International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

A Text File Encryption and Decryption System Based on ASE Algorithm using Java

R. Sudharsan[1], Ms. E. Durga Nandhini[2], Ms. Sarika Jain[3], Dr. S. Geetha[4]

[1]M.Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Chennai 600 089, Tamilnadu, India

[4]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

Abstract

Distributed computing is a model of web-based figuring where the assets like extra room, online programming are given by various cloud specialist organizations to various kinds of cloud clients who requirements cloud administrations. At the point when a cloud client rethinks the information on cloud, it needs to give greater security to reevaluated information forestalling information controlled or got to by unapproved clients. So, to keep up with information honesty, every single cloud administration must be put away safely. For more straightforward getting to of records and to create document lists, each record is put away in cloud server. Presently cloud clients search records and again send download solicitation to cloud server. This cycle is tedious and furthermore quite possibly the cloud specialist co-op could get to those documents which put away in cloud server, in light of the fact that both the encoded record and journalist key and record files are put away in cloud server. To conquer these issues, this framework presents capacity hubs for putting away document lists and encoded records and cloud server stores documents keys. At the point when a cloud client transfers document, the record list is produced consequently and record is encoded by utilizing AES calculation with naturally created key. After that by Visual cryptography plot, the key is changed over into picture and afterward created as key picture and source pictures individually. The encoded record and the document lists are put away hub, key and source picture are put away in cloud server and key picture is passed to record proprietor. At the point when record proprietor or document clients need to download or get to documents then perform search and afterward put key picture as an info. If legitimate, it coordinates the key with the source picture and later it very well may be downloaded.

1. Introduction

Distributed storage framework is a help model in which information are kept up with, oversaw and reinforcement somewhat on the cloud side, and in the meantime, information keeps accessible to the clients over an organization. Versatile Distributed storage (MCS) signifies a group of progressively well-known on-line administrations, and even goes about as the essential record stockpiling for the cell phones. MCS empowers the cell phone clients to store and recover records or information on the cloud through remote correspondence, which further develops the information accessibility and works with the document sharing cycle without depleting the nearby cell phone assets. The information protection issue is central in distributed storage framework, so the touchy information is scrambled by the proprietor prior to re-appropriating onto the cloud, and information clients recover the intrigued information by

encoded search conspire. In MCS, the cutting-edge cell phones are defied with a considerable lot of similar security dangers as computers, and different conventional information encryption techniques are imported in MCS. In any case, portable distributed storage framework brings about new difficulties over the customary scrambled search plans, with regards to the restricted figuring and battery limits of cell phone, as well as information sharing and getting to approaches through remote correspondence. Consequently, a reasonable and effective encoded search plot is fundamental for MCS.

2. Literature Survey

A. Moffat et.al,

Methodology: It describes about the compressing documents and images. The images and documents are compressed and they are managed respective to their gigabytes.

Algorithm Used: Memory-based inversion algorithm

Advantage: Security analysis show that the security level is guaranteed and enhanced for wireless communication channels.

Disadvantages: The draw backs of using a frequency stored index is a of course, more complex processing for Boolean queries.it is most appropriate in system that will only be required to support ranked queries and extra processing cost for Boolean queries.

D. Boneh et.al,

Methodology: A cryptographic system that uses two uses two keys- a public key known to everyone and a private key or secret key known only to the recipient of the message.

Algorithm Used: Polynomial time algorithms 4

Advantage: With a simplified search and retrieval process, it reduces the network traffic for the communication of the selected index, and reduces the file retrieval time in our experiments.

Disadvantages: The public key length grows linearly with the total dictionary size If we have an upper-bound on the Total number of key word trap doors that the user will release to the email gateway (though we do not need to know These key words a-prior) we can do much Better using cover-free Families and can allow key word dictionary to be of exponential size.

R. Curtmola et.al,

Algorithm Used: Notation and Preliminaries

Methodology: Searchable symmetric encryption allows a party to outsource to storage of data to another party in a private manner

Advantage: In implementing the redesigned encrypted search procedure, redistributes the encrypted index to avoid statistics information leak, and wraps keywords adding noise in order to render them indistinguishable to the attackers.

Disadvantages: We address both of these issues by proposing new in distinguish ability and simulation-based definitions that provide security for both indexes and trapdoors, and show their equivalence.

