International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Enhancing Availability of Data in Mixed Homomorphic Encryption in Cloud

Bhargavi Patel

Assistant Professor, Engineering College, Tuwa, Godhra, Panchamahal, Gujarat, India

How to cite this paper: Bhargavi Patel "Enhancing Availability of Data in Mixed Homomorphic Encryption in Cloud" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1310-1314, URL: https://www.ijtsrd.com/papers/ijtsrd25104.pdf

IJTSRD25104

ABSTRACT

In Forthcoming times of information technology companies, cloud computing updated as the structural model. There are so many benefits of cloud computing in technical as well as in organization. But still there are many new objections will carried in cloud computing for example in data security in cloud storage. There are many approaches available for data security in cloud storage like encryption with obfuscation technique, watermark security, data partitioning technique. In above all the approaches, there is no possibility that cloud data centers are operate computation on encrypted data so every time if user wants to modify data, it is necessary to decrypt data. The most used technique for providing security in cloud storage is Homomorphic encryption. In the homomorphic encryption technique, there is no need to decrypt whole data whenever user wants to update data. In the existing system used the mixed homomorphic scheme which reduce noise level in homomorphic encryption technique. The existing system focus on data corruption and data modification but what if system failure and power failure occurs. The user data may be loss in any reasons and user may not have any copy of data. The Existing system not focus on data loss. So in proposed work focus on availability of data by erasure code. By applying the erasure code if in any case user data is loss, will be reconstructed which provide more security than existing system.

Keywords: *Cloud Computing; Data Security; Homomorphic Encryption; Availability of Data*

INTRODUCTION

There are many resources are available in cloud computing which leads in organization. By Combining the parallel processing and distributed computing as well as grid computing models makes the cloud computing.[10] There are three types of services in cloud computing. First one is the service which gives the user basic computing resources like virtual machine, storage network in the form of cloud storage and some processing power is called as Infrastructure-as-a-service(IAAS).[10] Second one is the service which provides the infrastructure of cloud with development language and development tools on which users can build and deploy their program is called as Platform-as-a-service(PAAS).[10] Third one is the service which yielded services to user. The services that runs on infrastructure of cloud computing arranged by broker also known as service provider is called as Service-as-a-service(SAAS).[10] Users need not manage resources provided by this three services, user just use this services as payper-usage and pay the bill as per usage. There are several challenges like security and privacy issues, multi-tenancy, scalability, customizable GUI and Business logic according to business type etc.

RELATED WORK

Moving the data in the cloud provide the user with a great efficiencies, since it don't have to care about the complexities of direct hardware management. By internet based online services, using the huge amount of storage space and customizable computing resources, this platforms eliminates the responsibilities of the local machines for data maintenance .So for the integrity of the data users are depended on the cloud service providers. Users' data mostly protected by applied distinct cryptographic algorithms like AES, DES, RSA, etc. by broker to protect data from hackers. All this techniques may also apply in cloud computing environment to secure the users data files. By using the algorithms the user loses control over the data. Therefore without the knowledge of the data in cloud we should provide security by Homomorphic Encryption Technique. As focusing on data corruption, it is also important to focus on data loss and data unavailability.

A. Data Security in Cloud Storage

Maintenance of data center is high in terms of cost for a low budget organization who use small data center. The best choice for low budget organization is to adopt cloud computing as cloud computing provides cloud data center. Using cloud data center, the management of data center is removed. As water and electronic, the computation services and storage can buy by low budget organization. The public Storage provider can store data. [15] There are different type of user, organizations and person can use the common cloud data storage.

In cloud storage client is unaware of where his data is stored. On the above layer of cloud where network computing system is stored all data. As cloud storage use by many different persons, it is necessary to have data security in

different levels. For different layer security, the cost should be different. [15]

- The user can lost their control from data in public cloud so there is many security issues in public cloud. Because all users data are stored in same place. [15]
- In an organization only authorized person can access the confidential data. So in private cloud the security is needed to protect all storage servers. [15]

The main problem in cloud storage is how to safe users data. In cloud, the service provider can guarantee for protection of data but user cannot believe. By this Data security is very big thing of cloud storage. [15]

