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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Exploration of Integrity Checks in Distributed Storage Networks with Secure Erasure Code

Mugdha Adivarekar, Vina Lomte

M.E Student, Dept. of Computer Engg., RMD Sinhgad School of Engineering, S. P. Pune University, Pune, India

Asst. Professor & HOD, Dept. of Computer Engg., RMD Sinhgad School of Engineering, S. P. Pune University, Pune, India

ABSTRACT: In case of cloud storage, Data confidentiality and datarobustness are the main security issues. For data confidentiality, we use encryption technique. For data robustness, there are two concerns: service failure, and service corruption and integritycheck scheme can be used to enhance data robustness against storage server corruption, which returns tampered cipher texts.In this paper secure erasure code based cloud storage system in distributed network is majorly taken into consideration tofind solution for data robustness of system.This system already takes care of data confidentiality as it calculates lost data on failed server using erasure codes. Homomorphic integrity tags can be computed from old integrity tags by storage servers without involvement of the user's secret key or backup servers.

KEYWORDS: Data confidentiality, data robustness, homomorphism, integrity check, secure decentralized erasure code

I. INTRODUCTION

Cloud technology is getting popular with day by day. Distributed storage servers in a network are the backbones ofthis system. Now a days Google drive and one drive by Microsoftare most popular cloud storage platforms. Apart from that drop box, banking sites also have started to provide some freespace on cloud along with its account.
No one possesses his/her documents on local machine. Most of people store their documents on cloud. For ordinary user it doesn't matter if his documents aresecure or not but in case of spy organization or businessman their documents are so much important.
Distributed storage system may have single point of failureso need to find security and integrity checks, these are the topics to worry. In cloud storage of distributed network admin and userface many problems. So we need to find solutions for major problem identified is to construct a robust distributed storage system which will support data integrity and data confidentiality and making system robust enough to face service failure and service corruption.
In case of distributed network there are different concerns tobe focused: (i) Security attacks,(ii)Security mechanisms and(iii)Service Continuity. Security attacks are attempts by attacker or hacker that compromises security.
Security mechanisms detect and prevent those security attacks and Service continuity is availability of service. So to fulfil all these requirements this topic helps to implement secure distributed storage where system consists of storage servers(SS) and key servers(KS).

II. RELATED WORK

H.-Y. Lin and W.-G. Tzeng[6] first started research regarding Decentralized Erasure code to enhance the privacy/confidentiality and robustness of the distributed storage network. Their research paper addresses the solution at low computation and storage cost. Decentralized erasure code is random linear code with sparse generator matrix.
Then H.-Y. Lin and W.-G. Tzeng [5] have initially proposed a threshold proxy re-encryption scheme and integrate it with decentralized erasure code so that Secure erasure code based storage network system is formulated. Re-encryption scheme allows encoding operations on encrypted data to provide datasecurity.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Shiuan-Tzuo Shen, Hsiao-Ying Lin, Wen-Guey Tzeng[1] have proposed to provide data confidentiality by means of adding integrity tags in data content before encryption. This paper is based on "A secure erasure code-based cloud storage system with secure data forwarding" as it gives prerequisites of the system i.e. data security.This is the base paper which I have referred. Laszlo Czap, Christina Fragouli, Vinod Prabhakaran, Suhas Diggavi[2] elaborates more about how erasure code is generated and and how it works during server failure in network so that missing component of file is retrieved easily by generating that missed component and also it subjects to Feedback of channel state on Eve and legitimate networks. Also if network channel introduce errors, then it would apply channel code to correct them. By leveraging erasures and feedback, secrecy rates can be increased. Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian[3] contributes to present a technique of efficient data forwarding scheme for erasure coded and encrypted cloud, which enforces cloud to provide reliability, confidentiality and forwarding same data to another user without retrieving back. This paper proposed Reed Salmon erasure code scheme. Hsiao-Ying Lin,Li-Ping Tung and Bao-Shuh P. Lin[4] also worked on retrieving file contents when they are split and erasure code is added to them. Combining these divided parts equentially while retrieving is one of the major challenges.

A. ***EXISTING METHODOLOGIES*:**

- For providing maximum availability Distributed cloud storage provides backup servers which have replicas over different locations in world.
- These servers implement RAID to have data copies with maximum fault tolerance and data availability.
- Code based methods for making replicas and Error correction codes are now rarely seen but they do exists in some scenario for archival and effective storage.
- Single storage server for whole file

B. ***DRAWBACKS***

1) Hidden Cost and Additional overheads of replicas
2) Distance multiplies risks
3) May leak stored data due to lack integrity proofs
4) Only one time encryption using general encryption schemes
5) The user has to do most computation and communication traffic between the user and storage devices is high.
6) The user has to manage his cryptographic keys.
7) If the user's device of storing the keys is lost or compromised, the security is broken.
8) It is hard for storage servers to directly forward a user's messages to another one.
9) The owner of the message has to retrieve, decode, decrypt and then forward them to another user.

