International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Key Aggregate Method for Secure Data Sharing in Cloud Storage Using MD5

Varsha S. Kadam[1], **R. H. Kulkarni**[2]

[1]Student at Department of Computer Engineering, JSPM Narhe Technical Campus, Savitribai Phule Pune University, Maharashtra, India
[2]Professor and HOD at Department of Computer Engineering, JSPM Narhe Technical Campus, Savitribai Phule Pune University, Maharashtra, India

Abstract: ***Cloud computing is getting popularity now a days. Cloud providers offers data storage and other services in very less cost. The main advantage of cloud is data sharing and remote data access. On the cloud data is get shared between numbers of users. The data security is totally depended on the security parameters used. To achieve this purpose we have described new strategy which depends on public key cryptography. We have designed aggregate key method which is constant size cipher text generated by using MD5 algorithm. The cipher text can be decrypted by using hash key generated. This constant size cipher key is nothing but aggregate key for selection of flexible choices of ciphers. The other encrypted files remains secret, only file can be decrypted for which aggregate key is generated. We can save this aggregate key or can send it to others for further data sharing technique.***

Keywords: Aggregate Key, Data Security, Cloud Services, Cryptography, Credentials

1. Introduction

Cloud computing has wide range of scope now a days. Cloud provides large amount of virtual environment hiding the platform and operating systems of the user. Cloud computing is getting popularity now a days due to its all-time availability and remote access. Cloud users have flexibility to share their data over cloud. Cloud user can easily access the data independent of its location. Figure 1 shows the cloud architecture. In the cloud computing number of user can share or use data which is stored on the only one physical location. The main problem of the cloud computing is the security lack. It is due to the number of people from different location are connected to each other and share same file among. Either cloud data owner or data user don't have control on the data present on the cloud. The main purposed of this method is to share the data to number of people at same time but securely. The cloud service provider can apply different methods to avoid the data attacks in the cloud computing, or to avoid hacking of data. But these methods of encryption are not sufficient as they don't have enough security. Privacy preservation is done by using token system in the cloud. Any user can access the data user wants. i.e. only selected content can be shared. Cryptography allow the data owner to share the data to in secure way. So user can encrypts data and uploads on server. Different encryption keys as well as decryption keys are generated for each bunch data. The encryption and decryption keys may be different for different set of data. The only that data can be decrypted for which aggregate key is generated.

This paper proposes a new cryptography technique in which constant size aggregate key is get generated. So as to use it to provide access to only same class of data for which the aggregate key is generated. The main concept of the aggregate key cryptography is that we are creating single aggregate key which hold the capability of decrypt the group of files. There is no need to use different key to decrypt the different data. The generated delegate key can be send to the cloud data user through the secure manner. The digital data is stored on cloud as a data pool. The responsibility of cloud owner is to maintain the track of the data and avoid. 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.

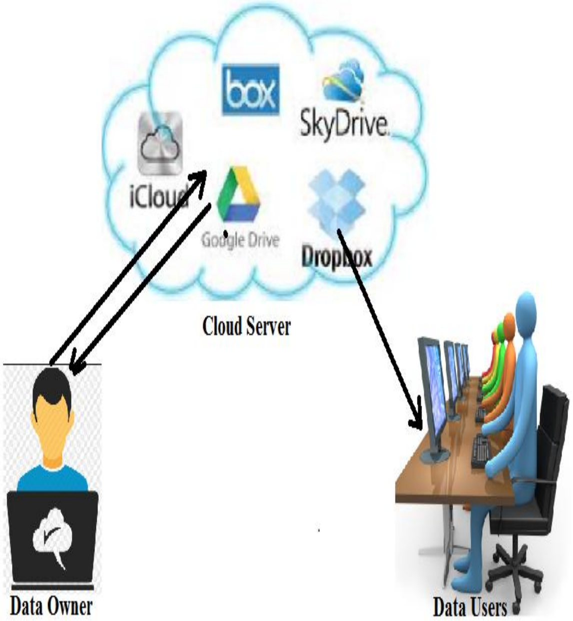

Figure 1. Cloud architecture

Cloud storage is based on highly virtualized infrastructure and is like broader cloud. The main advantages of cloud computing is data sharing. One can upload, download or modify the file on cloud. User can store any type of data on the cloud. That means data shared may be in the text format or it may be in the multimedia format. The sharing of data must be in flexible manner and to achieve this we have used secure and flexible data sharing approach. Otherwise the data attacker may steal our personal information and may misuse it. So security in the cloud computing plays an important role.

Sharing of data on cloud is done flexible and cost optimizing way so it motivates the end user as well as enterprises to store their personal data on cloud and share it in between number of cloud data users. The insider attack is the main thread in the cloud which is needed to address first. Cloud Service provider have a rights to decide whether audits are held for users who have physical access to the server. As a cloud service provider stores the data of different users on same server which is remotely located it is possible that user's private data is leaked to others.

