ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A Secure Data Forwarding Erasurecode based Cloud Storage System

Dr.G.Ravi[1], V.Sobanadevi[2]

Associate Professor & Head, Dept. of Computer Science, Jamal Mohamed College, Trichy. Tamilnadu, India[1]

Research Scholar Dept.of.Computer Science, Jamal Mohamed College, Trichy. Tamilnadu, India [2]

ABSTRACT: In this paper some problem of forwarding data to another user by storage servers directly under the command of the data owner. We consider the problem level model that consists of distributed storage servers and key servers. Since automatic generally storing cryptography keys in a single access device is risk, a user distributes his cryptographic key to key servers that shall perform cryptographic functions on behalf of the user are very high protected by secure mechanisms. To good formal the distributed structure of systems, we need the servers independently perform all operations. We propose a new threshold Adaptive Encryption Scheme and integrate it with a secure decentralized code to form a secure distributed storage system. The encryption scheme support encoding operations and over encrypted messages and resending operations. over encrypted and encoded information. The rigid integration of encoding and encryption, and forwarding create the Storage system efficiently meets the requirements of data healthiness, data privacy, and data forwarding. Accomplishing the assimilation with consideration of a distributed structure is performing. Our system meets the requirements that storage servers independently perform encoding and re-encryption and key servers independently to perform incomplete decryption.

KEYWORDS*:* Re-encryption key, Adaptive Encryption Scheme

I. INTRODUCTION

Storing data in a third party's cloud system causes serious concern over data confidentiality and there are some functionality restrictions on the storage system. We focus on designing a cloud storage system for data robustness, confidentiality, and improve the functionality of the storage server. These all can be achieved through a threshold Adaptive Encryption Scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated.

1.2 OBJECTIVES

✓ Applying anomaly detection by learning the normal behavior of an insider in terms of the sensitivity level of the data she is usually exposed to.
✓ Improving the process of handling leakage incidents identified by other misuse detection systems by enabling the security officer to focus on incidents involving more sensitive data.
✓ Implementing a (DMBAC) Dynamic Misuse ability-Based Access Control, designed to regulate user access to sensitive data stored in relational databases;
✓ Reducing the misuseability of the data.

II. SECURITY BROKEN

In existing method we had to use the process, messages are first encrypted by the owner and then stored in a storage server. When a user wants to share his messages, he sends a re-encryption key to the storage server. The storage server re-encrypts the encrypted messages for the authorized user. Thus, their system has data confidentiality and supports the data forwarding function. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages. When he wants to use a message, he needs to retrieve the codeword symbols from storage servers, decode them, and then decrypt them by using cryptographic keys.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

➢ The user has to do most computation and the communication traffic between the user and storage servers is high.
➢ The user has to manage his cryptographic keys. If the user's device of storing the keys is lost or compromised, the security is broken.

III. ADAPTIVE ENCRYPTIVE

In our proposed approach novel architecture for adaptive encryption of public cloud databases that offers a proxy-free alternative to the system proposed. The proposed architecture guarantees in an adaptive way the best level of data confidentiality for any database workload. The adaptive encryption scheme, which was initially proposed for applications not referring to the cloud, encrypts each plain column into multiple encrypted columns, and each value is encapsulated into different layers of encryption.

3.1. INDEPENDENT LEVEL

- It will be supports encoding, forwarding, and partial decryption operations in a distributed way.
- Each storage server independently performs encoding and re-encryption and each key server independently perform partial decryption.

IV. PROBLEM DEFINITION

The most common approach for representing user behavioral profiles is by analyzing the SQL statement submitted by an application server to the database (as a result of user requests), and extracting various features from these SQL statements. Data represent today an important asset for companies and organizations. Some of these data are worth millions of dollars and organizations take great care at controlling access to these data, with respect to both internal users, within the organization, and external users, outside the organization. Data security is also crucial when addressing issues related to privacy of data pertaining to individuals; companies and organizations managing such data need to provide strong guarantees about the con-dentiality of these data in order to comply with legal regulations and policies.

V.METHODOLOGIES

Methodologies are the process of analyzing the principles or procedure for analyzing and preserving the privacy of user details.

➢ **Key generator (PK and SK)**

The key generator the public key and secret key for the new user. These public and private or secret keys are used to encrypt and decrypt the messages for data confidential purpose. Usually public key is used to encrypt the data and secret key or private key is used to decrypt the cipher text to get the original plain text.

➢ **Share to Key server**

The user has to share his secret key to randomly chosen key server. This secret key is used to decrypt the encoded message when the authenticated person wants to share his data or retrieve his data.

➢ **Data storage**

- **Storing data in the storage server**

In the data storage phase, user A encrypts his message M and dispatches it to storage servers. A message M is decomposed into k blocks m_1, m_2, ……., m_k and has an identifier ID. User A encrypts each block m_i into a cipher text C_i and sends it to v randomly chosen storage servers. Upon receiving cipher texts from a user, each storage server linearly combines them with randomly chosen coefficients into a codeword symbol and stores it.

➢ **Data forwarding:**

- **Forward data to another user**

When user A wants to forwards his encrypted message with an identifier ID stored in storage servers to user B such that B can decrypt the forwarded message by his secret key.

To do so, A uses his secret key SK_A and B's public key PK_B to compute a re-encryption key $RK^{ID}_{A\rightarrow B}$ and then sends $RK^{ID}_{A\rightarrow B}$ to all storage servers. Each storage server uses the re-encryption key to re-encrypt its codeword symbol for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

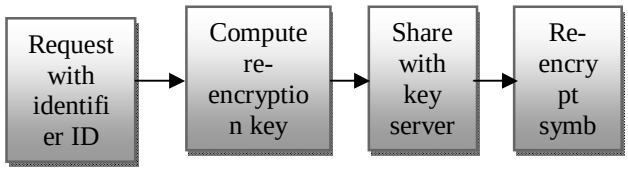
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

later retrieval requests by B. The re-encrypted codeword symbol is the combination of cipher texts under B's public key.

This type of secure distributed cloud storage system can be used in Google mail storage system to provide secure storage service. This type of secure distributed cloud storage system can be used in Dropbox storage services or Amazon cloud storage service.



V. FUTURE WORK

In particular process, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both.

VI. CONCLUSION

The threshold Adaptive Encryption Scheme supports encoding and forwarding, and influenced decryption process in a sending way. To decrypt a message of k parts that are encrypted and encoded to n secret code symbols, each key server only has to in some measure decrypt two codeword symbols in our system. By using the threshold Adaptive Encryption Scheme, we consider a safe cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Moreover, each storage server in matching performs encoding and re-encryption and each key server independently perform partial decryption.

REFERENCES

1.A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, "Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proc. Fifth Symp. Operating System Design and Implementation (OSDI) , pp. 1-14, 2002.

2.M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29- 42, 2003.

3.H.-Y. Lin and W.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

4.R. Bhagwan, K. Tati, "Total Recall: System Support for Automated Availability Management," Proc. First Symp. Networked Systems Design and Implementation (NSDI),2004.

5.A.G. Dimakis, V. Prabhakaran, "Ubiquitous Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes," Proc. Fourth Int'l Symp. nformation Processing in Sensor Networks (IPSN), pp. 111- 117, 2005.