Re-Encryption based Secure Communication for Scalable Data in Multiple Clouds

P. Reddy Prathyusha  
Department of Computer Science and Engineering  
Jawaharlal Nehru Technological University  
Anantapuramu, Andhra Pradesh  
E-mail: reddyprathyusa.26@gmail.com

C. Shoba Bindu  
Department of Computer Science and Engineering  
Jawaharlal Nehru Technological University  
Anantapuramu, Andhra Pradesh  
E-mail: shobabindhu@gmail.com

Abstract—The Cloud Computing provides the services to organizations based on the service models such as SaaS, PaaS and IaaS through deployment models like Public, Private and Hybrid clouds. There are lots of advantages with data outsourcing to the cloud. Cloud has the ability to function well even though changes are made to the data. But, one of momentous challenge is providing security to the cloud data. Now a day’s these cloud data is accessed by mobile users also. Such that there is need to diminish the communiqué cost and totaling load. In the previous scheme, the Attribute Based Encryption was proposed to provide security. Additionally Re-Encryption is also provided in order to minimize sustained users only in single cloud. In this paper, we will present a protocol that outsources the data in multiple Clouds to achieve more security and high scalability.

Keywords: Distributed Computing, Security, Mobile Computing, Scalability, Cryptography, Multiple Clouds

I. INTRODUCTION

The authorized users can access the large amount of data stored in a cloud and it is provided by cloud storage services. Data which is stored in the cloud should be confidential; Users have to pay some amount for data storage and computation of data actually used. But users do not bother about maintenance cost. One of non-trivial risk is cloud data being accessed by unauthorized users. So, there is a necessity to provide security for data to ensure the confidentiality.

Mobile cloud computing provides a way for the users to access the cloud data through mobile devices. Lots of transactions are done through mobiles. Such that, to preserve the battery consumption and computations there is the need to reduce the number of data transmissions. Additionally data are addressable with fine-grained access control to provide flexibility.

Tysowski E. et. al. [1] has presented the following implementation:

1. The data outsourcing, data storage is provided by the cloud provider in a secure manner. Then only authorized users can read stored data in the cloud, based on the attributes specified by the data owner.
2. The Traditional Attribute Based Encryption, an enhancement is made between the trusted authority and data owner thus resulting in keys division. So, messaging burdens and high computations are relieved to the data owner.
3. The group keying mechanism provides additional security; the data access is controlled by data owner with the additional secret key distribution.
4. The process of transforming the stored cipher-text is called Re-Encryption. Without the involvement of data owner, efficient user revocation permits, no need of subsequent key generation and removal of attributes.

The secure data outsourcing and mobile applications to a single cloud was done by the P.K. Tysowski and M.A. Hasan [1], by using the key management technique rather than the multiple clouds. With this technique, an additional layer of security is provided by the data owner to the data.

Now, we are providing the re-encryption based secure data transformation to multiple clouds such as Amazon and Azure. With the data outsourcing in multiple clouds, we can achieve better results than in the single cloud.

II. RELATED WORK

Several researchers have proposed various solutions for secure data communication in cloud. The public key management system (RSA) [3] is one of the techniques used to provide security to cloud data. Here, the main drawback is for each individual user, the data owner has to provide an encrypted version of the data. So, there is a high traffic cost on the mobile data owner. The cloud provider directly cannot access the data, would allow to read plaintext rather than decryption in the middle of data transmission called as “data re-encryption” [4].

Another technique is Cipher text Policy Attribute Based Encryption [5] has several benefits. Here, there is an access
structure that should be satisfied with certain attributes provided by the data owner and then the user can allow accessing the data. But, data owner should be available at anytime and frequent keys are needed whenever time will expires also a user revocation is difficult.

For secure distributed data storage, many schemes have been applied such as Hierarchical Identity Based Encryption [6], Cipher text Policy Attribute Based Encryption... etc. The content owner access the control of all the users. The combination of CP-ABE and Proxy Re-encryption schemes, between the data owner and provider the secret is pre-shared and re-encryption keys are computed by the cloud provider. The difficulty here is, for each user revocation key updates are required which is costly.

After such techniques to avoid single point of failure by using attribute-based access control [2], the Multi authority system is another technique [7]. Here multiple encryption keys are generated for hosting content by the data owner to communicating with attribute authorities. To decrypt the data each user has to submit multiple secret keys. However, it is expensive and complicate.

Trusted data sharing between the authorized users has proposed by the G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang [10], but it is impractical to resource-constrained devices and networks. After that, the revocation is handled in highly scalable system [11]. It requires the user identity solely to granting access is one of the limitations.

Another one is a combination of ABE along with Proxy re-encryption, it allows the users to access control of resources and relieves from re-encryption task to a cloud provider [13]. But it is impractical due to user’s mobility. The data outsourcing was implemented in an existing cloud platform that is Google App Engine [15]. But, it does not allow the direct connection to the security model of GAE.