3. Existing System

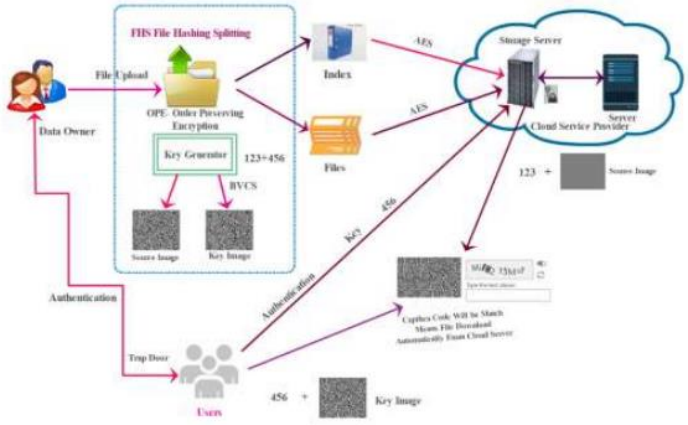
In this existing system file owner stores the file into the cloud server. So here, lots of file owners access permission in the same cloud server and at that time other file owner will access the other files. Owner can miss use the other owner's file. And the keys generated here can be easily hacked.

4. Proposing System

The Main aim of this Project is to secure the user files in cloud storage. Firstly, user uploads the files with their respective Login id. The main purpose of Cloud provider is to upload the files with secured image and generating OPE (Order Preserving Encryption) password. The purpose of secured image is, unauthorized user can't access the file in cloud. Here files are encrypted into two parts such as encrypted Index and encrypted files by using FAH (Fast Accumulated Hash) Algorithm. Now after splitting files, it automatically generates a secured image called as OPE password which is Not known to the third party. The secured is spitted into two images like Source and key image by using BVCS (Binocular Visual Cryptography schemes) algorithm. The encrypted file, Source image and OPE have been stored in cloud with respective file. If the user needs to view or select the particular file, the request must first be sent to the cloud service Provider. The provider verifies the user id and file request, later it will send OPE password and key image to user. Now the user has to send the key image to the cloud for accessing the files. The cloud matches the key image with the source image it already has. When both matches, it will send the file in the form of a Captcha and it can be downloaded. Hackers cannot hack the source image or key image and Captcha will be produced only when it is a valid user

5. Architecture Diagram

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



6. Modules

- Authentication
- File Uploaded with security
- mage Splitting (by BVCS)
- Encryption
- File view Request
- Verification

6.1 Authentication

Verification is the demonstration of affirming the reality of a trait of a solitary piece of information guaranteed valid by a substance. This module will keep up with the information of Client and Cloud Supplier. Verification is a cycle where the certifications gave are contrasted with those on record in a data set of approved client's data on a neighbourhood working framework. It could include affirming the character of an individual by approving their personality reports. Here Client and Cloud supplier subtleties like their name, email, contact number and area and so forth.

6.2 File Uploaded with Security

Transferring of information to the cloud server makes simpler for the client to recover the data. In this module, the Cloud supplier transfer the documents with got picture and OPE (Order Protecting Encryption) password. When gotten is empowered in cloud, client can undoubtedly store their information in portable cloud and recover the information rapidly. The reason for got picture is unapproved client can't get to the record in cloud. If somebody has any desire to see the record, they should realize the mystery picture or, more than likely can't see the document.

6.3 Image Splitting (by BVCS)

Picture parting is a method most frequently used to cut a bigger picture into more modest parts to make it load quicker. Cloud supplier transfer the client record with got picture, that picture ought to be parting into two pictures like source and key picture by utilizing BVCS (Binocular

Visual 23 Cryptography plans) calculation. Then, at that point, the critical picture and the OPE secret key will be ship off the specific client and the essential document can then be downloaded.

6.4 Encryption

The basic role of encryption is to safeguard the classification of advanced information put away on PC framework or communicated through the web or other PC framework. Current encryption calculation assumes a crucial part in the security confirmation of IT framework and correspondence as they can give secrecy as well as the honesty and non-disavowal. Encryption is utilized to shield information on the way sent from a wide range of gadgets across a wide range of organizations. Encryption is the best method for accomplishing information security. The Cloud supplier transferred the Client records that will be scrambled into two sections like encoded List and scrambled documents by utilizing FAH (Fast Gathered Hash) Algorithm prior to sending them to the cloud. The scrambled document needs to been put away hub with their particular record Id.

6.5 File View Request

In this module the end Client can see the accessible record list. If the client has any desire to see the document it ought to be chosen first and afterward send the record view solicitation to Cloud Supplier. Then, at that point, Cloud Supplier check the client profile after that it will send OPE secret phrase and key picture to client. Subsequent to matching the records, the documents can be downloaded. These secret qualities are utilized to see the record.

6.6 Verification

Check is the demonstration of looking into, examining or testing a specialized guideline. Presently the client needs to send the critical picture to the cloud for getting to the documents. The cloud coordinates the vital picture with the source picture it as of now has. When both matches, it will send the record as a manual human test. Then, at that point, it tends to be downloaded easily. It is the demonstration of evaluating, examining or testing to lay out and record that an item, administration or framework satisfies administrative or specialized guidelines.

