Available online at http://www.journalcra.com

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

International Journal of Current Research
Vol. 6, Issue, 04, pp.6218-6220, April, 2014

ISSN: 0975-833X

RESEARCH ARTICLE

RELIABLE RE-ENCRYPTION IN UNRELIABLE CLOUDS

Rajkumar Gaikwad, Kedarnath Raywade, *Prasad Guntuk, Dnyaneshwar Shinde

Department of Computer Engineering, Pune University, Pune, India

ARTICLE INFO

Article History:
Received 26th January, 2013
Received in revised form
24th February, 2014
Accepted 10th March, 2014
Published online 23rd April, 2014

Key words:
Attribute-based encryption (ABE),
Cloud computing, Re-encryption, R3.

ABSTRACT

The organization stores encrypted data on cloud and issues decryption keys to authorized users. Data owner issues decryption keys to authorized users. When user leaves organization, then he/she becomes unauthorized user for data access. When a user is left the organization, then data owner will issue re-encryption commands to the cloud to re-encrypt the data. So we prevent the left user from decrypting the data by using the old decryption key. And to generate new decryption keys to valid users only. So only authorized users can continue to access the data. By considering cloud architecture, such commands may not be received properly due to unreliable network communications. So we proposing a time based re-encryption scheme, which enables the cloud servers to automatically re-encrypt data based on their internal clocks of system. Within given time period users can access data, after timestamp they cannot access data.

INTRODUCTION

With rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs) (Jie Wu and GuojunWangy 2011), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data. We are proposing time based reliable re-encryption scheme. This scheme is based on the internal clock of cloud server, where each cloud server automatically re-encrypts the data based on an internal systems clock. The current system facilitates only one time encryption on the data file. This encrypted data is stored on the cloud server. Different users in an organization are allocated keys for accessing the data. When a user intends to access the data, he/she needs to submit the key allocated to them for accessing the system. In course of time, some users who are unauthorized from accessing the data file would be in a position to still access the file and retrieve the information. User access management becomes very critical for the organizations. In this paper we are providing data confidentiality (Jie Wu and GuojunWangy 2011), in which the file contents can only be known to data users with valid keys. The CSP is not considered a valid data user also the cloud servers should not re-encrypt any file unnecessarily. This means that a file that has not been requested by any data user should not be re-encrypted.

***Corresponding author: Prasad Guntuk,** Department of Computer Engineering, Pune University, Pune, India.*

We ensure data access control, where correctness requires data user with invalid keys cannot decrypt the file. In data consistency, all data users who request file F, should obtain the same content in the same time slice

Related Work

Table 1. Literature survey

S.N.	Paper Name	Advantages	Disadvantages
1	Reliable Re-encryption in Unreliable Clouds(1)	Providing time based automatic re-encryption.	Not considering space complexity.
2	Attribute-based encryption For fine-grained access control of encrypted data(3)	It Provide Security. ABE allows data to Be encrypted using An access structure Comprised of Different attributes.	This solution will lead to a performance bottleneck, especially when there are frequent user revocation
3	Proxy Re-encryption Systems for Identity-based Encryption(5)	Data Confidentiality	Do not consider The underlying system architecture of The cloud Environment. Command can Not be reached to every server, such as server crashes and network outages.
4	Cryptographic Cloud Storage(2)	Easy to Implement And provide Security	It may happen to hack the keys for decryption of Data.

We are storing encrypted data in the cloud to defend against the CSP (Kamala and Lauter 2010). Under this approach a third party to re-encrypt data such that previous keys can no longer decrypt any data. The solution by for instance, lets the data owner issue a re-encryption key to an untrusted server to re-encrypt the data. Their solution utilizes ABE (Goyal *et al.*, 2006) 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. In PRE (Toshihiko Matsuo ?), this allows the server to re-encrypt the data and stored cipher text to a different cipertext that can only be decrypted using a different key. During the process, the server does not learn the contents of the cipertext or the decryption keys. This concept does not considering the underlying architecture of cloud so we are considering cloud architecture by providing time based automatic re-encryption scheme (Jie Wu and GuojunWangy 2011) in which file is encrypted and decrypted on the time basis automatically.

Proposed System

The proposed system works on the process of re-encryption for ensuring data security. We are considering cloud architecture by providing time based automatic re-encryption scheme (Jie Wu and GuojunWangy 2011) in which file is encrypted and decrypted on the time basis automatically. This is a time-based re-encryption scheme, in which each cloud server to automatically re-encrypt data based on its internal clock. The idea of this scheme is to associate the data with an access control and an access time. Each user is issued keys associated with attributes and attribute effective times. The data can be decrypted by the users using the keys with attributes satisfying the access control, and attribute effective times satisfying the access time. Unlike the command-driven re-encryption scheme, the data owner and this share a secret key, with which each cloud server can re-encrypt data by updating the data access time according to its own internal clock. Even through this scheme relies on time it does not require perfect clock synchronization among cloud servers.

