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. 4, Issue 4, April 2016

Ensuring Data Security in Cloud by Using Erasure Code Method

Mandar D.Shinde[1], Ashish K. Patel[2], Rajesh B. Vishwakarma[3], Wilson A. Waghmare[4] ,

Prof. Umesh Talware[5]

UG Students, Dept. of Information Technology, Dhole Patil College of Engineering, Pune, Maharashtra, India[1,2,3,4]

Assistant Professor, Dept. of Information Technology, Dhole Patil College of Engineering, Pune, Maharashtra, India[5]

ABSTRACT: Cloud storage service is collection of storage servers, its provide storage service on internet. In third party cloud server stored data may cause serious concern. There is some limit of functionality of storage service as to save data confidentially use encryption scheme but few operations are supported over the encrypted data. Distributed storage system which have no centralized author their using is very challenging. We define proxy re-encryption scheme with erasure code help for secure data. To store data secularly and for easily retrieval distributed storage system support efficiently and the user can forward data to another user without retrieving back. Proxy encryption scheme support encoding operation over encrypted massage and it was main technical operation as well as forwarding data as encrypted massage. We suggest to determine copies of massage which is send to the storage server, distributed storage service stored data on storage server and key server which is work independently. These define parameters allow more flexibility adjustment between number of storage server and robustness.

KEYWORDS: Decentralized erasure code, proxy re-encryption, threshold cryptography, secure storage system.

I. INTRODUCTION

In recent years, many services are provided on the Internet such that users can use them from anywhere at any time. For example, the email service is probably the most popular one. A cloud which define unified entity on the internet. Users don't have concern about hoe to computing data and how it was stored. In our studies we focus on security, robustness and functionality. A cloud server define as large scale storage which contain among independent storage server. The major requirement of the storage service is data robustness. To store data on storage server there is among of way. When massage send to the cloud server one copy has been stored in cloud and then one copy save on proxy server. Another way is K block massage stored in N block as codeword symbol. Each storage server define the file in unique code word symbol. The massage can be recover from the code word symbol which is stored on cloud server by decoding the massage. Each code symbol of massage compute independently is as decentralized erasure code. To generated codeword symbol each encoding massage divide in parallel task. A decentralized erasure code is suitable for use in a distributed storage system. Further each symbol send to storage server and each storage server can independently compute the codeword symbol for the received massage symbol and store it. This is encoding and storing process and retrieving process. Data may not confidently secure on third party cloud server. To provide security in storage server user can encrypted massage by applying erasure code. When user want to use massage he need retrieve codeword symbol from storage server decrypt massage by cryptographic key. There are some challenges to encoding and encrypt massage one of the challenge is the user has to do most computation and the communication traffic between the user and storage servers is high. Second, the user has to manage his cryptographic keys. Security is broken when the user lost device key. Apart from the data storage and data retrieval challenging to support others function to cloud storage server such as, Storage server not able to forward massage directly to another sssss user Hence the user can first store massage, retrieved and then forward to another user. In our studies we can use command with this storage server can directly forward massage to another user without back on. We assume the system model is combination of distributed storage server and key server. These key servers are highly protected by security mechanisms. In distributed service have to all storage server function independently. As using proxy encryption scheme we integrate it and provide security to decentralized scheme. The encrypted scheme can work encoding massage of

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. 4, Issue 4, April 2016

storage server and forwarding encrypted massage to another user. In distribution service challenging work is to storage servers have to meet all requirement like data robustness, data security and data functionality which is help for the improve integrity encoding, encryption and forwarding massage. Our proposed system meets the requirements the storage servers independently create encoding or encrypted massage and key server perform partially decryption. In our studies we consider the system in a more general setting than previous works. This setting allows more flexible adjustment between the number of storage servers and robustness.

