MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

SCALABLE DATA SHARING BY USING KEY AGGREGATION

Mukesh Giri, Shivanand Gaikwad, Akshay Jadhav,
Rupesh Kandhare, Prof.Nitin Hambir

Computer Engineering, Dr.D.Y.Patil School of Engineering,
Pune,India

Abstract- *In cloud computing, Data sharing is an important functionality in cloud storage. Sharing of data is considered as a challenging security problem. The sharing of the user's finicky data on a third party cloud server does not guarantee the promised level of security and there is a threat to accommodation user data. We can provide how to securely, efficiently, and flexibly share data with third party or others in cloud storage. We design and describe new type of public-key cryptosystems which produce equable-size encrypted texts such that capable delegation of decryption rights for any set of encrypted texts is possible. The novelty in that provides secured data sharing in cloud storage with the help of key-aggregate. It mean the nova is that one can aggregate any set of secret keys and make them as compact as a single key, the secret key holder can release a equable-size aggregate key for flexible choices of encrypted text set in cloud storage, but the other encrypted files outside the set remain intimate. In particular, our schemes give the first public key patient-controlled encryption to user for flexible hierarchy, which was yet to be known*.

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

1. INTRODUCTION

Data sharing is an important functionality in cloud storage, in cloud computing. We can provide securely, efficiently, and flexibly sharing data with third party or others in cloud storage. We design new public cryptosystem for secure sharing of data on cloud. Traditional Key cryptosystem lack the enhanced security techniques as the keys are generated by the existing random key generation. A traditional way to ensure it is any unpredicted privilege escalation that will expose all data. In a shared-tenancy cloud computing environment, things become even worse Data in a destination virtual machine (VM) could be stolen by instantiating another VM co-resident with the destination one. . Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Regarding availability of files, these are a series of cryptographic schemes which go as far

as allowing a third-party auditor to check the availability of files on behalf of the data sender without leaking anything about the data, or without compromising the data owner's anonymity. Like that, cloud users probably will not hold the strong conviction that the cloud server is doing a good work in terms of confidentiality.

Sharing of data is the vital functionality in cloud storage. For example, bloggers can let their friends view a subset of their private pictures; an enterprise may grant her employees access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can be download encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly.

A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the Virtual Machine or the honesty of the technical staff. These users are boost to encrypt their data with their own keys before uploading them to the server.

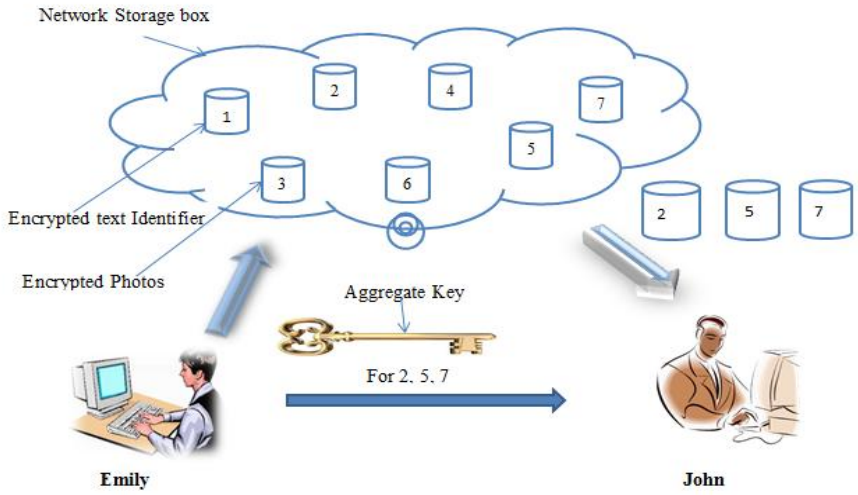

Fig.1:- File sharing between two users using single aggregate Key

Let's assume that Emily puts all her private data such as photo albums, some important documented on drop box or cloud storage, and she doesn't want to breach her photos or important documented. Due to various data leakage possibility Emily cannot feel comfortable by just relying on the privacy protection mechanisms provided by drop box, so she encrypts all the photos using her own keys before uploading. Any day, Emily's friend, John, told her to share the data taken over all these years which John appeared in. Emily can then use the share function of drop box, but the problem is how to commitment the decryption rights for these data to John. The possible option Emily can choose is to tight send John the secret keys involved. Directly, there are two great ways for her under the traditional encryption concept:

John the corresponding secret key directly and gives Emily encrypts all files with a single encryption key.

In first option is sends John the corresponding secret keys and Emily encrypts files with distinct keys. In this method is inadequate since all unwanted data also get expose to the John, which is inadequate. In second option, number of keys is as many as number of shared files, which may be hundred or thousand, as well as transferring these keys require secure channel and storage space which can be expensive.

To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the encrypted texts (produced by the encryption scheme) is decrypt able by a constant-size decryption key (generated by owner of master-secret key)? Therefore best solution to above problem is Emily encrypts data with distinct public keys, but send single decrypted key of constant size to John. Since the decryption key that should be sent via secure medium and kept secret small size is always enviable.

