Indian J.Sci.Res. 11(1) : 123-126, 2015 ISSN : 0976-2876 (Print)
ISSN : 2250-0138 (Online)

EFFICIENT DATA ACCESS IN CLOUD USING MULTIPLE KEY AGGREGATION TECHNIQUE

SUDARSHAN ADEPPA[a1]

[a]Dept of CSE, BKIT, Bhalki, India

ABSTRACT

Cloud is super enhancing technique which allows millions of users to store their data on clouds and provides a flexible way of data access from anywhere in the world. Users can upload the any type of data over the cloud and can be shared with any users across the globe. The cloud computing allows many users to store the data and allows us to access the data from any remote logging. We can use the cloud as public, private or both. In this paper, I present about cloud computing and secure data accessing from cloud. Data sharing is an important functionality in cloud storage. In this article, I discuss how securely, efficiently, and flexibly access and share data with others in cloud storage. Here public-key cryptosystems technique and identity based encryption is used to achieve the efficient data sharing over cloud. In this technique many constant single secrete key are generated and at the encryption end all secrete keys are aggregated into one single key. This aggregate single key works very flexibly.

KEYWORDS : Cloud, Data Access, Cloud storage, Secrete key.

As the increase in the use of internet applications, it leads to lack of efficient data storage and data manipulation problems. This problem leads to develop a technique to store the large amount of data in some location and to have easy access to the data from anywhere in the world. This technique is called cloud computing.

Cloud is a widely used technique to store the data on a physical devise of multiservers. These cloud servers are managed and maintained by the service provider. Many hosting companies own the clouds and protected from fraud users. We can buy these clouds to store our data and it can be accessible from any remote place and the capacity of storage is very high, so we can store any data related to user, organization. Cloud storage can provide the greater accessibility and reliability; rapid deployment; strong protection for data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. However, cloud storage does have the potential for security and compliance concerns. As we experience a huge demand in online services for personal applications and for corporate projects. So we need to store huge amount of data given by the users and we need to store and manipulate plenty of files, so this cloud sharing technique provides a secure way to store and share the data in any size. Cloud-based storage as a service includes inherent vulnerabilities, but they need not prevent a business user from taking advantage of its economies and flexibilities. Data in a target Virtual machine could be stolen by instantiating another virtual machine. The files stored on the cloud must be available to the users at any time. We have to use some efficient cryptographic technique to check the availability of files without leaking any data to fraud users. The user should get confident that the data on cloud servers are safe. Every user and organization should check the cloud storage about what types of cryptographic techniques are employed to protect the user data and files in cloud. If sometime user is not happy with security provided by the cloud servers than users are advised to encrypt their data with own encryption keys before we upload the data or files to the clouds. Sharing is an important functionality in cloud storage. Data from different clients can be hosted on separate virtual machines (VIRTUAL MACHINEs) but reside on a single physical machine. Data in a target virtual machine could be stolen by instantiating another virtual machine co-resident with the target one [G.Ateniese and B. Medeiros, 2004].

We can put data on cloud in two methods, in first method, when a girl puts her photos on cloud, and she doesn't want to expose her photos with others so before she uploads the data on cloud she will encrypt her photos by using her own key. When she wants to share her photos to her friend boy she will send the key to boy securely so boy can decrypt the photos very securely. A possible option Girl can choose is to securely send Boy the secret keys involved. Naturally, there are two extreme ways for her under the

[1]**Corresponding author**

traditional encryption paradigm Girl encrypts all files with a single encryption key and gives Boy the corresponding secret key directly. Girl encrypts files with distinct keys sends Boy the corresponding secret keys

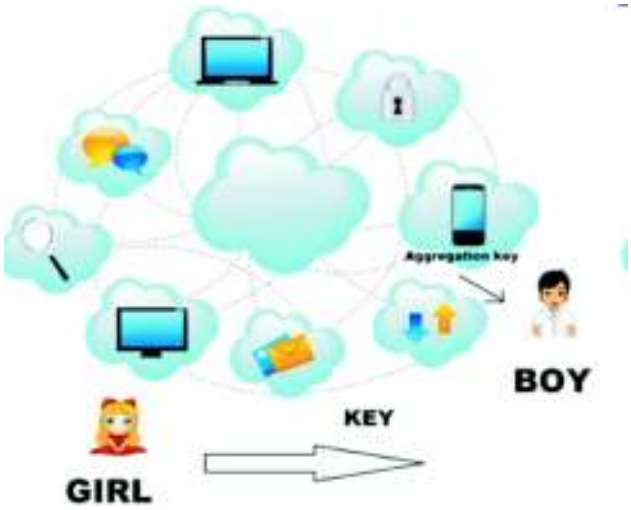

Figure 1: Cloud Structure

In second method user can encrypt each photo or file separately with separate key for each photos [G.Ateniese and B. Medeiros, 2004]. If user uploads thousand photos then he need thousand channel for each photos to encrypt with separate key, and it will be more expansive to store thousand keys every time. The above figure 1 shows the structure of cloud.

Encryption keys also come with two flavors - symmetric key or asymmetric (public) key. Using symmetric encryption, the Girl has to provide encryption key to boy when she starts data sharing. Generally girl will use public key cryptographic technique to encrypt and decrypt the data. Encryption key and decryption key are different in public-key encryption. The use of public-key encryption gives more flexibility for our applications. For example, in enterprise settings, every employee can upload encrypted data on the cloud storage server without the knowledge of the company's master-secret key.