II. LITERATURE SURVEY

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

2.1 Distributed storage system

In the recent year, a user can access the storage devices via network connection the Network-Attached Storage (NAS) and the Network File System (NFS) provide extra storage devices over the network with improvement in scalability, security, efficiency, robustness. Storage server can work efficiently as there is no any centralize authority access the stored data effectively. Make replica of each massage and stored it on different server it was best method of provide robustness against the server failure. Hence this method is costly as Z replicas result in Z time Expansion. A massage will be encoded and encrypted in codeword symbol and it will store on each storage server. A storage server failure is modeled as an erasure error of the stored codeword symbol. Random linear codes support distributed encoding, that is, each code word symbol is independently computed. The massage will be stored in blocks and then each storage server can combine the all blocks linearly with randomly chosen coefficient. And store codeword symbols and co efficient. In [6] Author define that robustness and confidentiality issues by presenting a secure decentralized erasure code for the networked storage system. Storage service in their system consist key server which contain cryptograph key share and work in distributed key.in their system massages can encoding then encrypted which stored in storage server and to retrieve massage key server van decrypt massage partially.

2.2 Proxy Re-Encryption scheme

In Proxy encryption scheme by using re-encryption key a proxy server can transfer a cipher text under public key to another pubic key. The server doesn't know the plaintext at the time of transformation. In 16 author define that some proxy re-encryption schemes and applied them to the sharing function of secure storage systems. In their work, messages are first encrypted by the owner and then stored in a storage server.

When user want to access his massage from storage server then he send re-encrypted key for the encrypted massage and storage server can decrypt massage for the authorised user. Hence system can help for the access data securely and forwarding to another user. Our work further integrates encryption, re-encryption, and encoding such that storage robustness is strengthened. The cloud work as intermediate of storage server and proxy server. Once a user desires to share his messages, he sends a re-encryption key to the storage server. When approved user send massage then storage server can encrypted and encoding the massage. Their secularly stored data on storage server, it will be support forwarding to another user confidentiality. In key private proxy re-encryption scheme storage server encrypted the massage so proxy server cannot verify this massage. With key attribute proxy server provide high security on proxy server.

2.3 Integrity checking Functionality

Integrity checking is main functionality of cloud storage. Users cans stored data on cloud storage. Public auditability of stored data is addressed in. Nevertheless all of them consider the messages in the clear text form. The user may want to check whether the data are properly stored in storage servers. Massage encrypted and decrypted properly or not.

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. 4, Issue 4, April 2016

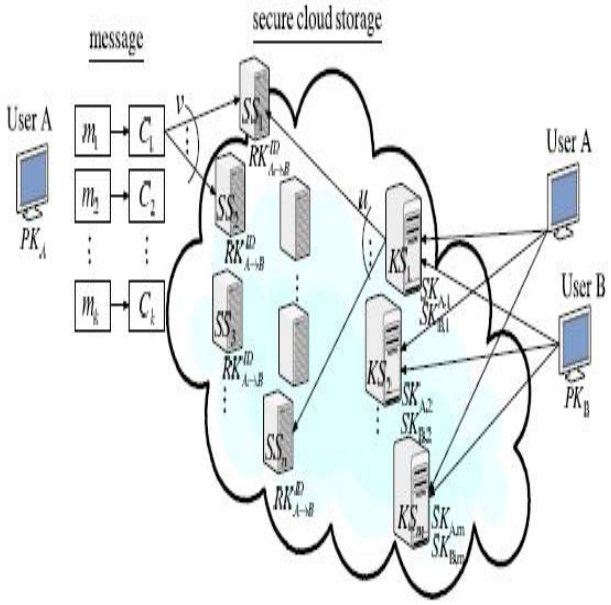


Fig. 1. A general system model of our work.

III. PROPOSED SYSTEM

In In system we define re-encryption system with attribute key. The distributed storage server support to robust and secure data storage and retrieval the data, user forward his data to another user without access back. In [11] defined by using cryptographic model to share secure data user can confidently secure data. In [10] explain erasure code base system it was decentralized code base system user can
encrypted massage and stored it on cloud server of third party , after the message symbols are send to storage servers each storage server independently computes a code word for received message symbols and stores it. In [11] proposed Proxy encryption support encoding massage and forward it any user without any back on process. It will be help for reduce security and consume time for one specific operation. This method is fully integrates encrypting, encoding and forwarding. Author proposed The threshold proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. It is fully decentralized with storage server performing encoding and re-encryption process and each key server perform partial decryption. In cloud computing integrity check is main functionality. User store data on data storage thus no data possess in user's hand. Encryption system can convert massage from plain text to cipher text. Proxy re-encryption provides data confidentiality in cloud storage system. Storage server can provide storage service and key server can provide key management service both are work independently. In distributed storage work in four stages first is system setup, storage service, data forwarding, and data retrieval. In first phase set up all system parameters and publish them. In second phase data will be encrypted and stored on cloud server and the massage decompose in to the blocks and has identifier ID, with the help of encrypt technique user encrypt each block in cipher text and sent it to all storage server then server combine them and store it in codeword symbol. In data forwarding stage user can forward massage to another user with identifier id. The massage will be forwarded by secret key. In the data retrieval phase the stored massage or forwarded massage can retrieval by user. The request has been send to the key server by user.

