IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 5, Issue 2)

Available online at: www.ijariit.com

Achieving secure file download by traffic and energy saving encrypted search technique and generate key image using BVCS

Jeshima Firdouse R.
rjjcfirdouse@gmail.com
Velammal Institute of Technology, Chennai, Tamil Nadu

Shivani G.
shivani.g.shivani@gmail.com
Velammal Institute of Technology, Chennai, Tamil Nadu

ABSTRACT

Cloud Computing is a model of Internet-based computing where resources like storage space, online software are provided by different cloud service providers to different types of cloud users who need cloud services. When a cloud user outsources the data on the cloud, it has to provide more security for outsourced data preventing data manipulated or accessed by unauthorized users. To maintain data integrity, each and every cloud service has to be stored securely. For easier accessing of files and to generate file indexes, each file is stored in a cloud server. Now cloud users search files and again send a download request to the cloud server. This process is time-consuming and also there is a chance that the cloud service provider might access those files which are stored in the cloud server because both the encrypted file with correspondent keys and file indexes are stored in a cloud server. To overcome these problems, this system introduces storage nodes for storing file indexes and encrypted files and cloud server stores file keys. When a cloud user uploads file, the file index is generated automatically and the file is encrypted by using AES algorithm with automatically generated key. After that by Visual cryptography scheme, the key is converted into an image and then generated as key image and source images respectively. The encrypted file and the file indexes are stored in the storage node, key and source image is stored in a cloud server and the key image is passed to file owner. Whenever file owner or file users want to download or access files then perform search and then put a key image as an input. If valid, it matches the key with the source image and later it can be downloaded.

Keywords*— BVCS, Traffic efficiency, Energy efficient, FAH Algorithm, AES Algorithm*

1. OBJECTIVE

Cloud computing can be referred to as the storing and accessing of data over the internet rather than your computer's hard drive. This means that the data from either the computer's hard drive or over a dedicated computer network. Cloud computing is stored at a remote place and is synchronized with other web information.

2. SCOPE OF THE PROJECT

The scope of the project is to solve the security problems and retrieve the document from the cloud servers and also to reduce the time to access the document from the cloud server.

3. SYSTEM ANALYSIS

3.1 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 another file owner will access the other files. The owner can miss using the other owner's file. And the keys generated here can be easily hacked.

3.1.1 Disadvantages

- Server Information Acquisition
- Keywords-files Association Leak.
- Statistics Information Leak.

3.2 Proposed system

The Main aim of this Project is to secure the user files in cloud storage. Firstly, the 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 the secured image is, the unauthorized user can't access the file in the 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 an OPE password which is not known to the third party. The secured is spat into two images like Source and key image by using BVCS algorithm. The encrypted file, Source image and OPE have been stored in the 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 the 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.

.

3.2.1 Advantages

- Reducing File Search and Retrieval Time

- Reducing Energy Consumption
- Reducing Traffic Overhead
- control the statistics information leak
- Top-k relevant files searching algorithm.

3.3 Block diagram

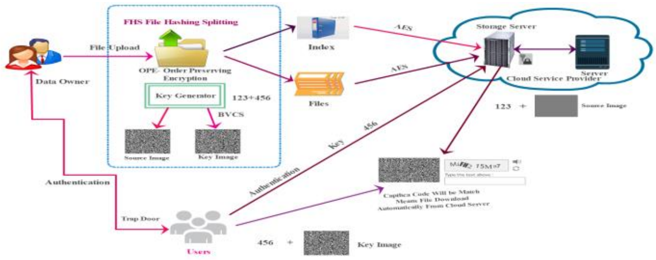

Fig. 1: States the block diagram of the search technique and key generation

4. MODULES

- Secure file uploading
- Splitting encrypted file
- Splitting encrypted file image split-up using BVCS
- Verification

4.1 Modules description

4.1.1 Secure file uploaded: In this module, to mitigate the security leakages it is implemented with security enhancement in consideration of the modified encrypted search procedure in order to mitigate statistics information leak and keywords-files association leak. The file is uploaded with secured images and password which is generated using File homomorphic Encryption algorithm. The main goal of these modules is to prevent the unauthorized user from gaining access to this file.

