Review Paper on Data Security For Unreliable Clouds Using Reliable Encryption

Ritesh B. Tandel
Department of Computer Science
Jagad Guru Dattatray College of Technology, Indore, MP, India

Krishnakant Kishor
Department of Computer Science
Jagad Guru Dattatray College of Technology, Indore, MP, India

Abstract

Data Security is one of the most critical aspects in a cloud computing environment due to the sensitivity and importance of information stored in the cloud. The risk of malicious insiders in the cloud and the failure of cloud services have received a great deal of attention by companies. This paper is related to data security and privacy. The data owner stores the encrypted data in the cloud, and issue decryption keys to authorized users. Then, when a user is revoked, the data owner will issue re-encryption commands to the cloud to re-encrypt the data, to prevent the revoked user from decrypting the data, and to generate new decryption keys to valid users, so that they can continue to access the data. However, since a cloud computing environment is comprised of many cloud servers, such commands may not be received and executed by all of the cloud servers due to unreliable network communications The above problem can be solved by proposing an instant mailing scheme and sending password to the valid user mobile device, which enables the cloud servers to automatically re-encrypt data based on their internal clocks. The solution is to build a new encryption scheme, by sending instant password to the valid data user through their mail and Short Message on Mobile. Every time there will be a different password such that even though the data user get revoked from the system without the knowledge of cloud server he login again with same password. Key terms : data owner, data user, cloud service provider, instant mailing system and instant short message scheme.

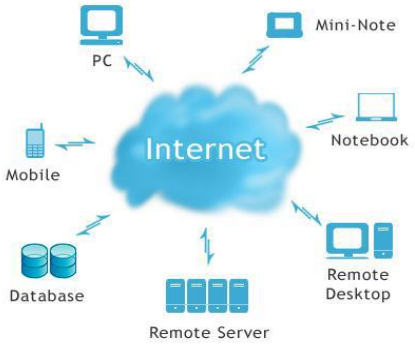
Keywords: Cloud Computing, Re-encryption, Decryption.

I. INTRODUCTION

Cloud computing is a technology that delivers many kinds of resources as services, mainly over the internet, while distributed computing is the concept of using a distributed system consisting of many self-governed nodes to solve a very large problem (that is usually difficult to be solved by a single computer). The idea of the "cloud" simplifies the many network connections and computer systems involved in online services. In fact, many network diagrams use the image of a cloud to represent the Internet. This symbolizes the Internet's broad reach, while simplifying its complexity. Any user with an Internet connection can access the cloud and the services it provides. Since these services are often connected, users can share information between multiple systems and with other users. Examples of cloud computing include online backup services, social networking services, and personal data services such as Apple's Mobile Cloud computing also includes online applications, such as those offered through Microsoft Online Services. Hardware services, such as redundant servers, mirrored websites, and Internet-based clusters are also examples of cloud computing. The security and reliability of this platform is fundamental to the business, as the trust and faith that the customers place on CSP. The use of cloud computing is increasingly popular due to the potential cost savings from outsourcing data to the cloud service provider (CSP). One technique to protect the data from a possible untrusted CSP is for the data owner to encrypt the outsourced data. Flexible encryption schemes such as attribute based encryption (ABE) can be adopted to provide fine grained access control. In an ABE system, a user's keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. ABE allows data to be encrypted using an access structure comprised of different attributes. Instead of specific decryption keys for specific files, users are issued attribute keys. Users must have the necessary attributes that satisfy the access structure in order to decrypt a file. The key problem of storing encrypted data in the cloud lies in revoking access rights from users. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud. A naive solution is to let the data owner immediately re-encrypt the data, so that the revoked users cannot decrypt the data using their old keys, while distributing the new keys to the remaining authorized users. This solution will lead to a performance bottleneck, especially when there are frequent user revocations.

Another alternative solution we propose here is instant mailing scheme to avoid malicious user to hack or trace the password of the data user. Here the instant password is sent to the valid data user's mail with respect to their mail id.

The solution is to build a new encryption scheme, by sending instant password to the valid data user through their mail. Every time there will be a different password such that even though the data user get revoked from the system without the knowledge of cloud server he login again with same password.



The Cloud

II. SYSTEM ARCHITECTURE

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. A cloud is essentially a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. As a distributed system, the cloud will experience failures common to such systems, such as server crashes and network outages. As a result, re-encryption commands sent by the data owner may not propagate to all of the servers in a timely fashion, thus creating security risks.

