviated. Notwithstanding being encoded, the information to be alleviated will be protected in the remote place.

REFERENCES

[1] C. Chu, S. Chow, and W. Tzeng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage,” IEEE Transactions on Parallel and Distributed Systems, 2014, 25 (2): 468-477.

[2] P. Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation, January 2007, http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

[3] University of Melbourne, Australia 2005 [3] Q. Zhang and Y. Wang, ”A Centralized Key Management Scheme for Hierarchical Access Control,” in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM 04). IEEE, 2004, pp. 20672071.

[4] Leng, C., Yu, H., Wang, and J., Huang, “Securing Personal Health Records in the Cloud by Enforcing Sticky Policies,” TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.

[5] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” Proc. ACM Workshop Cloud Computing Security (CCSW 09), pp. 103-114, 2009.

[6] Kan Yang and Xiaohua Jia,”An Efficient Dynamic Auditing Protocol for Data Storage in Cloud Computing”, 2012 IEEE Transactions on Parallel and Distributed Systems.

[7] Huiki Xu, Shumin Guo and Keke Chen,”Building Confidential and Efficient Query Services in The Cloud using Data Perturbation”, 2014 IEEE Transactions on Knowledge and Data Engineering, VOL.26,NO.2.