2. LITERATURE SURVEY

Cloud computing is widely increasing technology in world. It proved to store the data on cloud using remote network and it give huge of quality application to the user, so it need mere security to protect the data on the cloud storage. There for in this project we going introduced some algorithm with provide securely, efficiently, and flexibly share date with different cloud storage. We also introduced new public key cryptosystems which produce constant size encryption texts.

We were surveyed and studied different project related this area. Following is the listed of the things that were required to be studied for this project.

Cloud computing is visualized as design for succeeding generation. It has many facilities though have risks of attacker who can access the data or leak the user's identity. While setting a cloud users and service providers authentication is necessary. The issue arises whether cloud 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 user's identity.

There are many cloud customer who needs to transfer there information to different customers without providing a lot of personal details to that customer. The namelessness of the customer is to be preserved in order that to not reveal the identity of information owner. Provable Data possession (PDP) uses similar demonstrating marks to scale back computation on server, and network traffic. PDA ensures the info gift on cloud that is un-trusted is original while not accessing it. Security mediator (SEM) is approach permits the user to preserve the namelessness. Users are meant to transfer all their information to SEM in order that the SEM isn't able to perceive the information though it's reaching to generate the verification on data because the users are signed at SEM it mustn't recognize the identity of up loader.

There is other way for sharing encrypted text data is Attribute-Based Encryption (ABE). It is likely to encrypt text data with attributes which are equivalent to users attribute rather than other encrypting part of data. In ABE attributes description is considered as set so that only some particular key which is matched with attribute can decrypt the encrypted text. The user key and attribute are matched if it matches then it can decrypt a particular encrypted text

else it cannot decrypt that encrypted text. When there are attributes are overlay among the encrypted text and a private key the decryption is granted.

A multiple set of group key management is a hierarchical access control by applying an integrated key graph also handling the group keys for different users with multiple access authorities. Central admin key management plan uses tree structure to minimize the data processing, storage overhead and communication. It maintains things related to key downloading and also updates it. It accomplishes an integrated key graph for every use.

Public-key cryptography is known as asymmetric cryptography. It requires two different keys first one is private and next one is public. Two different parts of this key pair mathematically linked with each other. The first one is or public key is used for encryption and second one is or private key is used for decryption. Public Key encrypts the plain text to generate an encrypted data, while the private key is used to decrypt cipher text or to create original data. The term "asymmetric" arises from the use of different keys; each key is the inverse of the other. Public-key algorithms are primary security methods in cryptographic applications and protocols. They support various networking standards, such as (TLS) Transport layer Security. Some public key algorithms provide key distribution and secrecy for example Daffier-Hellman key exchange, some provide digital signature Digital and some provide both for example RSA

3. PROBLEM STATEMENT

One of the main efficiency drawbacks of the most existing Attribute-based encryption (ABE) schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a cipher text grows with the complexity of the access policy. The above observation motivates us to study ABE with verifiable outsourced decryption in this thesis work. Here emphasized that an ABE scheme with secure outsourced decryption does not necessarily guarantee verifiability (i.e., correctness of the transformation done by the cloud server).

4. SYSTEM ARCHITECTURE

KEY-AGGREGATE ENCRYPTION

A key aggregate encryption has four phases as:

4.1 Setup Phase

It takes implicit security parameter. An account on server which is not trusted executed by own for setup phase.

4.2 KeyGen Phase

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

4.3 Encrypt Phase

Anyone can send the encrypted data using this phase.. 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.A user which has a set of attribute can access the structure and can decrypt the message.

4.4 Decrypt phase

It takes input pk as public parameter, CT as ciphertext. Ciphertext contains a as a access policy and sk as a private key contains 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.

5. CONCLUSION

To share data flexibly is main thing in cloud computing. Outsourcing of data to server may lead to leak the private data of user to everyone. Users prefer to upload there data on cloud and among different users. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. It is required to keep enough number of cipher texts classes they increased fast and the cipher text classes are bounded that is the limitation. Public key cryptosystems provides delegation of secret keys for different cipher text classes in cloud storage. In which 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.

REFERENCES

[1] *Cheng-KangChu, Sherman S.M.Chow, Wen Guey Tzeng, Jianying Zhou, and RobertH. Deng, Senior Member, "Key-Aggregate for Scalable Data Sharing in Cloud Storage", IEEE Transaction on Parallel and Distributed System, Feb 2014, Vol. 25, NO. 2.*

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

[3] *E. Horvitz, and K. Lauter, J., Benaloh, M. Chase —Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, in Processing of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.*

[4] *T. Okamoto and K. Takashima, —Achieving Short Cipher texts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption, in Cryptology and Network Security (CANS '11), 2011, pp. 138–159.*

[5] *B. Lynn, and H. Shacham, D. Boneh, C. Gentry, "Aggregate and Variably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology – EUROCRYPT 03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416432.*

[6] *S. S. M. Chow, Y., B. Waters Dodis, and Y. Rouselakis, —Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions, in ACM Conference on Computer and Communications Security, 2010, pp. 152–161*

[7] *K. Takashima and T. Okamoto, —Achieving Short Cipher texts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption, in Cryptology and Network Security (CANS '11), 2011, pp. 138–159.*