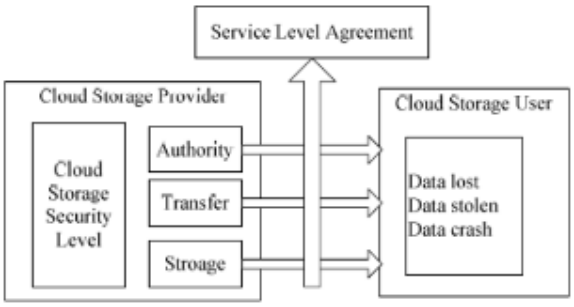

Fig 1. Framework to ensure data security [15]

Fig 1. Shows the framework which combine the scenario of cloud storage provider and user. A guarantee between service providers to user is called service level agreement. Different Types of services, their qualities and user payment can define by SLA. In some times Users may check that data is lost, stolen, crash. The possibility of data disaster can be defined by SLA. There are many different technologies are available which helps service provider to achieve SLA. Different SLA have Different Cost.[15]

To provide data security in cloud storage there are mainly three parts. [15]

- Secure Storage
- Transfer
- Authority

Secure Storage: The data may be safe during any nature disaster is the fundamental requirement of data security. The data may be protected by dividing the user data into number of small files and store it into different places. If data pieces in one data center or disk crashed, the data can be resumed by left pieces. It's an important method to remote access performance and system availability. Cloud storage service provider may construct data center in several regional. Most of service provide file level save and acquire service. How to separate files to pieces and how to place these pieces is important to make files safe. File security level from low to high is divided into single server level, cross-server level, cross-cabinet-level, cross-data center level. [15] These are divided by where the pieces stored in cloud storage. The higher the security level higher storage cost, cost is also higher in the Cloud computing system the user can customize according to their different levels of the circumstances of storage services.[15]

Transfer: The data must transfer though network. To make the data available at any time, provider must separate data to several data center and do some optimize in position near the final user. Data saved in cloud storage often used for cloud computing and share. To transfer an amount of data is difficult for the existing network conditions.[15]

Authority: Authority is important to user to avoid antiauthority access. For the storage provider, it needs to do user authority and access control. During the user access the data in cloud, all operation should be recorded and traceable. It's important to make anyone else can't see the data, including administrator. [15]

PROPOSED SYSTEM FRMEWORK

The term Data availability is used by computer storage manufacturers, storage service providers to describe products and services that ensure that data continues to be available at a required level of performance in situations ranging from normal through disastrous. Anytime a server loses power, for example, it has to reboot, recover data and repair corrupted data. The time it takes to recover, known as the mean time to recover (MTR),

could be minutes, hours or days. Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or restore lost data. Data loss is distinguished from data unavailability, which may arise from a network outage. Although the two have substantially similar consequences for users, data unavailability is temporary, while data loss may be permanent.

In an existing system not focus on Data availability. In proposed work the erasure code are used for availability of data in case of failure. A Reed-Solomon erasure code adds redundancy to the system to tolerate failures. By extending the existing system after applying the homomorphic encryption and RSA encoding and key switching matrices in existing system then EDB block apply erasure code to this block. So by providing the erasure code in any case system failure or system reboot or any nature disaster happen the data can be available to user. The user is not aware about any failure and gets data available whenever required. When user download the data first decode with erasure code and then by applying the decryption process get the data.

B. System Architecture

In the proposed system, develop the model for availability of data in mixed-Homomorphic encryption scheme. Fig 2. Shows the general layout of proposed work. The proposed system work on four module: encryption, decryption done by BGV Homomorphic encryption and for availability of data encoding and decoding by Reed Solomon error correcting erasure code.

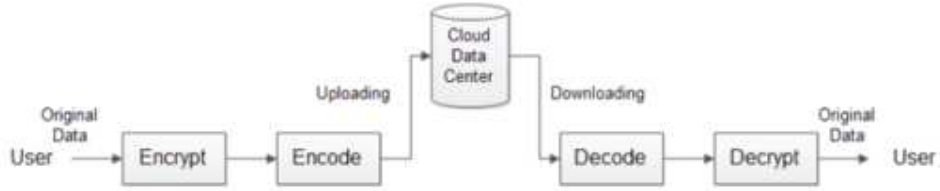

Fig2. System Architecture of Proposed Work

PROPOSED ALGORITHM

A. Steps for Uploading File:

1. User file which he wants to upload divide into number of parts
2. All byte of user file can be encrypted by homomorphic encryption
3. Crete a separate file in which the decrypted data encoded with RSA algorithm and also have key-switching matrices.
4. Apply erasure code. There N number of bytes data in users file. This method generate the number of Encrypted Data Block per file (EDB). Every file contains number of EDB blocks. Every EDB block have key-switching matrices of k bytes, and two block i.e. RSA and Decrypted data. Number of Distributed servers in cloud storage can stored this EDB block.