7. Screen Shots

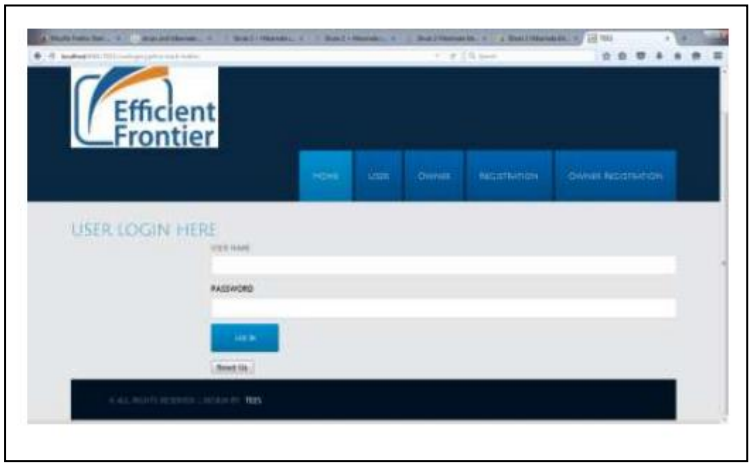
7.1 Homepage

Homepage displays the login details of the user and owner.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

7.2 User Login

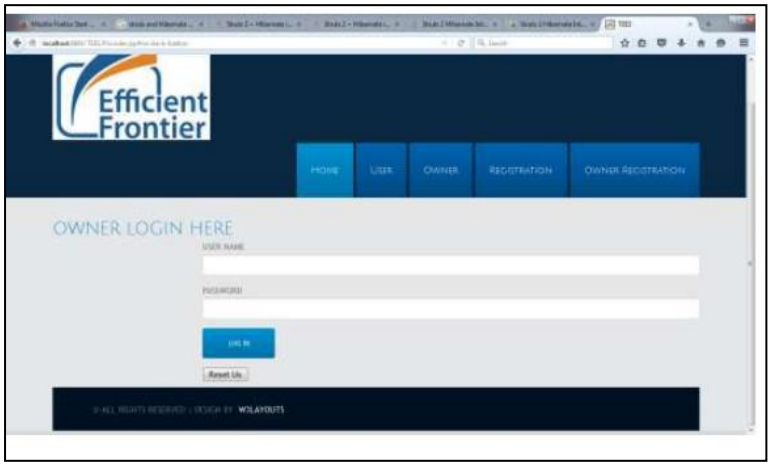
User logs into the cloud server with the respective username and password to access the files present in the cloud.



7.3 Owner Login

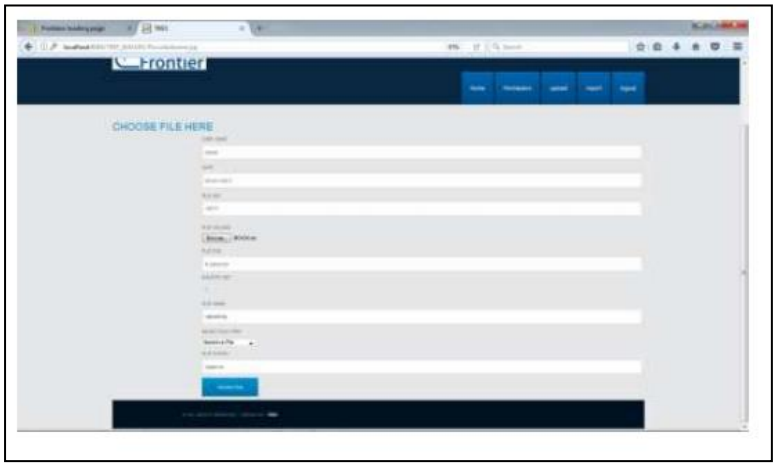
Owner logs into the cloud server with the respective username and password to upload the files present in the cloud.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



7.4 Owner Uploading Files

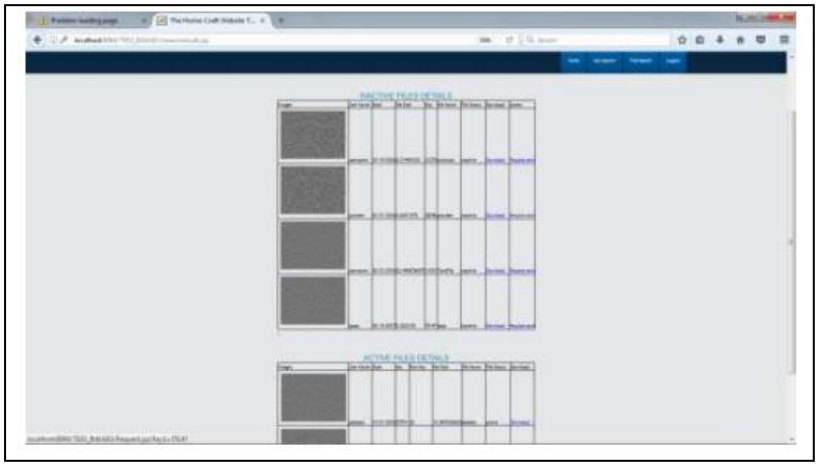
Owner uploads the files in the cloud server so as to allow the user to access the files present in the cloud.