System Architecture

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures of the system, System architecture is primarily concerned with the internal interfaces among the system's components or subsystems, and the interface between the system and its external environment, especially the user. System architecture can be contrasted with system architecture engineering, which is the method and discipline for effectively implementing the architecture of a system. As shown in following Fig (1). Normal user, owner and admin all act as a client and through browser they communicate to server for to accessing, manipulating data and user management module.

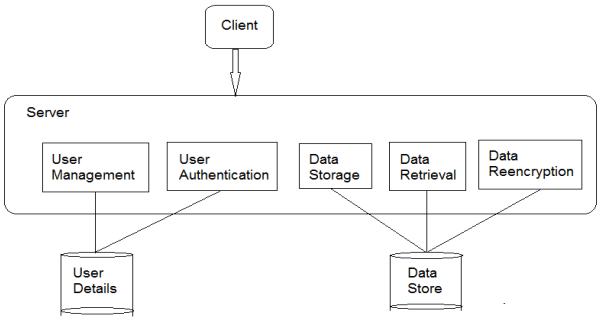

Fig. 1. System Architecture

Algorithm

System based on two algorithms: AES algorithm and Reliable Re-encryption (R3) algorithm. R3 algorithm has two phases, Initial Encryption Phase-I and Re-encryption Phase-II.

A.Initial Encryption (Phase-1)

1.Owner uploads data on a centralized location
2.Generate random key using current timestamp and encrypt file using AES
3.Store encrypted data with current timestamp
4.Identify active users in the system, distribute key generated to users which is stored in user-file mapping data store.
5.During data access, which if valid, user Gets the valid data.

B. Re-encryption (Phase-2)

1.When Admin changes the user status from active to inactive, the re-encryption module is activated
2.The data is decrypted using the existing key
3.A new random key is generated using the new timestamp and file encrypted using AES
4.The re-encrypted data is stored with new timestamp
5.Identify current active users in the system and distribute new key generated to users which is stored in user-file mapping data store for active users only.
6.User specifies this key during data access, which if valid, user gets the valid data.

While Receive a request R (File; TSi)
Do
If current time is later than ti+1 or changes in user management
Then
Re-encrypt the file Window i with TSi
Else
Hold on the read command until ti+1

C. AES Algorithm

AES (Advance Encryption Standard): It is used for Encryption, Decryption and Key Generation purpose.
The AES fixes the block length to 128 bits, and supports key lengths of 128, 192 and 256 bits. Following Fig 2. Shows .basic block diagram of AES.

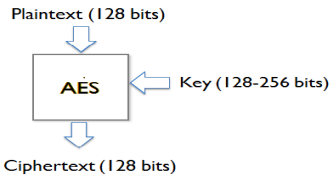

Fig. 2. Basic block of AES

Conclusion and Future Scope

We are providing Access Control Correctness in which data user with invalid keys cannot decrypt the file and in data Consistency all data users who request file f should obtain the same content in the same time slice. The file content can be known to the data user with valid keys and the cloud server should not re-encrypt any file unnecessarily. Instead of using R3 (time based) Re-encryption algorithm by considering all the conditions and situation we can develop another algorithm and provide more security to the essential data on cloud servers.

REFERENCES

Armbrust M., A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloudcomputing," *Communications of the ACM*, 2010.

Ateniese G., K. Fu, M. Green, and S. Rosenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, 2006.

Bethencourt J., A. Sahai, and B. Waters, "Ciphertext-policy attributebasedencryption," in *Proc. of IEEE Symposium on S&P*, 2007.

Boldyreva, A. SV. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. of ACM CCS, 2008.

Cristiano F., "Probabilistic clock synchronization," *Distributed Computing*,1989.

Goyal V., O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS, 2006.

Jie Wu, and GuojunWangy, "Reliable Re-encryption in Unreliable Clouds", School of Information Science and Engineering, 2011.

Kamala S. and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security, 2010.

Ramanathan P., K. Shin, and R. Butler, "Fault-tolerant clock synchronization in distributed systems," *Computer*, 2002.

Romer K., "Time synchronization in ad hoc networks," in *Proc. of ACMMobiHoc*, 2001.

Sahai A. and B. Waters, "Fuzzy identity-based encryption," *Advancesin Cryptology–EUROCRYPT*, 2005.

Toshihiko Matsuo "Proxy Re-encryption Systems for Identity-based Encryption" NTT DATA COROPORATION

Yu S., C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, andfine-grained data access control in cloud computing," in *Proc. of IEEEINFOCOM*, 2010.

****