Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Group Data Sharing in Cloud Environment

Daundkar Anita Mohan, Prof. Arati Dandavate
Computer Department &University,
Pune, India

Abstract—It is very important to share the data in a group without revealing its plaintext or decryption key to outside group member in cloud environment. Previously this has been achieved by using Conditional Proxy Re-encryption. In Conditional Proxy Re-encryption (CPRE) scheme data before uploading on the cloud get encrypted with condition value and then stored on the cloud by passing conditional value to all the group members. But this is not suitable when the size of the group is very large and not static. Whenever group member changes content owner need to encrypt the data again with new condition value and then he passes new condition value to all the members. This is very tedious job. New scheme for condition Proxy Re-encryption i.e. Outstanding CPRE (O- CPRE) scheme is proposed which reduces the client overhead. In this scheme when group member changes only the conditional value get changed and then get uploaded onto the cloud without encryption of data. O-CPRE is much more suitable for secure big data sharing in cloud environment than the other existing schemes

Keywords—Cloud Computing, Data Sharing, Conditional Proxy Re-encryption, Proxy Re-encryption

I. INTRODUCTION

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Cloud computing paradigm has been adopted to a wide range of businesses and organization recently. Advances in cloud computing technology have drastically changed the shape of current computing industry. By exploiting the innovative technology, companies are able to purchase the computing resources in need from a cloud service provider such as Amazon EC2 rather than establishing and maintaining their own computing environment, which is usually much more expensive than paying corresponding cloud services per use. The cost saved in this way can be invested to improve the core competitiveness and productivity of the companies. For a company, the transition from its own private computing environment to a cloud computing environment means a huge financial advantage. At the same time, that means that all the data of the company even including confidential data is in the hand of another organization, which is a serious security concern. For instance, the data stored ina remote cloud storage can be exposed when the server is attacked. There may be the possibility of data leakage and privacy. To prevent accessing private information user can encrypt data by its own private key and also can decrypt the data after getting it from the server. So the data will be secure. But when there is group of members then it becomes burden on the cloud server for encryption and decryption of data. It becomes complicated problem an even more complicated conundrum if the data isbeing shared among a group of users whose membership is not necessarily static. Recently, the concept of proxy re-encryption has been proposed to allow a group of users to share a confidential data at a remote server without exposing the data to the server. A proxy re-encryption transform a cipher text C, which is encrypted by the public key of a user A , to another cipher text C0 in a way that C0 can be decrypted by the private key of another user B. to make this possible ,A needs to create a re-encryption key for B and sent this to the server along with C. Once C is requested by B the server re-encrypts the C and transform it int C0 using the re-encryption key from A, and sends C0 to B . During this process, the server (as well as anyone who broke into the server) is not able to see the plaintext of C. On the other hand, B will be able to decrypt C0 using its own private key. While the idea of re-encryption is appealing, there is one issue. Once A creates a re-encryption key for B , B can collude with the server to decrypt all of the old and new messages A created/will create, to which B does not obtain the permission to access. To solve this problem, the concept of conditional proxy re-encryption (CPRE) has been emerged. In this scheme, A creates an encrypted message along with re-encryption keys (one for each member of a group) with a certain condition value (for the whole group). The condition value is used when A encrypts a message as well as when it creates a re-encryption key for another user. As a result, a malicious user who can collude with the server's administrator still cannot decrypt messages encrypted by A as long as A does not provide an re-encryption key which contains the condition value associated with the messages.

© 2014, IJARCSSE All Rights Reserved

II. RELATED WORK

Efficient Conditional proxy Re- encryption with chosen cipher text Security by S. Sree Vivek et. Al. [1] states thata more efficient CCA secure unidirectional C-PRE scheme with less number of bilinear pairings. The scheme is more elegant when The LOCO-I Lossless Image Compression Algorithm: Principles and Standardization into JPEG-LS [2] describes lossless compression for continuous tone images. Fixed prediction algorithm is used. Method is very slower.compared to its counterparts. This system defines security of the scheme in the random oracle model under appropriate security definitions. There are still many open problems to be solved, such as designing CCA secure C-PRE scheme in the standard model, C-PRE in other settings like identity based and certificateless cryptography.