7.5 User Requesting Files

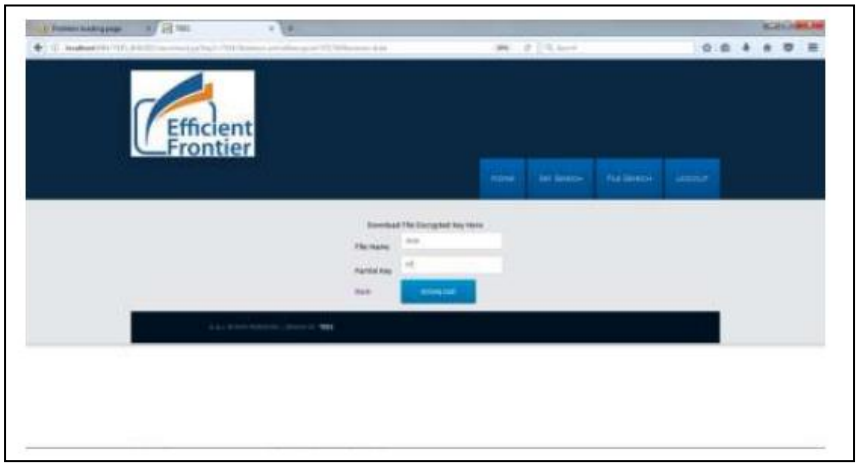
It displays the user requested files in the form of monochromatic images such that the image is not hacked easily.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



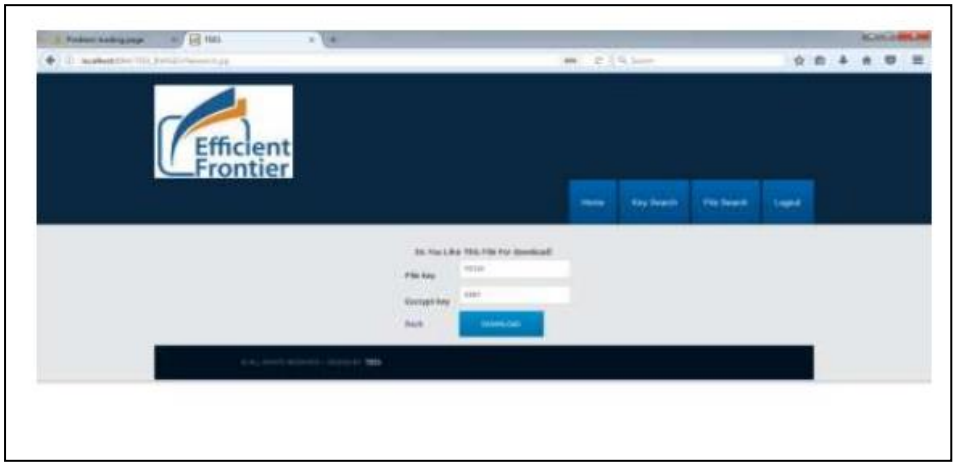
7.6 Entering File Key

After the successful download, the user should enter the file key in order to download the respective files.



7.7 Final Output

Finally, the user should enter the encrypted key and the file key for further downloading of the file documents.



8. Conclusions

In this work, we proposed a clever scrambled search framework Tees over the portable cloud, which further develops network traffic and search time proficiency contrasted and the conventional framework. We began with an exhaustive examination of the customary scrambled search framework and broke down its bottlenecks in the versatile cloud: network traffic and search time failure. Then, at that point, we fostered a productive design of Tees which is reasonable for the versatile cloud to resolve these issues, where we used the TMT module and the RSBS calculation to adapt to the wasteful inquiry time issue, while a hidden entrance pressure strategy was utilized to diminish network traffic costs. At long last our assessment concentrate tentatively exhibits the presentation benefits of Tees.

References

[1] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] X. Yu and Q. Wen, “Design of security solution to mobile cloud storage,” In Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[3] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[4] O. Mazhelis, G. Fazekas, and P. Tyrvainen, “Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage,” in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized in-cloud security services for mobile devices,” in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.