PROTECTED DATA FORWARDING BY ERASURE CODING TO CLOUD STORAGE SYSTEM

[1]*P. CHANDU*, [2]*DNVSLS INDIRA*
[1]M. Tech, CSE Dept, G.E.C. Gudlavalleru.
Email: chandu535@gmail.com.
[2] M.Tech, CSE Dept, Asst. Professor, G.E.C., Gudlavalleru.
Email: indiragamini@gmail.com.

ABSTRACT-*For providing long-term storage services over the Internet we use a cloud storage system that is consisting of a collection of storage servers. A third party's cloud system can be used for storing data but it leads to a question as we are concerned over data acquaintance. We rely on encoding schemes not only for protecting data acquaintance, but also it limits the functionality of the storage system because some of the operations are supported by encoded data. Making a secure and reliable storage system that provides multi-functioning feature is challenging when the storage system is under distributed state and has no central authority. We suggest a threshold proxy re-encoding scheme and integrate it with an un-unified erasure code in such a way that the secure distributed storage system is developed. The distributed storage system supports the secure and robust data storage and retrieval and also it lets every single user in forward his data that is present in the storage servers to different user without retrieving back the data. The proxy re-encoding scheme is the main technical contribution that supports many encoding operations over encoded messages as well as forwarding operations which are over encoded and sufficiently encoded messages. Our method fully integrates encoding and forwarding. As per the information that we analyzed, we suggest you suitable parameters that are to be considered while the number of copies of a message is to be dispatched to different storage servers and also to the storage servers which are queried by a key server. These parameters provide flexibility in adjusting the number of storage servers and firmness.*

1. INTRUDUCTION

As high-speed networks and omnipresent Internet access become available in the latest years, many services are being provided through the Internet as a result of which users are facilitated to use them from any part of the globe irrespective of time. We can take e-mail service probably as the most popular example. The resources on the Internet are treated as a unified entity (i.e., a cloud) according to the theory of cloud computing. The customers who are using cloud computing are just interested in storing the information they don't want to know how the infrastructure of storing. In this, we explored firmness, acquaintance, and operations structure of cloud computing. Cloud storage system is not a single storage server here the architecture will be in the distributed format. So there will be number various server storages which are independent. For storage systems a key concern is data robustness. We can store data in storage system in various methods. Replicate a message is one way that gives robustness of data. Replication of a message means the copy of data will store in each and every server for the backup purpose. This is what we call robustness because we can retrieve the message any time until the server exists. Encoding a message is another way to keep robustness. Encoding procedure is it convert k symbols to a form of n symbols code words with help of erasure coding. Codeword symbols will present in each and every storage system. A storage server failure corresponds to an erasure error of the codeword symbol. As long as the number of failure servers is under the tolerance threshold of the erasure code, from codeword symbols which we have stored in various servers we can recover the message with the help of decoding process. So naturally there will be a tradeoff between tolerance threshold of server failures and size of storage servers. Codeword symbol will computes with the help of decentralized erasure code for the sake of

message. Thus, the encoding process for a message can be split into n parallel tasks of generating codeword symbols. For distributed storage system efficient one is decentralized erasure code. After the message symbols are sent to storage servers, each storage server independently computes a codeword symbol for the received message symbols and stores it. This finishes the encoding and storing process. For the sake of security of messages in storage servers we have to follow, messages can be encrypted with the help of cryptographic method which we have to do initially before using an erasure code method. If the user wants to get his message, he have to get the codeword symbols and after he have to perform decoding. At last he has to decrypt as final stage with the help of cryptographic keys. Above mentioned procedure has some crisis or following problems:

- Since the communication traffic is more the computations done by user between him and storage servers are high.
- The cryptographic keys are to be managed by user himself as keys cannot be lost or compromised.
- It is hard for storage servers to support functions other than data storing and retrieving, etc.

For example, storage servers cannot send a user's messages to another user. After retrieving, decoding and decrypting the user have to send these to another user for sake of getting message. In this paper, discuss the consequences in forwarding data among users through the usage of storage servers directly by the command of owner. We assume a system model that comprises of distributed storage servers and key servers. Storing of cryptographic keys in a single device is considered risky; we suggest each user to distribute his cryptographic key to other key servers that perform the cryptographic functions on behalf of the user even in his absence. The security mechanisms provide a wide and tight range of security to these key servers. To well fit the distributed structure of systems, we require that servers independently perform all operations. With this consideration, we propose a new threshold proxy re encoding scheme and associate it with a secure decentralized code to build a secure distributed storage system. The encoding scheme supports encoding operations over encoded messages and forwarding operations over encoded and messages which were encoded. The encoding one perfect integration and forwarding makes the storage system efficient enough to meet the requirements such as data firmness, data acquaintance, and data forwarding. Expecting the integration with in the distributed structure is somehow critical thing. Her we proposed a system that has the features servers themselves performs encoding and re-encoding independently. Not only that and also key servers which does partial decryption. When compared to previous ones it is most general to applicable that means flexible. This setting provides you flexibility adjustment within the number of storage servers and firmness in the cloud storage architecture.