Proxy re-encryption system, a semi-trusted proxy can convert a ciphertext originally intended for Alice into a ciphertext intended for Bob, without learning the underlying plaintext. Proxy re-encryption has found many practical applications, such as encrypted email forwarding, secure distributed file systems, and outsourced filtering of encrypted spam. In ACM CCS'07, Canetti and Hohenberger presented a proxy re-encryption scheme with chosen-ciphertext security, and left an important open problem to construct a chosen-ciphertext secure proxy re-encryption scheme without pairings. In this paper, we solve this open problem by proposing a new proxy re-encryption scheme without resort to bilinear pairings. Based on the computational Diffie-Hellman (CDH) problem, the chosen-ciphertext security of the proposed scheme is proved in the random oracle model.

Security and Privacy Challenges in Cloud Computing EnvironmentsCloud computing has generated significant interest in both academia and industry, but it's still an evolving paradigm. Essentially, it aims to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and in- formation infrastructures consisting of pools of computers, networks, and storage resources. Cloud computing reduces the cost of resources and ultimately improves the performance and efficiency of the system. The aricle provides the challenges faced in cloud areVirtualization and Hypervisors, Authentication and Identity Management,Access Control and Accounting,Trust Management and Policy Integration, Secure-Service Management.

III. SYSTEM DESIGN MODEL

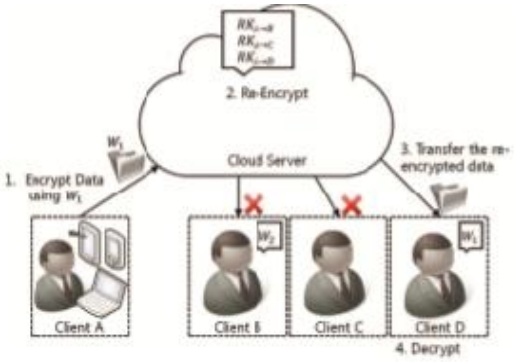

Fig.1 System Model

Fig 1. Describes System model for data sharing in cloud computing. Two different entitiesand they can be identifed as follows:

- Cloud server
- Client

Cloud Server:: It provides users with operation and storage while users pay reasonable fee for the service. The cloud server stores user's ciphertext and re-encrypts and sends data on the request of a customer. This study proposes
a honest-but-curious system model. The cloud server in this model runs a given protocol as best as it can and pays attention to user's data simultaneously. Therefore, there is possibility of passive attacks such as looking at content of data or eavesdropping in data transfer process. In addition, attacks to the CPRE scheme
are also possible, such as comparison of findings from iterative operation of ciphertext or creating re-encryption keys to be sent to the cloud server. In the following descriptions, will use Cloud Server, and Cloud interchangeably.
Client:This entity has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation. Clients can be either individual consumers or organizations. The client can connect to the cloud with various devices. It includes resource-constrict mobile devices such as smart phone or tablet.
Therefore, it can be relieved of the burden of maintaining and computation by storing the large data files in the cloud storage. In our environment, client can be originator of data files as well as destination of data sharing.
Design process consist of following phases.

- Setup
- Data Encryption
- Data Re-encryption for sharing
- Data Decryption
- Changing a condition value.