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. 4, Issue 4, April 2016

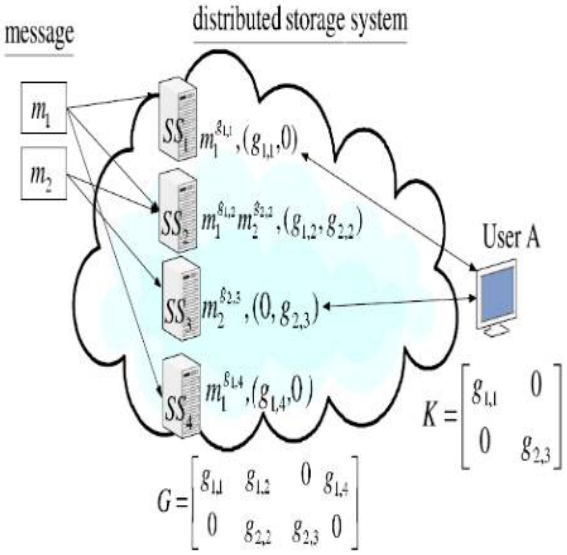


Fig.2: A storage system with random linear coding over exponents

System Recovering is when main storage server failed to retain data then user retrieve data from the key sever decrypted partially data.

IV. EXPERIMENTAL RESULTS

Fig 3. File Upload

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. 4, Issue 4, April 2016

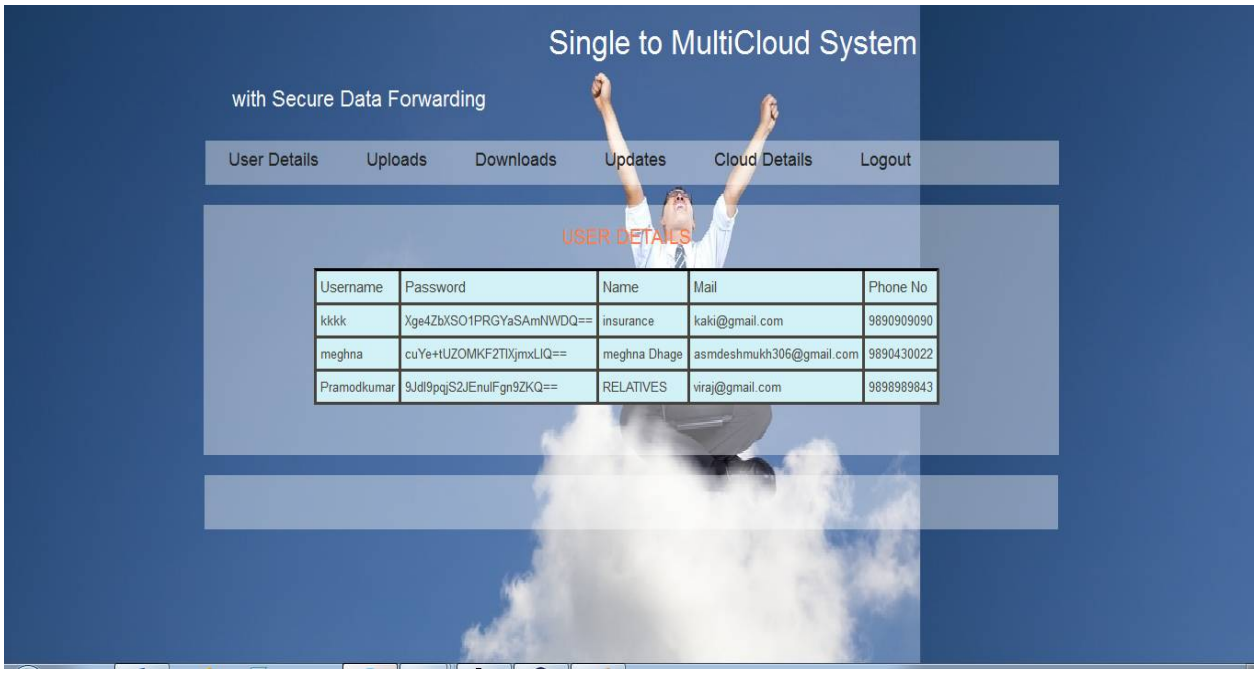


Fig 5. User Details

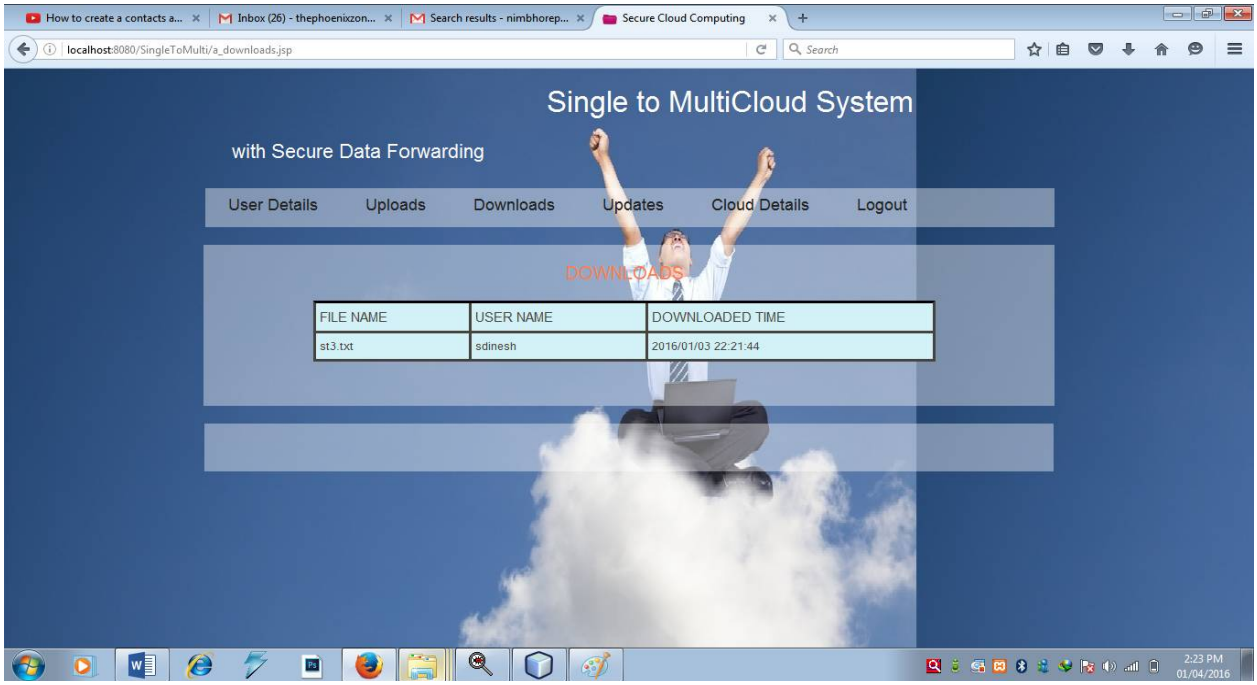


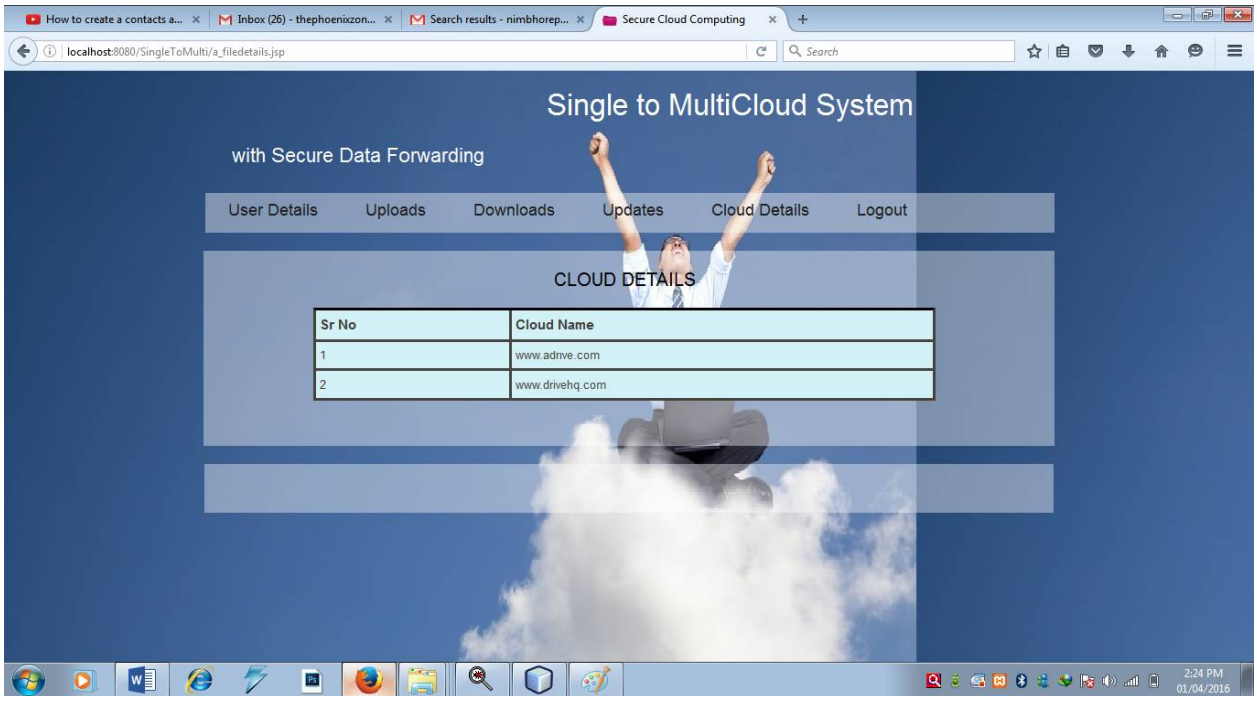
Fig 6 User Files Details

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. 4, Issue 4, April 2016



.

Fig 7. Cloud Details

\

V. CONCLUSION

In this paper, we studied the cloud sever where data can be stored on storage server and key server. We integrate a newly proposed threshold proxy re-encryption scheme and erasure codes over exponents. In distributed storage system proxy encryption scheme support system setup, data storage, data forwarding and partially decrypted. To decrypt a message of k blocks that are encrypted and encoded to n codeword symbols, each key server only has to partially decrypt two codeword symbols in our system. We