2. SYSTEM DEVELOPMENT

a) Construction of Cloud Data Storage (Admin Module):

- The username and password for server setup process can be set by the admin after he pass his login.
- In this process a remote servers IP-address has to be set by admin initially and send them to the receiver.
- The details provided above can be viewed when ever required by clicking the key server.
- The passed IP-addresses are noted in available storage server and when we click on this button for viewing currently available IP-addresses.

b) Data Encoding

➢ **Cloud Login Module:**

- Details such as Username, e-mail, Password, DOB, Gender, Location and these were stored in database of the cloud system.
- For using and entering, the user has to register his details into the cloud system and has to activate it using code will send to e-mail.
- Users have to open account and view the

code generated by the cloud System.

➢ **Upload Module:**

- By browsing the system the user has to choose one file that is to be uploaded.
- The cloud server can give the encoded form of the uploading file.
- In this new folder will be created for storing the files.

c) Data Forwarding

- In File Forward process contains the selected file name, e-mail of the forwarder and enters the code to the forwarder.
- Apart from checking his account properly a user can also view the code that is forwarded from the previous user.
- The current user has to login again into the cloud system to check the previously received details.
- If the forwarded file is present n receive details only then the user is allowed to go to the download process.

d) Data Retrieval Module

- The server process can be run, means it can be connected with its particular client and only client has to download the file to download file key.
- In the file key downloading process the fields to be filled are username, filename, question, answer and code.
- By pressing the download button the client is allowed to view the encoded key.
- The client can view and use the file if and only if the file is completely downloaded.

3. RELATED WORK

We briefly review distributed storage systems, proxy re-encoding schemes, and integrity checking mechanisms.

2.1 Distributed Storage Systems

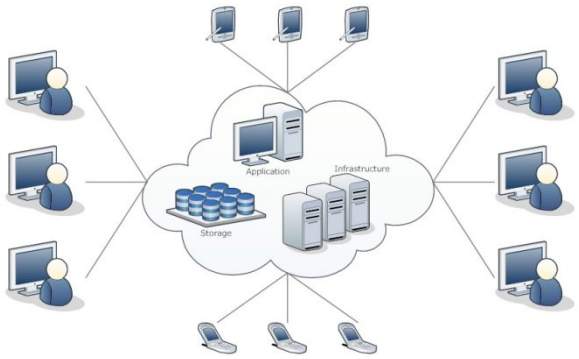
We briefly review distributed storage systems, proxy re-encoding schemes, and integrity checking mechanisms.

2.1 Distributed Storage Systems

At the early years, the Network-Attached Storage and the Network File System provide extra storage devices over the network such that a user can access the storage devices via network connection. Afterward, many improvements on scalability, firmness, efficiency, and security were proposed. A decentralized architecture for storage systems offers good scalability, because a storage server can join or leave without control of a central authority. To provide firmness against server failures, a simple method is to make replicas of each message and store them in different servers but this method is expensive as z replicas result in z times of expansion. One way to reduce the expansion rate is to use erasure codes to encode messages. A message is encoded as a codeword, which is a vector of symbols, and each storage server stores a codeword symbol. A storage server failure is modeled as an erasure error of the stored codeword symbol. Random linear codes support distributed encoding, that is, each codeword symbol is independently computed. To store a message of k blocks, each storage server linearly combines the blocks with randomly chosen coefficients and stores the codeword symbol and coefficients. To retrieve the message, a user queries k storage servers for the stored codeword symbols and coefficients and solves the linear system. Considering the case that n = AK for a fixed constant a. They showed that distributing each block of a message to v randomly chosen storage servers is enough to have a probability 1 - k/p- o(1) of a successful data retrieval, where v = b*l*nk, b > 5a, and p is the order of the used group. The s parsity parameter v = b*l*nk is the number of storage servers which a block is sent to. The larger v is, the communication cost is higher and the successful retrieval probability is higher. The system has alight data acquaintance because an attacker can compromise k storage servers to get the message. Someone addressed firmness and acquaintance issues by presenting a secure decentralized erasure code for the networked storage system. In addition to storage servers, their system consists of key servers, which hold cryptographic key shares and work in a distributed way. As long as the number of available key servers is over a threshold t, the message can be successfully retrieved with an overwhelming probability.