In cloud to achieve the integrity along with avoiding anonymity is a major task and it's to complicate also. To check the data integrity user can check the data integrity by using MD5 algorithm. User also performs integrity checking operation on the cloud. The main concern of sharing data securely and for this answer is the cryptography. The question is how can the encrypted data is to be shared. The data owner can provide encryption and decryption key to decrypt the data to the data user who want to use the data. For an example Alice keeps her private data i.e. photos on dropbox and she doesn't want to share it with everyone. As the attacker may access the data so it is not possible to rely on predefine privacy preserving mechanism so she all the photos were encrypted by her on encryption key while uploading it.

2. Literature Survey

There are number of systems available as discussed in different articles. We have studied different methods for cloud data integrity this methods are as follow:

The paper number [9] this paper defines methods to achieving privacy and security in the Cloud and also briefly discuss the secure data sharing methods. This paper provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security attacks of one's personal data present on the Cloud. These elaborate the factors that affect the security of information of present on the cloud. It explains the needs of security for enterprises to understand the dynamics of information security in the Cloud.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," [10]. This paper describes the broadcast encryption which enables a broadcaster to transmit encrypted data or information to a set of users so that only a targeted subset of users can decrypt the data. Other than above characteristics, it also allows the group monitor to include new members by preserving previously computed information, and user decryption secret keys need not be computed again and again, the Aggregation logic and size of cipher texts are remain same and the group encryption required different key but to decrypt the data only one key is required.

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". This system utilize the data of cloud to encrypt and to decrypt the cloud data. The original data get divided into number of parts and some parts are used for encryption and decryption purpose. When revocation is needed owner of data required some slice to encrypt or decrypt the data. The owner of data can retrieve this signature by using intermediator and then he can allow user to upload or download the data over the cloud.

3. Proposed System

In propose system we are using two different keys to encrypt and decrypt the data. First key is known as encryption key and other key is the aggregate key which can be used for the decryption purpose. This encryption method is basically design for the aggregation based encryption. The owner of data can use different key to encrypt the data and he can send only one key to the data user who wants to use the data. Data owner is solo responsible for the data encryption and he can decide the which rights to be provide to different user so that he can have data access control. The data owner have rights to use the secret key from which aggregate key can be generated and which can be further used for the decryption purpose. Aggregate key can be send to the data user in secure manner. The authenticated user can decrypt any data block for which they have the aggregate key.

A key-aggregate encryption scheme KAC consists of five polynomial-time algorithms as follows. The data owner establishes the public system parameter via Setup and generates a public/master-secrete key pair by using keygen method. Encrypt method is used to encrypt the message by data owner or data user. User can encrypt the data or class of data for which user have provided rights.

1. Setup: The owner of data can run set up method to encrypt the key and generate the public key. 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 owner who have uploaded the data on the cloud.

2. KeyGen: This phase is executed by data owner to generate the public key for encryption and master key (pk, msk). The data owner generates a public secrete key to encrypt the data over cloud and thereafter the data get share with data user. He also create an aggregate key to access the block of ciphers of limited size. The keygen is helpful to generate the master key and aggregate key.

3. Encrypt: This phase get executed by the data owner while uploading the data on the cloud server. Encrypt (pk, m, i), the encryption algorithm takes input as public parameters pk, a message of file to be encrypt m, and i denoting ciphertext class which user have to download. The algorithm encrypts message m and produces a ciphertext C such that only a user that having a set of attributes which satisfies the access structure is able to decrypt the message. This algorithm encrypts the data provided by the data owner to 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 = ciphertext C.

4. Extract: This method is executed by the data owner for assigning the delegate key to the decrypting power for a certain set of cipher text classes to a delegate. The aggregate key is use to extract the particular block of the ciphers from the cipher files.

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

5. Decrypt: This is executed by the data user situated at remote location that has the decryption authorities. Decrypt (kS, S, i, C), the decryption algorithm takes input as public parameters pk, and 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.

3.1 System Architecture

In the proposed system there are three main parts i.e. data owner, data user and cloud service providers. User will get blocked if he enter wrong aggregate key for three times. The following figure shows the working of proposed system.

