Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 - 6953

A SURVEY PAPER ON KEY AGGREGATE CRYPTO SYSTEM FOR SCALABLE DATA SHARING IN CLOUD STORAGE

Darekar Dnyaneshwar,Ghadge Sagar,Khetmalis Varsha,Choramale Rupali,Prof. Gunaware Nilesh.G.

Department of Computer Engineering, H.S.B.P.V.T.COE Kashti, Tal-Shrigonda, Dist.-Ahemadnagar. India.

Abstract:*Cloud computing is a popular area of research for inventors. And it is very important in data sharing applications. On cloud the data being shared must be secure. The flexibility and the efficiency of the data is depend upon the security parameter. To achieve this purpose we describe new algorithm which depends upon public key cryptography and produce constant size cipher text. These ciphers can be decrypt by using a secret key. This secret key can develop the constant size key known as aggregate key, for selection of flexible choices of ciphers. The other encrypted files except these cipher remain private. We can able to save this aggregate key or can send it to others for further data sharing***.

Keyword:*Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.*

1. INTRODUCTION

Now a day's internet is most widely used in many applications. In that cloud computing has wide scope of area, so that the data can be upload or download from cloud and can accessed easily. Many number of users can access data and share that data through disparate virtual machines but present on single physical machine. But the thing is user don't have physical control over the redistribute data. The need is to share data securely among users. The assistance provider uses various authentication method to avoid the loss and leakage of data on cloud. Affection preserving in cloud is done to make sure that user's identity is not revealed to everyone. Anyone can access large amount of data on cloud as much they want i.e. only selected content can be shared. Cryptography allow the data holder to share the data to in secure way. So user can encrypts data and uploads on server. Disparate encryption keys as well as decryption keys are develop for each bunch data. The encryption and decryption keys may be disparate for disparate set of data. Only those set of decryption keys are shared that the selected data can be decrypted.

This paper propose a public-key cryptosystems which develops constant size cipher text. So that it transfer the decryption rules for number of cipher text. The difference is one can gathera set of secret keys and make them as small size as a single key with holding the same ability of all the keys that are formed in a group. Then develop compact key can be send or stored on the cloud in secure manner. The digital data is stored inside the cloud storage as a logical data pool. These cloud storage providers maintains all the data related operations and these are responsible for keeping the data available, protected and running. Other people uses storage capacity from the providers to store end user, they pay for that. Cloud storage services may be accessed through a web service application programming interface (API),such as cloud desktop storage, a cloud storage gateway or Web content management systems.

2. LITERATURE SURVEY

There were many structures proposed to ensure affection and security is discussed in a number of existing articles. M. Chase and S. S. M. Chow, "Provide Affection and Security in Multi-Authority Attribute-Based Encryption"[9] This paper framework the need for achieving affection and security in the Cloud and also briefly framework the need for secure data sharing in the Cloud. Itarrange a survey on affection and security in the Cloud fixate on how affection as should also take into deliberation Cloud computing and what work can be done to anticipate affection and security breaches of one's personal data in the Cloud. This analyzed aspect that affect managing info. security in Cloud computing.

It analyze the imperative security needs for enterprises to understand the dynamics of info. security in the Cloud.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Affection of Electronic Medical Records,"[10]. This paper uses advertisement encryption which enables a advertisement to transmit encrypted data or info. to a set of users so that only a propose subgroup of users can decrypt the data. Other than above characteristics, it also allows the group monitor to consist of new associate by preserving previously enumerated info. and user decryption secret keys need not be enumerated repeatedly and repeatedly, the Aggregation logic and size of cipher texts are remain unaffected and the group encryption key desire no alteration.

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" [4].This structure uses the slice of data cloud to encrypt or decrypt the data. The authentic data are first divided into a number of slices. When a repudiation occurs, the data holder needs only to fetch one slice, and re-encrypt and re-publish it. The data holder fetch the signature from secure mediator and then it allows user to upload or download the data bygone the cloud.