B. Algorithm Steps for Downloading File:

1. for finding the Encrypted data block, User can queries to all the Distributed storage servers
2. Apply decoding and recover the file if any file is missing.
3. Getting encrypted data block, user decode the data by RSA
4. After decoding, by applying the Homomorphic encryption user can decrypt the data and get the original file.

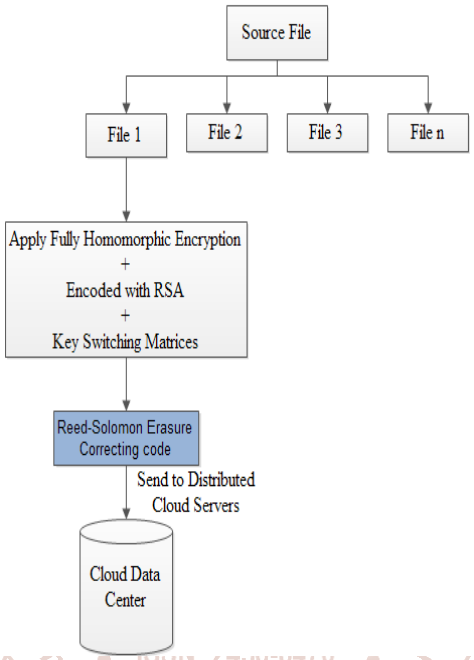

Fig3. Flow Chart of Proposed Work of Uploading Process

THEORETICAL RESULT ANALYSIS

Suppose after encryption we have ABCDEFGHIJKLMNOP encrypted format data available. Apply reed Solomon encoding to this data. The data converted into 4 X 4 matrix format as shown in figure 3.4. In this example, the four pieces of the file are each 4 bytes long. Each piece is one row of the matrix. The first one is "ABCD". The second one is "EFGH". And so on.

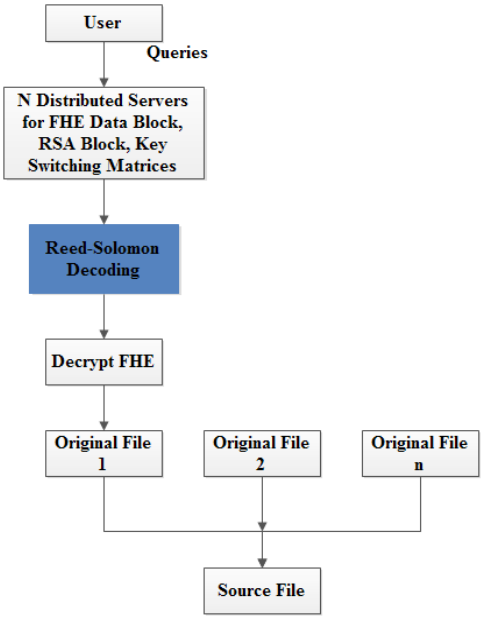

Fig4. Flow Chart of Proposed Work of Downloading Process

Fig5. Encrypted Data into 4X4 Matrix Format

The Reed-Solomon algorithm creates a coding matrix that you multiply with your data matrix to create the coded data. The matrix is set up so that the first four rows of the result are the same as the first four rows of the input. That means that the data is left intact, and all it's really doing is computing the parity.

The result is a matrix with two more rows than the original. Those two rows are called parity pieces. Each row of the coding matrix produces one row of the result. So each row of the coding matrix makes one of the resulting pieces of the file.

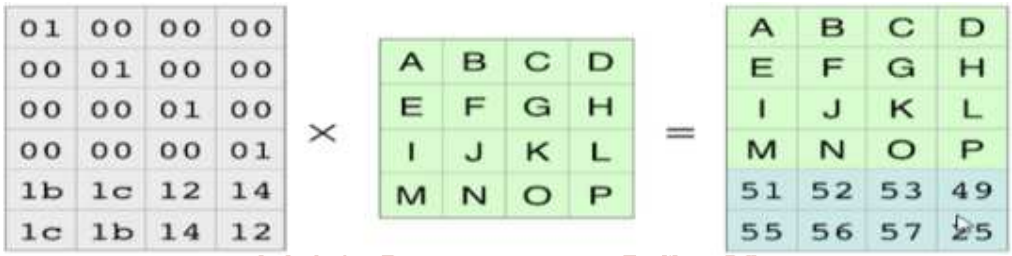

Fig6. Encrypted Data multiply with Coding Matrix

Fig7.2 rows Data Loss out of 6 rows

The coding matrix, the matrix on the left, is invertible. There is an inverse matrix that is when multiplied by the coding matrix, produces the identity matrix. As in basic algebra, in matrix algebra you can multiply both sides of an equation by the same thing.