C. ***PROBLEM ANALYSIS***

To provide data robustness is to replicate a message such that each Storage server stores a copy of the message. It isvery robust because the message can be retrieved as long as one storage server survives. If the number of failure servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process.
This provides a trade-off between the storage size and the tolerance threshold of failure servers. A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message. A decentralized erasure code is suitable for use in a distributed storage system. Authors have proposed new integrity check scheme to ensure data robustness to deal with storage server failure. Retrieved cipher text(Ci) is used to check its integrity before erasure-decoding or decryption. Homomorphic integrity tags are compatible with data forwarding and repairing. System consists of n storage servers, m keyservers and 4 phases:

1. Setup phase
2. Storage phase
3. Integrity check phase
4. Retrieval phase

Server A requests for integrity check for File M of identifier I_m to key server KS.KS queries random w servers for w encoded tuples to calculate integrity checks by

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

a) Bilinear map
b) Pseudorandom function
c) Decentralized erasure code
d) Threshold public key encryption

III. PROPOSED SYSTEM

A. *DESIGN CONSIDERATIONS:*

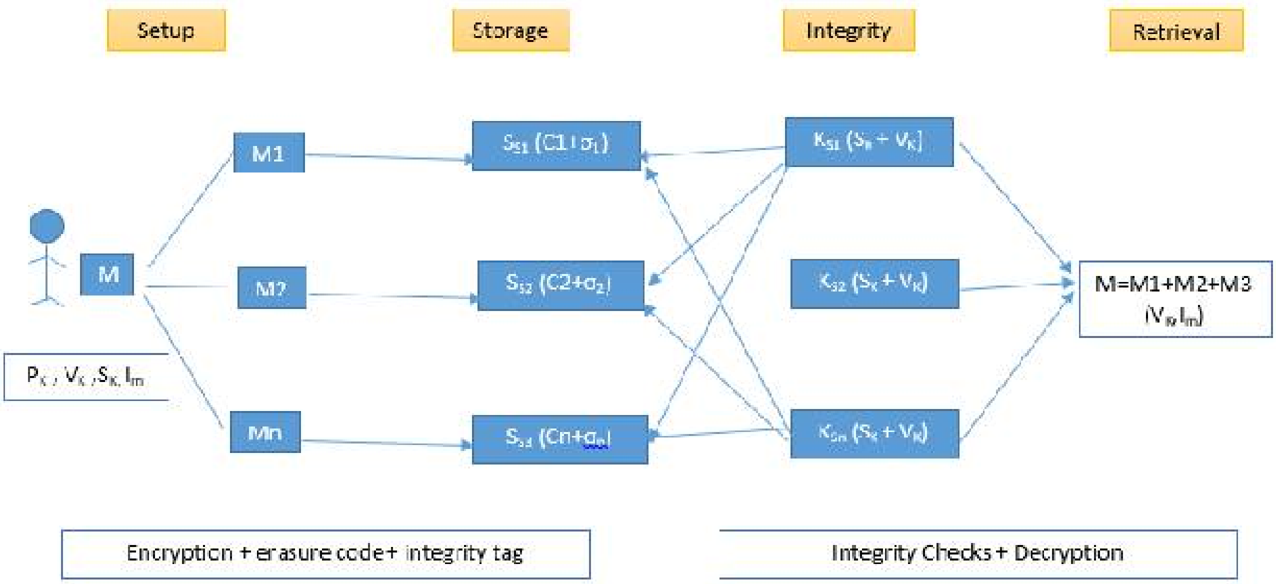
System consists of 4 phases - Setup, Storage, Integrity Check and Retrieval Phase.

Setup phase consists of users having their files to store with unique file identifier. Encryption and erasure codes are added in this phase.

Storage phase consists of Storage servers and their verification keys.

Integrity Phase calculates integrity tag code with the help of verification key.

And Retrieval phase consists of activities like retrieving files with decryption and checking their integrity with verification keys.



