Secure File Handling System for Cloud Computing with Load Balancing

Sanas Pooja[1], Konde Pooja[2], Nalawade Geetanjali[3], Jagtap Shraddha[4]

[1,2,3,4]Department of Computer Engineering, Navsahyadri Education Society's Group of Institutions Pune

---***---

Abstract— *Cloud provides large Shared Resources where users (or Foundations) can enjoy the Facility of Storing Data or Executing Applications. In Spite Of gaining convenience of large resources storing critical data in cloud is not secured. Hence, cloud security is an important issue to make cloud useful at the enterprise level. That's Why we use here different encryption algorithms i.e homomorpic algorithm and RSA algorithm also we provide the load balancing concept to provide the security to file downloading. File handling, sharing and downloading with security will be done by this software.*

Keywords— *Cloud Computing, homomorphic Encryption, Load Balancing, File Encryption, RSA algorithm*.

I. INTRODUCTION

Cloud storage is a new cost-effective paradigm that aims at providing high availability, reliability, massive scalability and data sharing. However, outsourcing data to a cloud service provider introduces new challenges from the perspectives of data correctness and security. As the rate of cloud adoption is growing, the security risks associated with networked applications in general and cloud in specific is also growing. For this we are providing a secure file handling system to cloud by using the techniques homomorphic algorithm and load balancing.

II. RELATED WORK

In cloud to distribute the workload and to allocate the resources efficiently we are using Load balancing technique.

III. LITERATURE SURVEY

[1] Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi Party Computation. In this paper, the user's data is encrypted using padding scheme, called Optimal Asymmetric Encryption Padding (OAEP) together with Hybrid Encryption algorithm that is based on RSA (i.e., HE-RSA), in order to allow multiple parties to compute a function on their inputs while preserving Integrity and Confidentiality. The Homomorphic Encryption (HE) is performed on the encrypted data without decrypting it in computationally powerful clouds and the Secure Multi-Party Computation (SMPC) can be used in the cloud to ensure security and privacy of the users[2] Authentication Scheme using Unique Identification method with Homomorphic Encryption in Mobile Cloud Computing. The purpose of this project is to design and implement a framework that employs unique authentication method that relies on third party identification which is required to accurately identify and authenticate legitimate user in order to reduce the risk of disclosing confidential data to unauthorized party in Mobile Cloud Computing[3] Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm.[4] Homomorphic Encryption for Security of Cloud Data[5] A Secure Cloud Computing Architecture Using Homomorphic Encryption[6] A Study of Data Storage Security Issues in Cloud Computing[7] Multicloud Stored Encrypted Big Data Secured By Honey Words[8] A review of homomorphic encryption of data in cloud computing. The term encryption refers to converting the original data into human unreadable form (encoding). The conversion of the encoded data into original form is known as decryption. By encrypting the data only the authorized person can decode the original data. Thus data confidentiality is achieved by the encryption. In this paper, we reviewed the algorithms proposed for the homomorphic encryption of data in cloud computing.

IV. PROPOSED SYSTEM

In our project we have created a system which will perform certain operations on the user's data which is to be stored on cloud. It will encrypt the data so as no one can able to see the data even after hacking the cloud and user's data. We have also used the RSA algorithm so as user can store any type of data and can share it to only the person to whom he wanted to share it. The thing that we have used is load balancing to make the data storing effective and to handle multiple user's using the system at a time.

So basically our idea is to provide security to the data and not the person. So that no one hack stole or modify the data besides of the original user.

V. OBJECTIVE OF PROPOSED SYSTEM

Now a days there are many problems of hacking and attacking so to overcome this we have developed this software to maintain the security of system.

1. Execution of file handling System properly and the factors related to the results and tools and techniques.
2. To Provide Security to the System for handle cloud files.
3. To proper working of encryption and decryption of files.
4. To upload and download files with different extensions.
5. Describe the process of File uploading and downloading.

VI. ARCHITECTURE

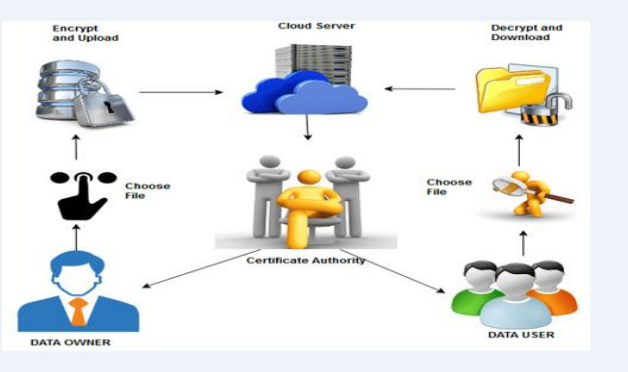

Fig 1. System Architecture

VII. DESCRIPTION

When the data is transferred to the Cloud server we use standard encryption methods to secure the operations and the storage of the data. Our basic concept is to encrypt the data before send it to the Cloud provider. The only person who can decrypt the data is it's data owner. Homomorphic Encryption is used to perform operations on encrypted data without knowing the private key (without decryption), the data owner is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data. But the last one needs to decrypt data at every operation. The data owner will need to provide the private key to the server. If the user wants to share his data with another person he has to share his one time password received on the phone number he has specified to that person. Thus data confidentiality is achieved by the system

