IJARST

International Journal of Advanced Research in Science and Technology

journal homepage: www.ijarst.com

ISSN 2319 – 1783 (Print)
ISSN 2320 – 1126 (Online)

File Storage System Using Hybrid Cryptography

K.Prathik Raj[1], H.Abhinav[2], Saurya.K[3]

SNIST, India

ARTICLEINFO

Article history:
Received 24 Apr 2023
Accepted 16 May 2023
Available online 07 July 2023

Keywords:
Cryptography,
data security,
public key,
resource consumption,
secret key,
DES,
AES.

ABSTRACT

Data stored in the cloud is increasingly gaining popularity for all users including personal, institutions and business purposes. The data is usually highly protected, encrypted and replicated depending on the security and scalability needs. Despite the advances in technology, the practical usefulness and longevity of cloud storage is limited in today's systems. This project provides a solution to the problem of securely storing the client's data by maintaining the confidentiality and integrity of the data within the cloud. This project addresses the problem of ensuring data confidentiality against cloud and against accesses beyond authorized rights. To resolve these issues, we designed a data encryption model that is in charge of storing data in an encrypted format in the cloud. To improve the efficiency of the designed architecture, the service in form of the model designed allows the users to choose the level of security of the data and according to this level different encryption algorithms are used. Data transmitted through internet is getting larger every day. Therefore an algorithm is required by which our data can be transferred speedily and securely. The main aim of this particular research is to protect the transmitted data with the help of encryption and decryption techniques

1. INTRODUCTION

The aim of the project is to create an encrypted and secured file storage system to transfer files within users in a remote location. This system will require an input that is successfully encrypted using any of the algorithm techniques and store them anywhere. The uploaded file can be downloaded by other users, but to read the data present in it, they have to decrypt the file using the decryption algorithm and the information provided about the file within the users by the owner. The system uses public-key cryptographic techniques like RSA and Symmetric key cryptography like AES. Hashing techniques like static hashing and dynamic hashing are used for performing integrity. Due to the encryption of data, confidentiality is also achieved in the process. The project is also open to new challenges and future changes to other advanced technologies in keeping the data secured.

2. PROPOSED MODELLING

In our proposed system 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 shall perform cryptographic functions on behalf of the user. These key servers are highly protected by security mechanisms.

Here Storage system has allocated by different data container. Once owner uploads the data with AES encryption mechanism, system again takes the data and makes Secure Data segregation process. All the data pieces will be saved in different location in cloud storage. Here public distributor monitors all the data and corresponding positions where it is saved. When a proper client is asking the data, cloud system will provide the data in reversible manner. So, our system will prevent our data from both Inside and Outside attackers.

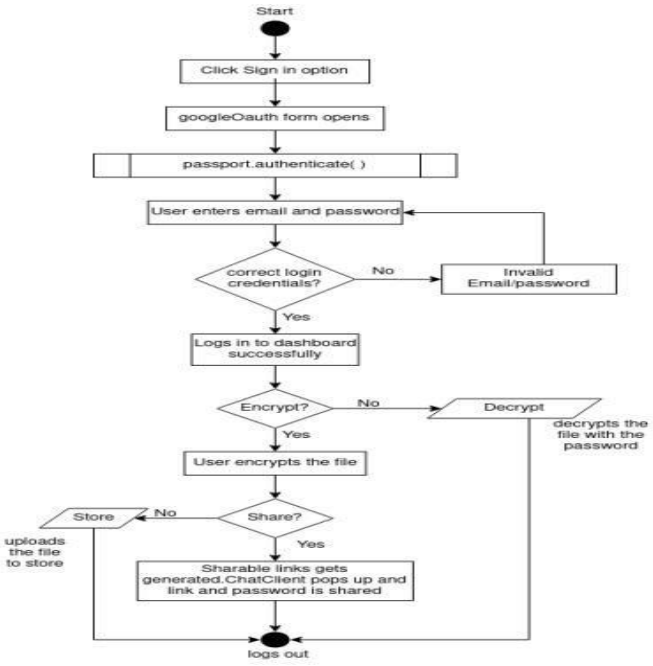
ADVANTAGES:

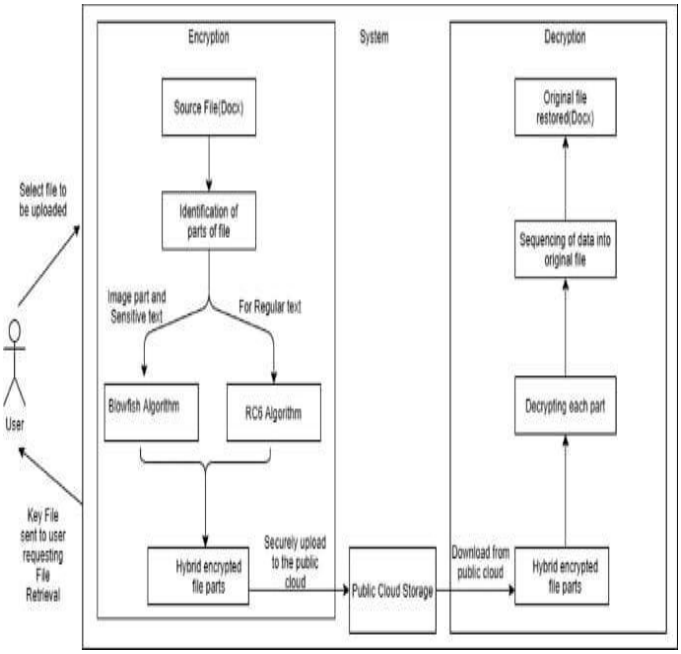
❖ Tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.

❖ The storage servers independently perform encoding and re-encryption process and the key servers independently perform partial decryption process.

❖More flexible adjustment between the number of storage servers and robustness

3. SYSTEM DESIGN





Usecase Diagram

4. CONCLUSION

Erasure codes are promising for improving the reliability of the storage system due to its space efficiency compared to the replication methods. Traditional erasure codes split data into equalsized data blocks and encode strips in different data blocks. This brings heavy repairing traffic when clients read parts of the data, since most strips read for repairing are not in the expected blocks. This paper proposes a novel discrete data dividing method to completely avoid this problem. The key idea is to encode strips from the same data block. We could see that for repairing failed blocks, the strips to be read are either in the same data block with corrupted strips or from the encoded strips. Therefore, no data is wasted. We design and implement this data layout into a HDFS- like storage system. Experiments over a small-scale test bed shows that the proposed discrete data divided method avoids downloading data blocks that are not needed for clients during the repairing operations..

REFERENCES

James S. Plank, Erasure Codes for Storage Systems A Brief Primer, USENIX .login, Vol. 38 No. 6, 2013.

Hsing-bung Chen, Ben McClelland, et al., An Innovative Parallel Cloud Storage System using OpenStack's Swift Object Store and Transformative Parallel I/O Approach, Los Alamos National Lab Science Highlights, 2013.

CorentinDebains, Gael Alloyer, Evaluzation, Evaluation of Erasure-coding libraries on Parallel Systems, 2010.

Peter Sobe, Parallel Reed/Solomon Coding on Multicore Processors, in Proceedings of International Workshop on Storage Network Architecture and parallel I/O, 2010.

BabakBehzad, Improving parallel I/O auto tuning with performance modeling, in Proceedings of ACM International Symposium on High-performance Parallel and Distributed Computing (HPDC), 2014.

Hsing-bung Chen, parEC – A Parallel and Scalable of erasure coding support in Cloud Object Storage Systems, Los Alamos National Lab.

A. Varbanescu , On the Effective Parallel Programming of Multi-core Processors, Ph.D Thesis, TechnischeUniversiteit Delft , 2010.

William Gropp Ewing Lusk, Anthony Skjellum, Using MPI:

Portable Parallel Programming with the Message-Passing Interface, The MIT Press, 2014.

Hsing-bung Chen, Parallel Workload Benchmark on Hybrid