- Mathematical Model

  Let I_H be a homomorphic integrity tag for combined data ($a.c1 + b.c2$, VK_A) and is defined as-

  $I_H = (a \otimes \sigma_1) \oplus (b \otimes \sigma_2)$

  Where

  σ_1 - integrity tag for c1

  σ_2 - integrity tag for c2

  $\otimes$- Multiplication (.) in homomorphism domain

  $\oplus$- Add (+) in homomorphism domain

  Homomorphism is map one field to another which is additive, multiplicative and unit-preserving.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

B. *OBSERVATIONS:*

This system is having very high robustness and security compared to error correction codes and other encryption algorithms. Here we address the problem of forwarding data to another user by storage servers directly under the command of the data owner.
We consider the system model that consists of distributed storage servers and key servers. Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers that perform cryptographic functions on behalf of the user.
These KS are highly protected by security mechanisms. To well fit the distributed structure of systems, we require that servers independently perform all operations. With this consideration, we propose integrity check schemeand integrate it with a secure decentralized code to form a secure distributed storage system.
The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. Our SS act as storage nodes in a content addressable storage

IV. ADVANTAGES

1)The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.
2) More flexible adjustment between the number of storage servers and robustness.
3) By using the integrity check scheme, we present a secure cloud storage system that provides secure and integrated data storage and secure data forwarding functionality in a decentralized structure.

V. SIMULATION RESULTS

I have simulated this system in a simple stand-alone windows application. Some implementation screen shots are added here to visualize the encryption-decryption process with file forwarding and its retrieval. Figure 1, 2 and 3 will demonstrate core functionality.

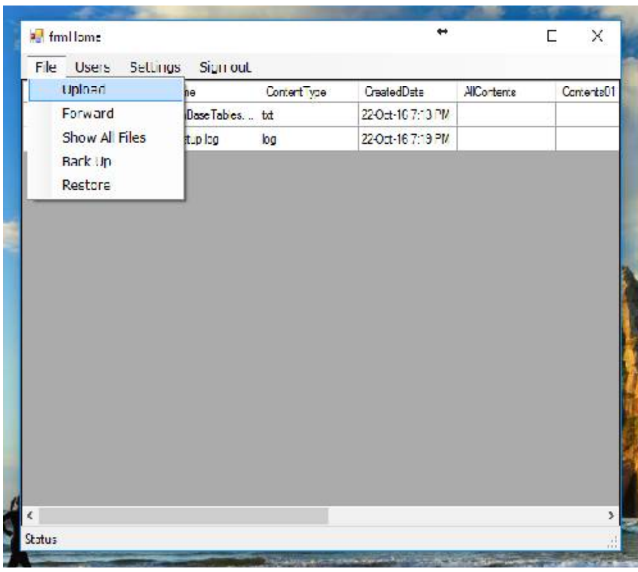


Fig.1.Upload file

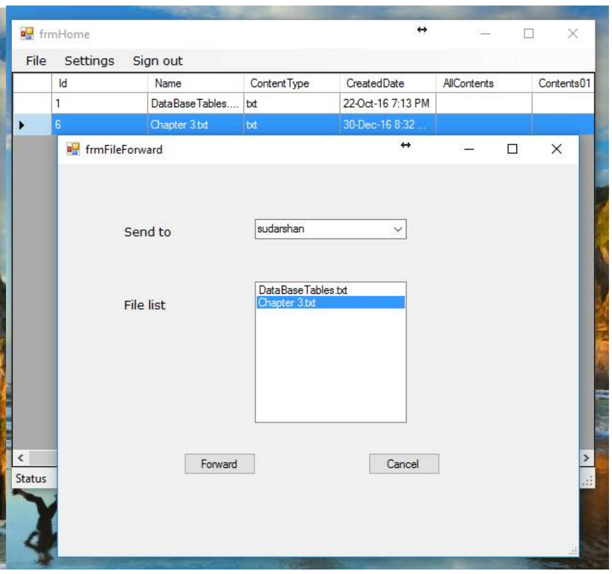


Fig. 2. Forward file

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Admin has role to accept user requests. Also he can view all the documents in system. Admin has authority to backup and restore option like figure 1.
Once the user is accepted in system, he can have functionalities like upload and forward.
In figure 2- User is able to upload document then forward it to intended user.

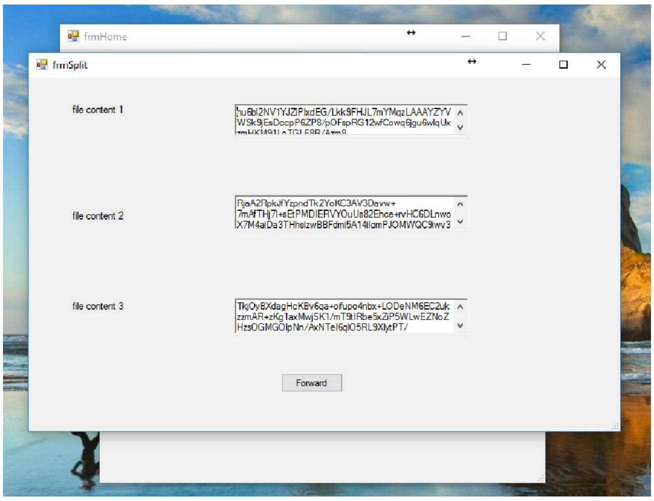


Fig. 3. Encrypted Contents

In figure 3 – data file is divided into no.of servers available in network and they are stored in encrypted form along with Integrity checks and erasure code. So that data confidentiality and robustness is preserved.
Then receiver can retrieve the file sent by sender by double click over file.