VIII. ALGORITHM

1]Input string

D=(d_1,d_2,d_3,….,d_n)

D_1,d_2,d_3….in are the data files uploaded.

2]Encrypt data

E=(e_1,e_2,e_3…..,e_n)

e_1,e_2,e_3,…. are the encrypted file.

3] Identify drive

S=(s_1,s_2,s_3,…..s_n)

(s_1,s_2,s_3…are separate or multiple drive)

4] Classification of file

D+E¬S

If -> d_1∈ (e_1,e_2,e_3.....e_n)

E <- D

If d_n ∈ (e_1,e_2,e_3…e_n)

E <- d_n

Where e_1,e_2,e_3= encrypted data

D = uploaded data

E <- D ¬S

Where,

S=data shows in each drive separately.

5] Calculating data by users

S_i =d_i/e_i ¬- U

Where,

S_i=Stored data

d_i =uploaded data

e_i=encrypted data

U= user

IX. FLOWCHART

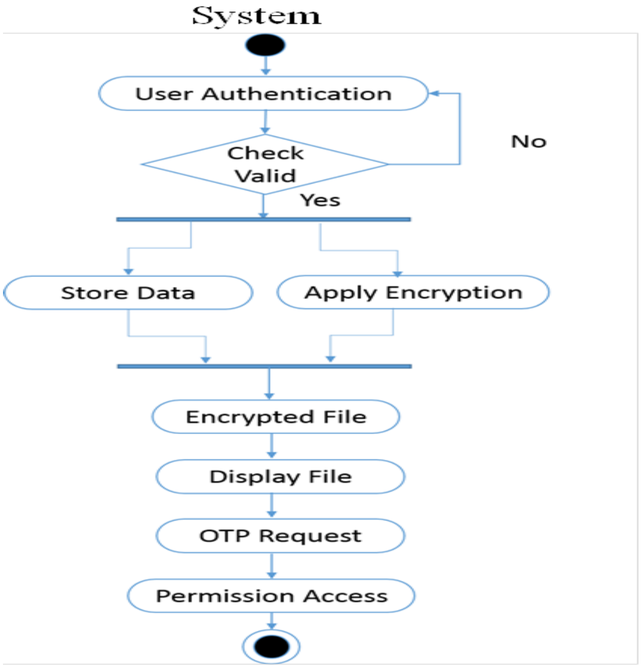

Fig 2. Flow Chart

X. FUTURE SCOPE

Cloud Computing security is a big challenge and also an issue to many researchers. The first priority was to focus on security which is the biggest concern of organizations that are considering a move to the cloud.

XI. CONCLUSION

To summarize, the work gives a model of a framework that can be used by organizations to protect and manage their data stored over untrusted public clouds. As part of the work the possibility of using delta encoding concepts along with homomorphic encryption scheme with additive homomorphism to update encrypted files, instead of transmitting entire encrypted versions each time after an update, was explored. Under the test environment, the developed prototype has delivered promising performance results as compared to other common solutions. Hence the proposed approach might be considered for use in real world scenarios.

XII. REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U. S. Department of Commerce, (2017)

[2] K. Lauter, M. Naehrig, V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?", CCSW' 11, Chicago, llinois, USA, pp. 113–124, (2015).

[3] Craig Gentry, "Fully homomorphic encryption using ideal lattice", in Proceedings of STOC'09, (2017).

[4] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, "Fully homomorphic encryption over the Integers", in Proceedings of Advances in Cryptology, EUROCRYPT'10, pages 24–43, 2016.

[5] Craig Gentry, "Computing arbitrary functions of encrypted data", Communications of The ACM, 53(3): 97-105, (2017).

[6] J. Li, D. Song, S. Chen, X. Lu, "A Simple Fully Homomorphic Encryption Scheme Available in Cloud Computing", In Proceeding of IEEE, (2015).

[7] Baohua Chen, Na Zhao, "Fully Homomorphic Encryption Application in Cloud Computing", in Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 11th International Computer Conference, (2018).

[8] Yan Zhang, Li Zhou, Yuanfan Peng, Jing Zhang, "A secure Image Retrieval Method Based on Homomorphic Encryption for Cloud Computing", in proceedings of the 19th