AGGREGATIONS TECHNIQUE

The data sharing in cloud can be done efficiently using a public key encryption technique called key aggregate cryptosystem. key aggregate cryptosystem uses a cipher-text identifier. These cipfer text identifiers are categories into different classes. Here in this technique user message or files are encrypted under the identifiers of cipher-text, where each owner holds a master key called master secrete key The key owner holds a master-secret called master secret key, which 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, i.e., the decryption power for any subset of cipher-text classes. With our solution, Girl can simply send Boy a single aggregate key via a secure e-mail. Boy can download the encrypted photos from Girl's Dropbox space and then use this aggregate key to decrypt these encrypted photos. The scenario is depicted in Figure 1. The sizes of public key, master key and aggregate key is constant in key-aggregations technique.

The data owner establishes the public system parameter via Setup and generates a public/master-secret3 key pair via Key Gen. Messages can be encrypted via Encrypt by anyone who also decides what cipher-text class is associated with the plaintext message to be encrypted. The data owner can use the master secret to generate an aggregate decryption key for a set of cipher-text classes via Extract. The generated keys can be passed to delegates securely via secure e-mails or secure devices) finally, any user with an aggregate key can decrypt any cipher-text provided that the cipher-text's class is contained in the aggregate key via Decrypt.

DATA ACCESS AND SHARING OVER ENCRYPTION

Once the data is stored in cloud, users can access the data at anytime. For this purpose here we use an Aggregate key is used for the secure data sharing over the distributed data sharing in cloud environment. Aggregate key consist of various derivation of identity and attribute based classes of respective data owner in the cloud. Aggregation key is used to sharing the data between one to other. The key aggregation technique is useful when the delegation to be efficient and flexible. Key aggregation enables content provider to share other's data in a confidential and elective way, with a fixed and small cipher

text expansion, by distributing to each authorized user a single and small aggregate key. Girl wants to share her data on the server. The key generation phase is provided by public key and master key pair. In this public and master key pairs are secretly done by Girl. Girl encrypts the data using public key and these data are uploaded to the server. Girl is willing to share a data to boy. Girl can compute the aggregate key for boy, it's performed by master key, and this aggregate key is sent to boy via email and this aggregation key is used to download the data and decrypt the data. In this example input is master key and data and output is aggregate key. It's the primary key having more than one column. Key aggregation is group of public key and private key used for transmission of data. The combination of public and private key is known as key aggregation. Key is nothing but composite or concatenated key. Example different books may have identical title, authors. In this case we can take title, author, and publication date as the aggregate key which acts as primary key. Map reduce function is also used in key aggregation.

IDENTITY BASED ENCRYPTION

To secure the data from others we need to use some different encryption techniques. Its primary innovation was its use of user identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users' certificates [T. Okamoto and K. Takashima, 2011]. It also makes it much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components. At the time Shamir published his proposal he had already determined a way of using the existing RSA function for an identity-based signature (IBS) scheme, but had yet to solve the problem of identity-based encryption (IBE). This remained an open problem until 2001, when two independent lines of research (Boneh and Franklin, as well as Cocks) arrived at solutions to the problem. Since time, identity-based cryptography has been a heavily-researched topic in the field of cryptography.

In addition to academic research, commercial product offerings are also now available, most notably those of Voltage Security, Identity-based encryption (IBE) is a public key encryption where it uses user identities by setting user identity such as email address. The IBE contains a private key generator (PKG) which holds the master key and issues secrete keys to all users with respect to identity. The encryption can take the public parameter and a user identity message. The recipient can decrypt this cipher-text by his secrete key SECURITY OF IDENTITY-BASED CRYPTOGRAPHY. The vast majority of proposed identity-based cryptography schemes and certainly all of those discovered so far that are computationally efficient, are based on mathematical functions called bilinear no degenerate maps. A bilinear no degenerate map is a function pairing elements from one cyclic group to another of the same prime order, where the discrete log problem is hard in the first group [Frank E. Gillett, 2008].The security of identity-based cryptography is based on the assumption that the particular bilinear maps chosen are one-way functions, meaning it is easy to calculate their result given a pair of operands but hard to calculate the inverse. This property is often referred to as the Bilinear Diffie Hellman Assumption, since the Bilinear Diffie-Hellman problem is reducible (algorithmically equivalent) to the discrete-log or inverse operation for these bilinear maps [T. Okamoto and K. Takashima, 2011].

IBE: Issues: One main problem: size of the ciphertext is very large; two elements of ZN per bit.Boneh, Gentry and Hamburg. An IBE which encrypts a single bit. (A general description of which the Cocks-IBE is not an instantiation.)2. Reuse of randomness for encrypting more than one bit. Significantly reduces the size of the cipher-text. Trade-off: substantial increase in encryption time. Better balance: ongoing research work.

CONCLUSION

Cloud computing technique makes very easy to play with data at anytime with anyone. The cloud storage provides very efficient technique to store huge amount of data on cloud and it can be accessed from any remote area

securely without data leakage. Here public key cryptosystems technique and identity based encryption is used to achieve the data sharing in cloud. As day to day the popularity of cloud is increasing and many users are storing various data in cloud for sharing with friends and in community. So we need to ensure the data security across the cloud. The key aggregation technique increases the security scalability to share the data in cloud among various users. Our approach is more flexible than hierarchical key assignment which can only save spaces.

REFERENCES

G.Ateniese and B. Medeiros, Identity-based Chameleon Hash and Applications, Financial Cryptography Proceedings of FC 2004, LNCS, Springer-Verlag.

J. Baek, J. Newmarch, R. Sfavi-Naini,W. Susilo, A Survey of Identity-Based Cryptography.

Frank E. Gillett, "Future View: The new technology ecosystems of cloud, cloud services and cloud computing" Forrester Report, August 2008.

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.

T. Okamoto and K. Takashima, "Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption," in Cryptology and Network Security (CANS '11), 2011, pp. 138159.