VI. Applications

1. Government Organizations such as defence sector, spy organizations where high data confidentiality and security is required.
2. Space research centres
3. Nuclear power plants.
4. Our service can be used by the Data Centres on clouds fort he storage of the users data and also forward securely. Our service can be used by the business organizations for maintaining the integrity and secrecy of the important information.
5. Spy organizations those work for our nation need to be very secure due to highly sensitive data.
6. Nuclear power plants are also need to be taken care because a smallest mistake can harm many people.
7. In banking domain, we may provide integrity check scheme for KYC documents management.
8. Our system is highly distributed where storage servers independently encode and forward messages and key servers independently perform partial decryption.

VII. Conclusion and Future Work

The implementations of the traditional systems have resulted in crashes, DOS attacks and unavailability due to regional network outages. In the proposed system a secure distributed storage system is formulated by integrating a encryption scheme with a decentralized erasure code.
Proposed scheme supports not only the expected encoding operations over encrypted messages but also the forwarding operations over encoded and encrypted messages. Enhanced robustness of system is achieved by Integrity checks at low cost and compatible manner.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Future scope:
1) To use efficient algorithms for encryption and decryption purpose
2) To implement storage servers and key servers to the cloud
3) To automate process of generating integrity tags while encryption.

VIII. ACKNOWLEDGMENT

I take this opportunity to express my heartfelt gratitude to my guide and head of department, Prof. Vina M Lomte, Department of Computer Engineering, RMDSSOE, Savitribai Phule Pune University, for her kind cooperation, constant Encouragement and suggestions and capable guidance during he research, without which it would have been difficult to proceed with.

REFERENCES

1. Shiuan-Tzuo Shen; Hsiao-Ying Lin; Wen-Guey Tzeng,"An Effective Integrity Check Scheme for Secure Erasure Code-Based Storage Systems", IEEE Transactions on Reliability,vol. 64, no.3 , pp. 840 - 851,Jun.2016
2. Laszlo Czap,Christina Fragouli,Vinod Prabhakaran,Suhas Diggavi,"Secure Network Coding With Erasures and Feedback", IEEE Transaction on InformationTheory ,vol.61,no.4,pp.1667-1686,Apr.2015
3. Jian Liu,Kun Huang,Hong Rong,Huimei Wang and Ming Xian,"Efficient and Secure Data Forwarding for Erasure-code based Cloud Storage", Proc 2015 IEEE Intl Workshop on cloud computing system,Networks and applications,vol.24,pp.1820-1826,Sept.2015
4. Hsiao-Ying Lin,Li-Ping Tung and Bao-Shuh P. Lin, "An Empirical Study on Data Retrievability in Decentralized Erasure Code Based Distributed Storage Systems", IEEE 7th International Conference on Software Security and Reliability, vol. 21, no. 11, pp. 30-39, Aug. 2013.
5. H.-Y. Lin and W.-G. Tzeng,"A secure erasure code-based cloud storage system with secure data forwarding", IEEE Trans. Parallel Distrib. Syst.,vol. 23, no. 6, pp. 995-1003, Jun. 2012
6. H.-Y. Lin, W.-G. Tzeng, and B.-S. Lin,"A decentralized repair mechanism for decentralized erasure code based storage systems", in Proc. 10th IEEE Int. Conf. Trust, Security and Privacy in Computing and Commun.(TrustCom'11), vol.45, pp. 613-620., Nov. 2011
7. H.-Y. Lin and W.-G. Tzeng,"A secure decentralized erasure code for distributed networked storage", IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 11, pp. 1586-1594, Nov. 2010.
8. C. Wang, Q. Wang, K. Ren, and W. Lou,"Ensuring data storage security in cloud computing", in Proc. 17th Int. Workshop Quality of Service (IWQoS'09), vol.6, pp. 19. , Jul. 2009
9. G. Dimakis, V. Prabhakaran, and K. Ramchandran,"Decentralized erasure codes for distributed networked storage", IEEE Trans. Inf.Theory, vol. 52, no. 6, pp. 2809-2816, Jun. 2006..

BIOGRAPHY

Mugdha Adivarekar is a Student in the Computer Engineering Department, RMD Sinhgad School of Engineering, Warje, Pune University. She is pursuing Master of Computer engineering degree in. Her research interests are Information Retrieval, Data mining, Algorithms, etc.