define secure and robust cloud server. Data will be stored on storage server and key server, we can forward data to another user both server are work independently and decrypt data partially. The key server work as access node for providing front end layer as traditional file interface. Our storage server highly computable provide secure and robust data. In our studies storage server stored data in encrypted format with codeword symbol and with using key storage server massage can decrypt and when user want to forward massage to another user he can easily forward it from storage server.

REFERENCES

1. J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, "Oceanstore: 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. P. Druschel and A. Rowstron, "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. A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer, "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. A. Haeberlen, A. Mislove, and P. Druschel, "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Failures," Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143-158, 2005.
5. Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The Least-Authority Filesystem," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008.
6. 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.

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. 4, Issue 4, April 2016

7. D.R. Brownbridge, L.F. Marshall, and B. Randell, "The Newcastle Connection or Unixes of the World Unite! ," Software Practice and Experience, vol. 12, no. 12, pp. 1147-1162, 1982.
8. R. Sandberg, D. Goldberg, S. Kleiman, D. Walsh, and B. Lyon, "Design and Implementation of the Sun Network Filesystem," Proc. USENIX Assoc. Conf., 1985.
9. 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.
10. S.C. Rhea, P.R. Eaton, D. Geels, H. Weatherspoon, B.Y. Zhao, and J. Kubiatowicz, "Pond: The Oceanstore Prototype," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 1-14, 2003.

BIOGRAPHY

Mr. MandarD. Shindepursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Mr. Ashish K. Patelpursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Mr. Rajesh B. Vishwakarmapursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Mr. Wilson A. Waghmarepursuing his Degree Course in Bachelor of Engineering from Dhole Patil College of Engineering, Pune, Maharashtra, India

Prof. Umesh Talwareis an AssistantProfessor in Department of Information Technology in Dhole Patil College of Engineering, Pune, Maharashtra, India.