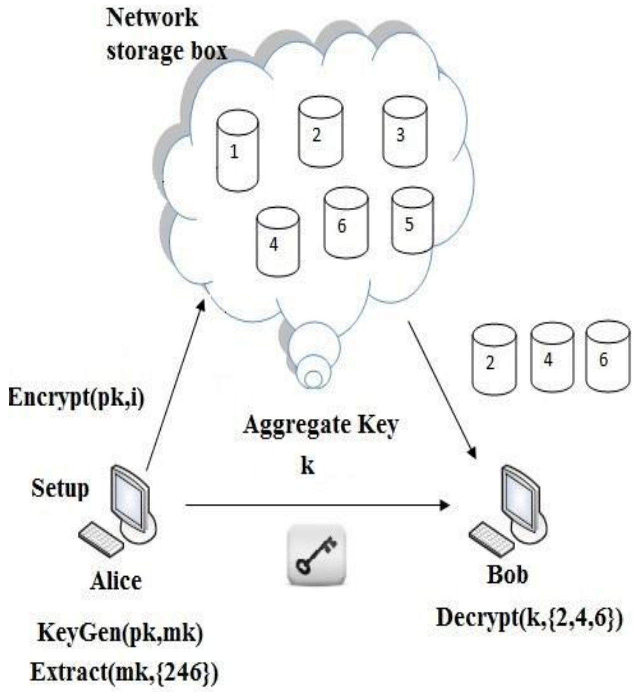

Figure 2: System Architecture

In the aggregate key cryptosystem authentication is very important if user fails to provide valid credentials then data owner may be block to the particular user. User either one of sender or receiver. Permission functions are the functions such as read, write and update. Encryption function encrypt data using public key that key size is fixed for every user but it can be generated dynamically by using MD5 algorithm. The split function uploads the data but before uploading t splits the encrypted data into different parts and stored that part on different clouds. Extractor can check is user having proper rights to access particular file or not. In case it accessible then it decrypt from that whole bunch. The above figure shows the aggregate key master key generation location. Each user will get different and unique key as per the request generated by user. Initially the public key is used to encrypt the file and then it get merge into the master key. When any user request for the data then he need to provide the index of particular file. Then the keys are get extracted from the master key and again we form aggregate key from this keys. This aggregate key is of constant size. To generate this aggregate key we have used MD5 algorithm.

KAC is developed for the secure data sharing. Data owner can send his data with secure and confidently. KAc is very secure and reliable method for sharing data in cloud computing. The aim of KCA is illustrated in Figure 2. For sharing the selected file with user cloud service providers first check the rights of particular user. If he having rights for that file then only user can perform particular office. Later the public/master key pair (pk, mk) is generated by executing the KeyGen. The master key is kept secret and the public key pk and param are made public to access the file. Anyone can encrypt the data file m and this data is uploaded to the cloud server. If Alice is wants to share a set S file of her data with a friend Bob then she can perform the aggregate key generation algorithm and can send the generated key to user side. KS for Bob by executing Extract (mk, S).

3.2 Encryption of File

To encrypt the user data we are using secrete key resides at the private cloud. This key is used to convert plain text to cipher text and again for the decryption of the user data. To encrypt and decrypt we have used three basic functions as follow:

KeyGenSE: In this k is the key generation algorithm which can generate the secrete file by using security parameter.

EncSE (k, M): in this formulae M is the text message and key is the secrete key by using this both we have generated a cipher text C.

DecSE (k, C): Here C is the cipher text and k is the encryption key by using cipher text and secrete key we have to generate plain text.

3.3 MD5 Algorithm

The main steps of MD5 algorithm to generate the hash value are given as below:

1. Append padding bits so message becomes 448 module 512.

2. Append length to the input message so that it becomes exact 64-bit in length.

3. Initialize the 32 bit MD buffer A, B, C, D.

4. Process the message in 16-word block,

F (X, Y, Z) = XY or not (X) Z
G (X, Y, Z) = XZ or Y not (Z)
H (X, Y, Z) = X xor Y xor Z
I (X, Y, Z) = Y xor (X or not (Z))

5. The final digest message will be stored in buffer.

4. Conclusion

To share data flexibly and securely in cloud computing is vital thing. Users always prefer to upload there data on cloud and share the uploaded data among different users. The main drawback of cloud computing is the security issue. Cryptography is a one of best solution which provides security to share selected data with desired cloud data users. Sharing of decryption keys in secure way plays important role. The proposed Public-key cryptosystems provides delegation or leader key of secret keys for different cipher text classes in cloud storage.

Cryptographic schemes are getting more versatile and trustable, it involve multiple keys for a single application. In this paper, we consider how we can "compress" secret keys by combining the multiple keys which support delegation or aggregation of secret keys for different cipher text classes in cloud storage system. Our approach is more flexible as compare to hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.

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.

[7] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.

[8] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in CM Conference on Computer and Communications Security, 2009, pp. 121–130.

[9] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[10] 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.

[11] 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.

[12] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002site)

Author Profile

Varsha S. Kadam received the B.E. Degree in Computer Engineering from Shivaji University. Pursuing M.E. in Computer Engineering from JSPM Narhe Technical Campus, Savitribai Phule Pune University, Maharashtra, India

R. H. Kulkarni is Professor and HOD at Department of Computer Engineering, JSPM Narhe Technical Campus, Savitribai Phule Pune University, Maharashtra, India. Pursuing PhD in Computer Science