Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Technophilia-2018.

Volume 5, Special Issue 04, Feb.-2018 (UGC Approved)

"File Sharing Using Key Aggregation Searchable Encryption Via Cloud Storage"

Navale Madhuri [1], Sukale Shubhada [2], Dhomse Nikita[3], Phapale Pratiksha[4], Dumbre Archana[5]

[1]*Computer Engineering, JCEI'S Jaihind Polytechnic, Kuran*
[2] *Computer Engineering, JCEI'S Jaihind Polytechnic, Kuran*
[3] *Computer Engineering, JCEI'S Jaihind Polytechnic, Kuran*
[4] *Computer Engineering, JCEI'S Jaihind Polytechnic, Kuran*
[5] *Computer Engineering, JCEI'S Jaihind Polytechnic, Kuran*

Abstract — *Storage is the most prominent feature of cloud computing, growing rapidly in quality which gives immediate access to information through web service application programming web-based content management systems. In this system we use a data encryption standard algorithm for security purpose and we provide a more functionality as compare to existing system. Distribute a single key to user for sharing a large number of document and submit a single trapdoor to the cloud for quering the shared document. It is a brokerless network because there is no any third party interface. There is direct communication between host to host. When we exchanging a key at that time there is no any third person present between two host. So it is a brokerless network. This system is based on identity person. We shared the document to the identified person.*

Keywords- *Secure Encryption, Multiple file sharing, cloud server, data privacy.*

I. INTRODUCTION

The proposed KASE strategy applies to any cloud storage that supports the searchable multiple data sharing functionality, which means any user may share a multiple selected files with a selected users. To support searchable multiple file sharing the main requirements for efficient key management .First, a data owner only distribute a single aggregate key to a user for sharing group of files.

First sender generate an aggregate key for encryption of multiple files and upload the group of data on cloud server and send aggregate key for receiver.

Then receiver receive aggregate key from sender and download the files from cloud server and decrypt this files using aggregate key and view original data.

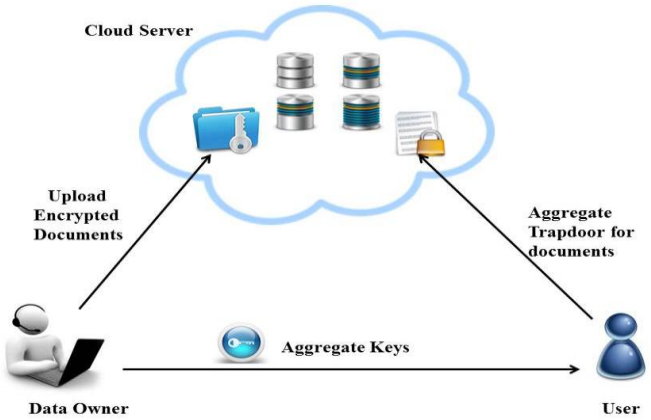

Fig.: Architecture Diagram

II. LITERATURE SURVEY

EXISTING SYSTEM

Key-aggregate Encryption for Data Sharing

Cloud storage is the most promissibal approach for data sharing hence we share secure data over cloud storage we share many files or single file at a time. When we share a file at that time we use encryption format of file for more data security. When we want to share a file in encrypted format first we want to generate a an aggregate key for

encryption of file with the help of different algorithm like MD5, DES, RAS etc and upload a file in cloud storage and receiver receive the file and decrypt the file using same key which is the sender send to receiver.

In particular chu et al. consider that to reduce number of aggregate key for multiple documents and to share a multiple document with different aggregate key each document have single key and each key is different from each other. Multiple key's are required for encryption of multiple document and same key's for decryption of multiple document. User could encrypt a message not only under a public key but also under the identifier of each document.

PROPOSED SYSTEM

- First define a general framework of file sharing using KASE via cloud storage composed of Data Encryption Standard (DES) algorithms for security parameter initial permutation, s-box /p-box, x-or/swap, final permutation. We then describe both functional and security requirements for designing a valid KASE strategy.
- We use Data Encryption Standard(DES) algorithm for more data security purpose.
- In group data sharing system based on the proposed file sharing using KASE via cloud storage strategy, and evaluate its performance. The evaluation confirms our system can meet the performance requirements of practical applications.

III. METHOD & MODULES

METHODS

Use case modeling identifies System and describes the system functions by using a tool called use cases System. Use cases describe the system functions System from the perspective of external users and in a manner and terminology System they understand. To accurately and thoroughly System accomplish this demands a high level of user involvement and a subject matter expert System who is knowledgeable about the business process or event.

1) Registration
2) Login
3) Generate Aggregate Key
4) Encryption on Files
5) Upload Files
6) Send Key To Receivers
7) Store Files
8) Receive Key
9) Decryption
10) View Original Files

MODULES

- Content-Based Sender/Receiver Module.
- Identity Based Encryption Module.
- Key Generation for Sender/Receiver Module.
- Secure Overlay Maintenance Module.

IV. RESULT & DISCUSSION

Algorithm – Data Encryption Standard (DES) Algorithm
Functional relations –

1. Data Storage Using Data Encryption Standard(DES).
2. File Retrieval Using Aggregate Key.

Mathematical formulation:

$L_i = R_{i-1}$

$R_i = L_{i-1} + f(R_{i-1}, K_i)$

V. CONCLUSION

We conclude that in existing system data sender need to create a multiple keys for user to sharing large number of documents and also created a multiple trapdoor to the cloud for quering shared document. But in purposed system we need not to create multiple keys for user to access multiple documents it provide a single key for large number of documents and provide a single trapdoor for quering that shared documents.

VI. ACKNOWLEDGEMENTS

First and foremost, we would like to thank my authors. Ms. MADHURI V. NAVALE, Ms. SHUBHADA R. SUKALE, Ms. NIKITA A. DHOMSE, Ms. PRATIKSHA K. PHAPALE, Ms.ARCHANA S. DUMBRE. for his guidance and support. We will forever remain grateful for the constant support and guidance extended by guide, in making this paper. Through our many discussions and ideas. The indispensable discussions we had with her, the penetrating question, has all led to the development of this paper.

VII. REFERENCES

[1] Baojiang Cui, Zheli Liu*, and Lingyu Wang, "Key Aggregation Searchable Encryption (KASE) for Group Data Sharing Via Cloud Storage" IEEE Transactions On Computers Vol: pp no.99, April 2015.
[2] K.Anusha, V.Lalitha, P.Siva Kumar, S.S.V.R Kumar.A, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing Via Cloud Storage" IJCSMC, Vol.5,Issue.4.April 2016,pp no 370-374.