2.2 Proxy Re-Encoding Schemes

In a proxy re-encoding scheme, a proxy server can transfer a cipher text under a public key PKA to a new one under another public key PKB by using the re-encoding key RKA!B. The server does not know the plaintext during transformation. Researchers proposed some proxy re-encoding schemes and applied them to the sharing function of secure storage systems.



In their work, messages are first encoded by the owner and then stored in a storage server. When a user wants to share his messages, he sends a re-encoding key to the storage server, then it re-encodes the messages for the authorized user. Thus, their system has data acquaintance and supports the data forwarding function. Our work further integrates encoding, re-encoding, and encoding such that storage firmness is strengthened. Type based proxy re-encoding schemes proposed by researchers. A user can decide which type of messages and with whom he wants to share in this kind of proxy re-encoding schemes. Key-private proxy re-encoding schemes are developed. In a key-private proxy re-encoding scheme, given a re-encoding key, a proxy server cannot determine the identity of the recipient. This kind of proxy re-encoding schemes provides higher privacy guarantee against proxy servers. Although most proxy re-encoding schemes use pairing operations, there exist proxy re-encoding schemes without pairing.

2.3 Checking of Integrity Functionality

A key interesting feature in cloud computing is it is capable of checking integrity functionality. In cloud storage after the completion of user's data updating into the storage system, user never contain the data right away with him. For confirming the data which was present in storage system is secured or not users have to know. That storage servers are efficient or not for that purpose the provable data possession theory and also at the same time proof of storage notion are proposed.

4. CONCLUSION

In this paper, we assume a cloud storage system consists of storage servers and key servers. We associate a newly proposed threshold proxy re-encoding scheme and erasure codes over exponents. The encoding, forwarding, and partial decryption operations are helped by threshold proxy re-encoding scheme in a separated way. To decode a message of 1000 blocks, they are encoded into n codeword symbols restricting each key server to partially decrypt only two codeword symbols. By the of threshold proxy re-encoding scheme, we allow a secure cloud storage system which allows secure data storage and forwarding functionality in an un-unified structure, apart from that each storage server individually performs encoding and re-encoding and each key server separately perform partial decryption. The newly proposed content and storage systems are highly compatible to addressable file systems and storage system. Our storage servers and key servers work as storage nodes in a content referable storage system for storing content addressable blocks and as access nodes for allowing a front-end layer such as a traditional file system interface. Study in detail can be done by continuing this project.

5. REFERENCES

[1] "Ocean store: An Architecture for Global-Scale Persistent Storage," Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190- 201, 2000.

[2] "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.

[3] "Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted

Environment," Proc. Fifth Symp. Operating System Design and Implementation (OSDI), pp. 1-14, 2002.

[4] "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Failures," Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143-158, 2005.

[5] "Tahoe: The Least-Authority File system," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008.

[6] "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

[7] "The Newcastle Connection or Unixes of the World Unite!," Software Practice and Experience, vol. 12, no. 12, pp. 1147-1162, 1982.

[8] "Design and Implementation of the Sun Network File system," Proc. USENIX Assoc. Conf., 1985.

[9] "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29- 42, 2003.

[10] "Pond: The Ocean store Prototype," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 1-14, 2003.

[11] "Total Recall: System Support for Automated Availability Management," Proc. First Symp. Networked Systems Design and Implementation (NSDI), pp. 337-350, 2004.

[12] "Omnipresent Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 111- 117, 2005.

[13] "Decentralized Erasure Codes for Distributed Networked Storage," IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.

[14] "Proxy Cryptosystems: Delegation of the Power to Decrypt Cipher texts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54-63, 1997.

[15] "Divertible Protocols and Atomic Proxy Cryptography," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 127-144, 1998.

[16] "Improved Proxy Re-Encoding Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

[17] "Type-Based Proxy Re-Encoding and Its Construction," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), pp. 130-144, 2008.

[18] "Key-Private Proxy Re-Encoding," Proc. Topics in Cryptology (CT-RSA), pp. 279-294, 2009.

[19 "CCA-Secure Proxy Re-Encoding without Pairings," Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC), pp. 357-376, 2009.

[20] "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS), pp. 598-609, 2007.

Authors:

P. CHANDU received B.Tech Degree in Computer Science and Engineering from Sri Sunflower College of Engineering and Technology. He is currently M.Tech student in Computer Science and Engineering Department in Gudlavalleru Engineering College. And his research interested areas are in the field of Cloud computing and Data Mining.

DNVSLS INDIRA having 7+ years of Teaching Experience, currently she is working as an Assistant Professor in Gudlavalleru Engineering College. She has completed her M.Tech from JNTU Kakinada and she got First Rank in M.Tech. Her research interested areas are Data mining, Network Security and Cloud Computing.