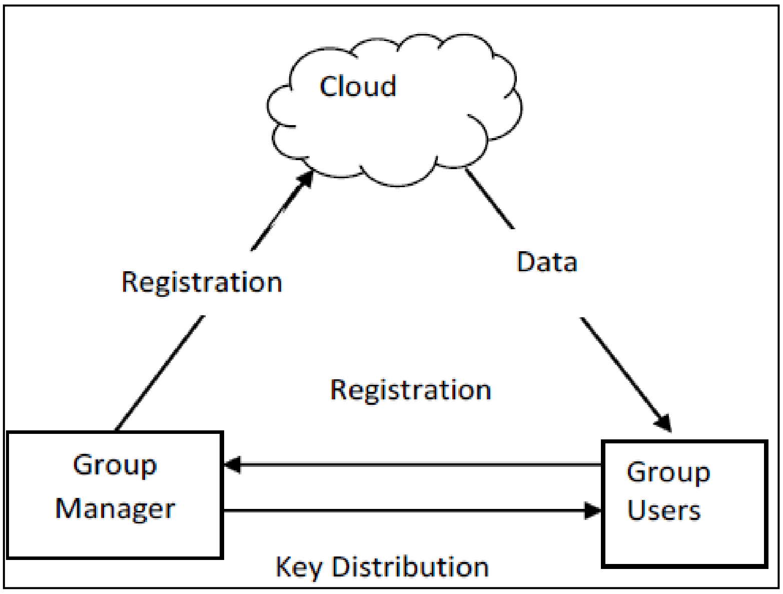

Fig.1: Dynamic advertisement Encryption

3. PROPOSED SYSTEM

In propose structure we are using two keys to encrypt and decrypt the data which are secret key and its aggregate key. This structure is basically design on the basis of key aggregation encryption. The data holder creates the public structure parameter and generates a secrete key which is public key pair. User is responsible for data encryption and he may decides cipher text block associated with the plaintext file which want to be encrypted. The data holder have rights to use the secret key from which he can generate an aggregate key which is use for decryption of a set of cipher text blocks. The both keys can be sent to end user in very secure manner. The authenticated user having an aggregate key can decrypt any block of cipher text.

A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. The data holder provides the public structure parameter via Setup and generates a public/master-secret3 key pair via KeyGen. Encrypt is use for message encrption by anyone who also decides what cipher text class is associated with the plaintext message to be encrypted. This project consist of five algorithms which are used to perform the above operations. These algorithms are as follow:

[1] **Setup:** The data holder executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter. The account is created on the untrusted server for sharing of data. This account is generated by data holder.

[2] **KeyGen:** This phase is executed by data holder to generate the public or the master key pair (pk, msk). This algorithm is use for the generation of public key. The data holder generates a public secrete key to encrypt the data over cloud. He also create an aggregate key to access the block of ciphers of limited size.

[3] **Encrypt:** 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 cipher text class. The algorithm encrypts message m and produces a cipher text C such that only a user that has a set of characteristics that

satisfies the access structure is able to decrypt the message. This algorithm encrypts the data organize by the data holder by using the secrete key. This encrypted data is then share among the cloud.

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

[4] **Extract:** This is executed by the data holder for delegating the decrypting power for a certain set of cipher text classes to a delegate. The aggregate key is use for extracting the particular block of the ciphers from the cipher file. But other encrypted data remains secure.

- Input = master-secret key mk and a set S of indices corresponding to disparate classes
- Outputs = aggregate

[5] **Decrypt:** 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 cipher text C, i denoting cipher text classes for a set S of attributes. The encrypted data is then decrypted by using the same secrete key which is use for encryption

- Input = kS and the set S, where index i = cipher text class
- Outputs = m if i element of S

permissions like read, write etc. to data for security and proceeds to encryption function. It encrypt data using aggregate key that key size is fixed for every user but it can be generated dynamically. Split function uploads the data but before uploading it splits the encrypted data into different parts and stored that part on different clouds. Here, Merge is the function of receiver side, it fetch the data from different clouds like C1,C2,C3…Cn. Decrypt function decrypt the date using the private key and aggregate key and proceed for the further processing.

Extractor checks wheatear that file is accessible to that user or not. In case it accessible then it decrypt from that whole bunch. Fig. 4 shows how the key’s assigned to the separate users. Each user has separate key as per the aggregation cryptosystem. Basically initially grated key is recycled to generate separate user key as per their bits status.In aggregate cryptosystem authentication is imperative for each user in which user login if user login successfully then proceed for further process. User may be sender or receiver.