III. SYSTEM MODEL

The centralized data stored as permanent in cloud and provided by the Cloud Service Provider. Users can directly access cloud data through the public internet. Here data access administered by a controller through an external client interface. Outsourcing data here is reliable but insecure. The public key database is maintained by controller for public key information stored in the cloud.

The private cloud to the clients formed by the manager is trusted behind an organization firewall. It is fast and scalable when compared to the public cloud. For set of authorized users a database of private key information is maintained by the manager.

Sometimes mobile user acts like data owner and to upload and downloads of cloud data, the data owner has to decide the privileges to access. But, it is difficult to continuous access by single data owner; there is a limited battery lifetime.

The data outsourcing to multiple clouds apart from the mobile applications, by using the same key management technique that uses Cipher text Policy Attribute Based Encryption to achieve high confidentiality and scalability and to reduce the communication workload on data owner. Here the data owner provides the data to multiple clouds along with some attributes and policies. The manager is trusted authority between the multiple cloud service providers and user. To access the data stored in various cloud users has to decrypt based on attributes and policies specified by the data owner. Finally, the original data can access by the authorized users.

Inner process of key management scheme that uses CP-ABE technique is data owner generates the private key, public keys and send to manager and share with trusted users and cloud service provider, respectively. Then a cloud service provider stores the keys from manager in database. The data owner encrypts the data along with the attributes and policies and cloud service provider stores the cipher text in permanent storage. Finally user obtains the keys from the data owner as a trusted user and decrypts the data to yield the original data from multiple clouds.

The above scenario is shown as follows in fig 1.

![Fig. 1.System model of multiple clouds.](image-url)
The proposed work has been implemented in multiple clouds and shows in the fig. 4. The CP-ABE scheme was implemented in Java [8] and uses Java pairing based cryptography (JPBC) [9] to provide the wide range environment. The Java development kit is useful to support the multiple cloud platforms.

Work has been done on the Desktop platform consisting the Microsoft XP operating system, with an Intel Celeron 560 bits and 2.13 GHz speed and 2 GB of RAM. Multiple clouds running instantly via HTTP requests. Through the desktop computer a connection has been established to the internet to access the multiple cloud data. Net Beans IDE (Integrated Development Environment) 7.0 was used to develop the applications on various operating systems. And it is open source, best to support the latest Java technologies. With the Net Beans it is easy to use, fast and smart editing of code.

My SQL is the database used to store the encrypted version of the data. It is popular open source database management system for developing the web-based software applications. The key management is the technique that uses the CP-ABE encryption to achieve the security in a highly scalable manner. The keys will generate, distribute and usage among the data owner, cloud service provider, manager and the user to provide the information as secure and scalable in multiple clouds.

In the implementation the data owner has the lead role. Firstly, the data owner has to connect with the controller based on the IP and Port number provided by the controller. Then, some policies provide to user for security purpose. After that the plain text has to upload to encrypt, the multiple clouds are running instantly in other side. Finally, User should satisfy the policies provided by the data owner. Then the user can decrypt the original data from multiple clouds.

Outsourcing the data to multiple clouds such as Amazon S3 (Simple Storage Service) [12] and Microsoft Azure [14] rather than the single is very beneficial such as reliability and availability are the major futures to multiple clouds. Providing the data without loss of original data to users is one of the major issues. The timings are represented for key generation, Encryption and decryption activities for both single and multiple clouds. This scenario is illustrated in fig 2. During the decryption by the user takes some time, this is not constant. It depends on the user that should satisfy the specified attributes and policies by the data owner.

![Fig. 2. Approximate timings for encryption and decryption of data in single cloud and multiple clouds of plain text size of 1.2MB.](image)

V. CONCLUSION

For secure data outsourcing, the key management Scheme used. Where the authorized users only can access the data stored in multiple clouds based on the satisfaction of required attributes and policies and additionally re-encryption performed for more security. With the multiple clouds there are many benefits, also reduces the burden on the data owner. The dependency will be reduced on a single vendor to deploy the applications in multiple clouds. Hence, examined the challenges such as security, scalability, reliability and availability of data in multiple clouds to trusted authorities are higher than the single cloud.

REFERENCES


AUTHORS BIOGRAPHY


2. C. ShobaBindu is an Associate Professor of Computer Science and Engineering at Jawaharlal Nehru Technological University College of Engineering, Anantapuramu. She obtained her Bachelor degree in Electronics and Communication Engineering, Master of Technology in Computer Science from Jawaharlal Nehru Technological University Hyderabad and Ph.D. in Computer Science and Engineering from Jawaharlal Nehru Technological University Anantapuramu. She has published several Research papers in National International Conferences and Journals. Her research interests includes network security and Wireless communication systems.