4.1.2 Splitting encrypted file: The primary purpose of encryption is to protect the confidentiality of digital data stored on a computer system or transmitted via the internet or another computer system. Modern encryption algorithm plays a vital role in the security assurance of IT system and communication as they can provide not only confidentiality but also the integrity and non-de-duplication. Encryption is the most effective way to achieve data security. The Cloud provider uploaded the User files that will be encrypted into two parts like encrypted Index and encrypted files by using AES (Advanced Encryption Standard) Algorithm before sending them to the cloud. The encrypted file has to been stored in storage node with their respective file Id.

4.1.3 Image split up using BVCS: Image splitting is a technique most often used to slice a larger image into smaller parts to make it load faster. Cloud provider upload the user file with a secured image, that image should be splitting into two images like source and key image by using BVCS (Binocular Visual Cryptography schemes algorithm. Then, the key image and the password will be sent to the particular user and the necessary file can then be downloaded. The password is generated which is then splitter into a source image and key image and they are stored to the user and cloud server

4.1.4 Verification: Verification is the act of reviewing, inspecting or testing technical-standards. 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 match, it will send the file in the form of a captcha. Then it can be downloaded easily. It is the act of reviewing, inspecting or testing in order to establish and document that a product, service or system meets regulatory or technical standards

.

5. ALGORITHM DESIGN

5.1 AES algorithm

AES (Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent. AES was designed to be efficient in both hardware and software and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

Steps in Advanced Encryption Standard

Step 1: Derive the set of round keys from the cypher key.
Step 2: Initialize the state array with the block data.
Step 3: Add the initial round key to the starting state array.
Step 4: Perform nine rounds of state manipulation.
Step 5: Perform the tenth and final round of state manipulation.
Step 6: Copy the final state array out as the encrypted data**.**

5.2 File hashing splitting algorithm

The two encryption methods used in this work for encryption use different keys. The key splitting module generates two random keys from the main key. It divides the key bits into half i.e. if the key is of length n then the generated random two keys will be of length n/2. The pseudo code for key splitting is given below:

Step 1: Input is n bit key.
Step 2: Set Key1 and Key2 as n/2 bit value and initialize it to 0.
Step 3: Initialize the random function with the given seed value. 323.
Step 4: Initialize length as n, i=0, j=0, flag=0.
Step 5: While (length! = 0)

5.1: If Flag==0 then
Find a bit of position randomly that has not been used. Find out the value at that bit position in the main key. If the value at that bit position is 1 then Set the i'th bit of key1 as 1 and Increment i value else Set the i'th bit of key1 as 0 and Increment i value Set Flag=1, Set the above-found bit position is used. Go to Step 5.3

5.2: Else
Find a bit of position randomly that has not been used. Find out the value at that bit position in the main key. If the value at that bit position is 1 then Set the i'th bit of key2 as 1 and Increment j value else Set the i'th bit of key2 as 0 and Increment j value Set Flag=0, Set the above-found bit position is used. Go to Step 5.3

5.3: Decrement the Length;
5.4: Go to step 5

Step 6: Return the keys key1 and key2 of size n/2.

6. REFERENCES

[1] Verifiable Symmetric Searchable Encryption For Semi-honest-but-curious Cloud Servers - Qi Chai, Guang Gong - Communication and Information Systems Security Symposium - 978-1-4577-2053-6/12/$31.00 ©2012 IEEE
[2] Searchable Encryption with Conjunctive Field Free Keyword Search Scheme - Fairouz Sher ALI, Songfeng LU-2016 International Conference on Network and

Information Systems for Computers - 978-1-4673-8838-2/16 $31.00 © 2016 IEEE DOI 10.1109/ICNISC.2016.82

[3] Privacy-Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics - Shuhui Hou, Tetsutaro Uehara - 2011 Third International Conference on Multimedia Information Networking and Security - 978-0-7695-4559-2/11 $26.00 © 2011 IEEE DOI 10.1109/MINES.2011.90

[4] Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data - Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou - Transactions On Parallel And Distributed Systems, VOL. 25, NO. 1, JANUARY 2014 - 1045-9219/14/$31.00 2014 IEEE Published by the IEEE Computer Society

[5] Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud - Bing Wang, Shucheng Yu, Wenjing Lou, Y. Thomas Hou - IEEE INFOCOM 2014 - IEEE Conference on Computer Communications - 978-14799-3360-0/14/$31.00 ©2014 IEEE.

BIOGRAPHY

Jeshima Firdouse R.
Student, Bachelor of Technology, Information Technology
Velammal Institute of Technology, Chennai, Tamil Nadu, India

Shivani G.
Student, Bachelor of Technology, Information Technology
Velammal Institute of Technology, Chennai, Tamil Nadu, India