4. PERFORMANCE ANALISYS

- **Security:** It increases the decryption process performance by using the N2k algorithm it is used to merge the separated file and generate the authentic form of the data. This algorithm does not require all the parts of the separated file. It only required minimum (n/2)+1 parts of the encrypted file.

- **Efficiency:** For encryption, the value e(g1,gn) can be pre-enumerated and put in the structure parameter. It is fast to compute a pairing. Efficient software implementations exist even for sensor nodes.

- **Mobility:** Structure can be handled through wireless network or electronic media with any platform.

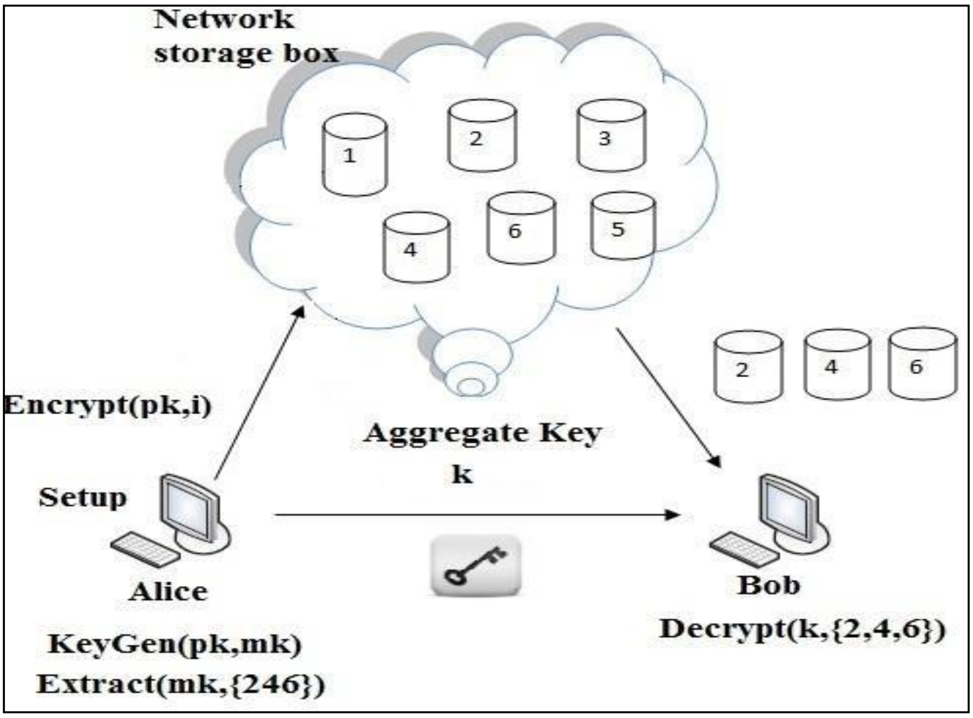

Fig.2: System Architecture

- **Comparison Factor:** For a concrete comparison, we investigate the space need of the tree-based key assignment approach. This is used in the complete sub tree scheme, which is a representative solution to the advertisement encryption problem following the well-known subgroup-cover framework. It employs a static logical key hierarchy, which is materialized with a full binary key tree of height h, and thus can support up to 2h cipher text classes, a selected part of which is intended for an authorized delegate. A comparison of the number of granted keys between three methods is depicted. We can see that if we grant the key one by one, the number of granted keys would be equal to the number of the delegated cipher text classes.

5. CONCLUSION

To share data flexibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among disparate users. The outsourcing of cloud data to server may causes leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for disparate cipher text classes in cloud storage.

Cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this paper, we consider how to “compress” secret keys in public-key cryptosystems which support delegation of secret keys for disparate cipher text classes in cloud storage. The delegate gets securely an aggregate key of constant size. It is required to keep enough number of cipher texts classes as they increase fast and the cipher text classes are bounded that is the limitation.

ACKNOWLEDGMENT

Author would like to take this opportunity to express our profound gratitude and deep regard to my Project Guide Mrs. Gunaware Nilesh G. for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.

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]. 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 Dataon the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013

[4]. 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" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.

[5]. 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..

[6]. 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.