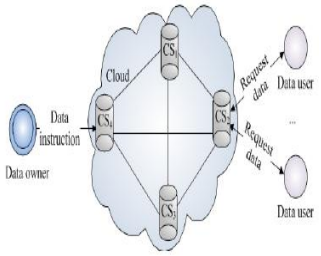


Figure show the cloud architecture with data owner, cloud service provider and data user

To illustrate, let us consider a cloud environment shown in Fig. 2, where the data owner's data is stored on cloud servers CS1, CS2, CS3, and CS4. Assume that the data owner issues to CS4 a re-encryption command, which should be propagated to CS1, CS2, and CS3. Due to a network outage, CS2 did not receive the command, and did not re-encrypt the data. At this time, if revoked users query CS2, they can obtain the old cipher text, and can decrypt it using their old keys. A better solution is to allow each cloud server to independently re-encrypt data without receiving any command from the data owner. The disadvantage was Bulk Data Transfers- Bringing a lot of data into or out of a cloud instance takes a good deal of time. Without a high-capacity connection, it could take days to load all that data. So in this paper we propose a reliable re-encryption scheme in unreliable clouds (R3 scheme for short). R3 is a time-based re-encryption scheme; this allows each cloud server to automatically re-encrypt data based on its internal clock. The basic idea of the R3 scheme is to associate the data with an access control and an access time.

- We propose an automatic, instant mailing system suitable for cloud environments.
- We Proposed an Automatic Short Message system on Mobile valid user mobile device.
- We extend an ABE scheme by advanced mailing password to the valid data user
- Our solution does not require perfect clock synchronization among all of the cloud servers to maintain correctness.

A. The advantage of this R3 scheme

- When you use internet with the cloud services then your company will have lots more room to store the files and that they need to store.
- User identified the data losses.
- Data security and access control when users require data for sharing on cloud server.

III. RELATED WORK

Researchers have proposed storing encrypted data in the cloud to defend against the CSP [1], [2]. Under this approach, users are revoked by having a third party to re-encrypt data such that previous keys can no longer decrypt any data [14].The solution by [15] for instance, lets the data owner issue a re-encryption key to an untrusted server to re-encrypt the data. Their solution utilizes PRE [6], which allows the server to re-encrypt the stored cipher text to a different cipher-text that can only be decrypted using a different key. During the process, the server does not learn the contents of the cipher text or the decryption keys. ABE is a new cryptographic technique that efficiently supports fine grained access control. The combination of PRE and ABE was first introduced by [9], and extended by [8], [11]. In [8], a hierarchical attribute-based encryption (HABE) scheme is proposed to achieve high performance and full delegation. The main difference between prior work and ours is that we do not require the underlying cloud infrastructure to be reliable in order to ensure correctness. Our scheme relies on time to re-encrypt data. However, in a cloud, the internal clock of each cloud server may differ. There have been several solutions to this problem. For instance, [10] proposed a probabilistic synchronization scheme, which exchanges messages to get remote servers' accurate clocks with high probability. At [11] used message delay to estimate the maximal difference between two communicating nodes to synchronize the clocks. At [13] proposed a clock synchronization scheme for cloud environments. At [14] the encryption and re-encryption is done using ABE technique. In this paper we have used instant mailing scheme for instant password.

IV. CONCLUSION AND FUTURE ENHANCEMENT

The proposed R3 scheme, a new method for managing access control based on the cloud server's internal clock. Our technique does not rely on the cloud to reliably propagate re-encryption commands to all servers to ensure access control correctness. We showed that our solutions remain secure using instant mailing system and Mobile password System. The future enhancement to this project is planned such that when data user request for a file if he is valid user must connected his/her mobile device with the accessible device to receive password.

REFERENCES

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security, 2010.
[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," Communications of the ACM, 2010
[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT, 2005.
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS, 2006.
[5] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. of IEEE Symposium on S&P, 2007
[6] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Advances in Cryptology–EUROCRYPT, 1998.
[7] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. of ACM CCS, 2008.
[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. of ACM CCS (Poster), 2010.
[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. of IEEE INFOCOM, 2010.
[10] F. Cristian, "Probabilistic clock synchronization," Distributed Computing, 1989
[11] K. Romer, "Time synchronization in ad hoc networks," in Proc. of ACM MobiHoc, 2001.
[12] P.Ramanathan , K.Shin and R.Butler , "Fault Tolerant Clock Sysnocronisation in distributed System," Computer 2002
[13] N. Antonopulos and L.Cillam, "Cloud Computing ", Principal , system and Application ," Spring Publishing Company,2010
[14] Qin Liu, Chiu C. Tan, Jie Wu and Guojune Wang , "Re Encryption in Unrelaible Clouds" IEEE ,2011
[15] Mohna Priya M, Premkumar . M & Jayanthi M.G , "Data Security for Unreliable Clouds using Raliable Encryption" October 2013