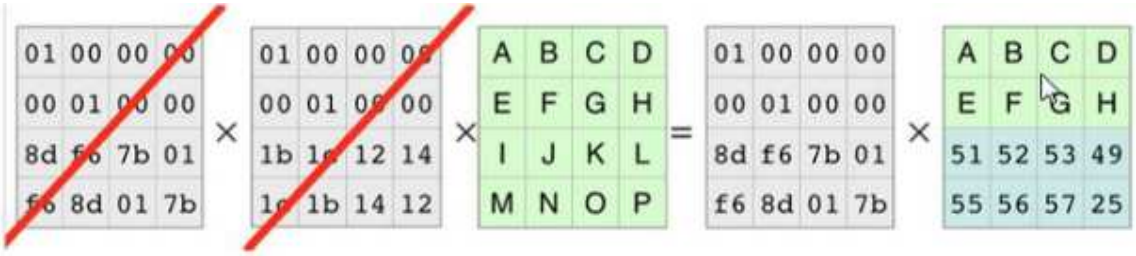

Fig8. Coding Matrix and Invert Matrix are cancel out by multiplying Invert Matrix both side

This leaves the equation for reconstructing the original data from the pieces that are available:

Fig9. Reconstruction of Original Data

CONCLUSION AND FUTURE WORK

The paper presents data availability in case of data loss and system failure by using reed Solomon error correcting code which is one kind of erasure code to provide better security for cloud storage. The proposed algorithm only focus on use of reed Solomon error correcting code as a erasure code for provide better security and availability of data but not focus on attacks may done on erasure code.

REFERENCES

[1] Maulik Dave, "Data Storage Security in Cloud Computing: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering 2013.

[2] Dr. L. Arockian, S. monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security", IEEE 2014.

[3] Boopathy D, M.Sundaresan, "Data Encryption Framework Model with Watermark Security for Data Storage in Public Cloud Model", IEEE 2014.

[4] Jian Li, Sicong Chen, Danjie Song, "Security structure of cloud storage based on homomorphic encryption scheme", IEEE 2013.

[5] Amit Kumar Aman, Vijay Prakash, "Efficient Public Verifiability and Data Dynamics for Storage Security in Hybrid Clouds", IEEE 2013.

[6] Md. Rafiqul Islam, Mansura Habiba, "Agent Based Framework for providing Security to data storage in Cloud" IEEE 2012.

[7] Mehdi Hojabri, "Ensuring data storage security in cloud computing with effect of Kerberos", International Journal of Engineering Research & Technology 2012.

[8] Guobo Xie, Bingying Yao, "Cloud Storage Identity Design Based On Fingerprint Identification", IEEE 2013

[9] C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha, "PDDS – Improving cloud data storage security using data partitioning technique" IEEE 2012

[10] R.Kangavalli, Dr. vagdevi S, "A Mixed Homomorphic Encryption Scheme for Secure Data Storage in Cloud", IEEE 2015

[11] R.Kanagavalli and Vagdevi S,"A Survey Of Homomorphic Encryption Schemes in Cloud Data Storage", IJRDET, 2014, Vol 3, p.p. 71-75.

[12] Manoj Kokane,Prem Kumar Jain,Poonam Saranghar,"Data Storage Security in Cloud Computing",IJARCCE,2013.

[13] J.W.Bos,K.Lauter,J.Loftus and M.Naehrig,"Improved security for a ring based fully homomorphic encryption scheme",IACR Cryptology,ePrint Archive,2013.

[14] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of REFERENCES Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013.

[15] Xiao Zhang, Hong-tao Du, Jian-quan Chen, Yi Lin, Lei-jie Zeng, "Ensure Data Security in Cloud Storage", IEEE 2011.

[16] Cloud Computing for Dummies, Wiley publishing, Inc.

[17] William Stallings, "Cryptography and Network Security-Principles and Practice"5th Edition, 2011, Prentice Hall.