© 2014, IJARCSSE All Rights Reserved

IV. DATA SECURITY IN CLOUD ENVIRONMENT

A. DATA INTEGRITY:

Data integrity may be easily preserved by employing traditional cryptographic methods such as message authentication codes (MAC). It is a fixed size block of data based on file F using any secret key. The data owners maintain small amount of MAC before outsourcing the data and whenever data is needed, MAC is verified with the previously computed MAC to verify the correctness of the received data from cloud.In cloud environments traditional methods are implemented no more since the data is dynamic and there is huge cloud storage. So it becomes quite impractical that for checking whether the data is stored securely we retrieve all the data stored on server. Integrity threats include data deletion, data manipulation. The computation details are not transparent to cloud customers so the CSP behave dishonestly and may alter the data.

B. DATA CONFIDENTIALITY:

A user can access the services provided by SaaS model through web browser over theinter net. So to protect the data during transmission HTTPS is implemented. If user uploads data to the CSP security must be there so that only authorized users access the data,the same requirement with PaaS. While in IaaS, multiple users data reside on the same location so in IaaS confidentiality arises in a way to include isolation over the different user's data.

C. DATA AVAILABILITY & MANAGEMENT:

Availability is affected different the server or service organization is penetrated or spoofed. In cloud characteristic broad network access DNS is one of the main attack on availability. So for better service offering over the internet user must have reliable DNS. So for long term data storage data availability is of much importance due to possibility of data loss.

D. DATA AUTHENTICITY:

Cryptographers invent a vast number of primitives for preserving the privacy of users' data. Among these primitives, anonymous password authentication (APA) has been used for ensuring the private authentication process. Zero knowledge authentications in cloud environment enjoy the benefits of password authentications while offering user privacy preservation.

E. DATA BREACHES, LEAKS & HACKS:

Due to Multitenancy environment in cloud breaching the data will become a potential threat. Data breach effects two security properties of data confidentiality, integrity & authenticity. Confidentiality -refers that only authorized parties or systems can access the data and integrity refers that data is not deleted, manipulated or fabricated by some third party who is not authenticated to perform such task. Data breach may occur internally by some data manager who has direct access to the data or from outside by some malicious hacker. However confidentiality and integrity issues are addressed by strong cryptographic mechanism like DES and AES with common PKI infrastructure. In this data and key management become an issue for data owner which can be addressed by combining techniques of attribute based encryption, proxy re-encryption and lazy re encryption.

V. CONCLUSION

The proposed system a content sharing scheme that is safe in the cloud computing environment, based on a conditional proxy re-encryption scheme. This system can significantly reduce burden of a client due to two charateristics. First is re-encryption process is delegated to a cloud server. A client is only involved in process of encryption and decryption of data and creation of re-encryption keys. Second, the number of re-encryption keys to be required for sharing is minimized.

Secure data access when sharing in a group, Implementation and maintenance, Reliability and scalability, Guaranteed levels of services, Total cost of ownership are the main feature of this system.

REFERENCES

[1] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient Conditional Proxy Re- encryption with Chosen-Ciphertext Security," Proceedings of the 12th Information Security Conference (ISC), pp.151-166, 2009.

[2] R. H. Deng, J. Weng, S. Liu, K. Chen, "Chosen- Ciphertext Secure Proxy Re-encryption with- out Pairings," Proceedings of the 7th Interna- tional Conference on Cryptology and Network Security (CANS), pp.1-17, 2008.

[3] L. M. Kaufman,"Data Security in the World of Cloud Computing," IEEE Security & Privacy, vol. 7, issue 4, pp. 61-64, 2009.

[4] H. Takabi, J. Joshi, and G. Ahn,"Security and Privacy Challenges in Cloud Computing Envi- ronments," IEEE Security & Privacy, vol. 8, issue 6, pp. 24-31, 2010.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiev- ing Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,"Proceed- ings of the 29th IEEE International Confer- ence on computer Communications, pp.534- 542, 2010.

[6] J. Zhao, D. Feng, Z. Zhang, "Attribute- Based Conditional Proxy Re-Encryption with Chosen-Ciphertext Security," Proceeding of Global Telecommunications Conference (GLOBECOM), 2010.

© 2014, IJARCSSE All Rights Reserved