

TEES - An Professional Exploration Method Above Encrypted Data on Mobile Cloud

L.Gunaseeli

*PG Student, Faculty of Computing, Sathyabama University,
Chennai – 119, India.*

Dr. R. Aroul Canessane

*Faculty of Computing, Sathyabama University,
Chennai – 119, India.*

Abstract

In this planned proposal, we present a Cloud Computing is a model of internet based computing where the resources like storage space, online software are provided by different cloud service providers to different types of cloud users who needs cloud services. Iaas – Infrastructure. As a service is one of the cloud service, mostly used by cloud users for outsourcing data and retrieving data from anywhere in the world. When a cloud user outsources the data on cloud, it has to provide more security for outsourced data preventing data manipulated or accessed by unauthorized users. So 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 files are stored in cloud server. Now cloud users search files and again send download request to cloud server. This process is time consuming and also there is a chance that the cloud service.

1. INTRODUCTION

The provider might access those files which stored in cloud server, because both the encrypted file and correspondent key and file indexes are stored in cloud server. To overcome these problems, this system introduces storage nodes for storing file indexes and encrypted files and cloud server stores files keys. When a cloud user uploads file, the file index is generated automatically and file is encrypted by using AES algorithm with automatically generated key. After that by Visual cryptography

scheme, the key is converted into image and source image and later it can be downloaded.

2. COPMARATIVE ANALYSIS:

S. no	Title	Author	Descriptions
1	“Fuzzy keyword search over encrypted data in cloud computing,” March 2010.	[11] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. j. Lou	As A Service is one of the cloud service, mostly used by cloud users for outsourcing data and retrieving data from anywhere in the world. When a cloud user outsource the data on cloud [1].
2	“Fuzzy Keyword Search on Encrypted Cloud Storage Data with Small Index 2011,	[12] C. Liu, L. H. Zhu, L. Li, and Y. Tan	It has to provide more security for outsourced data preventing data manipulated or accessed by unauthorized users. So to maintain data integrity, each and every cloud service has to be stored securely [2].
3	“Access pattern disclosure on searchable encryption: Ramification, attack and mitigation,” 2012.	[17] M. Islam, M. Kuzu, and M. Kantarcioglu	For easier accessing of files and to generate file indexes, each files are stored in cloud server. Now cloud users search files and again send download request to cloud server. This process is time consuming and also there is a chance that the cloud service [3].
4	“Preferred keyword search over encrypted data in cloud computing,” 2013.	[19] Z. Shen, J. Shu, and W. Xue	The provider might access those files which stored in cloud server, because both the encrypted file and correspondent key and file indexes are stored in cloud server. To overcome these problems, this system introduce storage nodes for storing file indexes and encrypted files and cloud server stores files keys [4].

5	“Semantic keyword search based on trie over encrypted cloud Data,” 2014,	[33] Z. Fu, J. Shu, X. Sun, and D. Zhang,	When cloud user uploads file, the file index is generated automatically and file is encrypted by using AES algorithm with automatically generated key. After that by Visual cryptography scheme, the key is converted into image and source image and later it can be downloaded [5].
---	--	---	---

3. EXISTING SYSTEM:

Every cloud user buy an space from a different cloud service providers, after that cloud users upload files into cloud server. At this time the file is encrypted and then file indexes are generated. That encrypted file is stored on the storage nodes, the file indexes and correspondent keys are stored in cloud server. By this way, files and its indexes are stored securely without any other information leak of the files. Whenever a cloud user or data owner wants to download or access files from cloud server, firstly the user needs to enter file index for identifying files from server. After that cloud user or file owner select particular file and then enter file key, this process is known as Two Round Search(TRS). Within this process the ranking function is also involved for increasing rank of the file index which is used by file requested user for making more reliable file indexes. After this, Cloud Server automatically checks the file key from cloud user or file owner. If it is valid then, request is automatically passed into the storage node. On the storage node the decryption operations would performed and then the decrypted file is transferred to file requested user that may be file owner or file user.

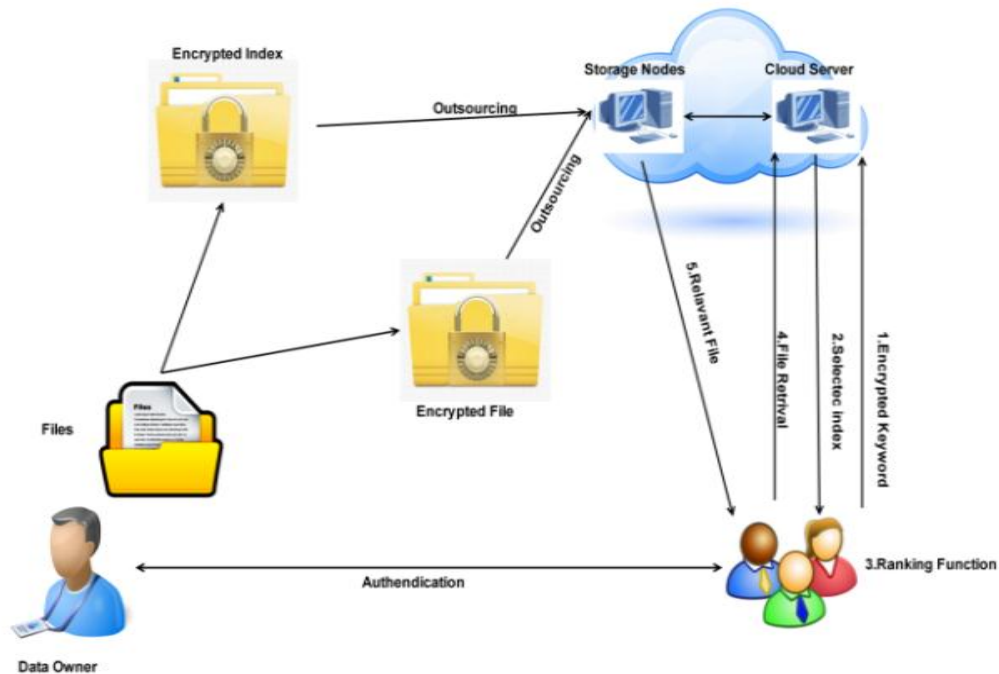
This process is time consuming and also there is a chance that the cloud service provider might access those files which stored in cloud server, because both the encrypted file and correspondent key and file indexes are stored in cloud server. Any system urbanized must not have a highly require on the available technical resources. This will surely lead to high demands on the obtainable technical property. This resolve direct to high difficulty creature placed on the client. The developed system should have a humble requisite, as only minimal or null changes are required for implementing with this system.

Disadvantages:

1. Server Information Acquisition
2. Keywords-files Association Leak.
3. Statistics Information Leak.
4. TRS(two round search)
5. encryption and the ranking incur the

Identifying files from server.

Existing diagram:



4. PROPOSED SYSTEM:

In this proposed system, cloud users buy a space from particular cloud server among more number of cloud service providers. Firstly, cloud user creates a file with 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 splitted 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

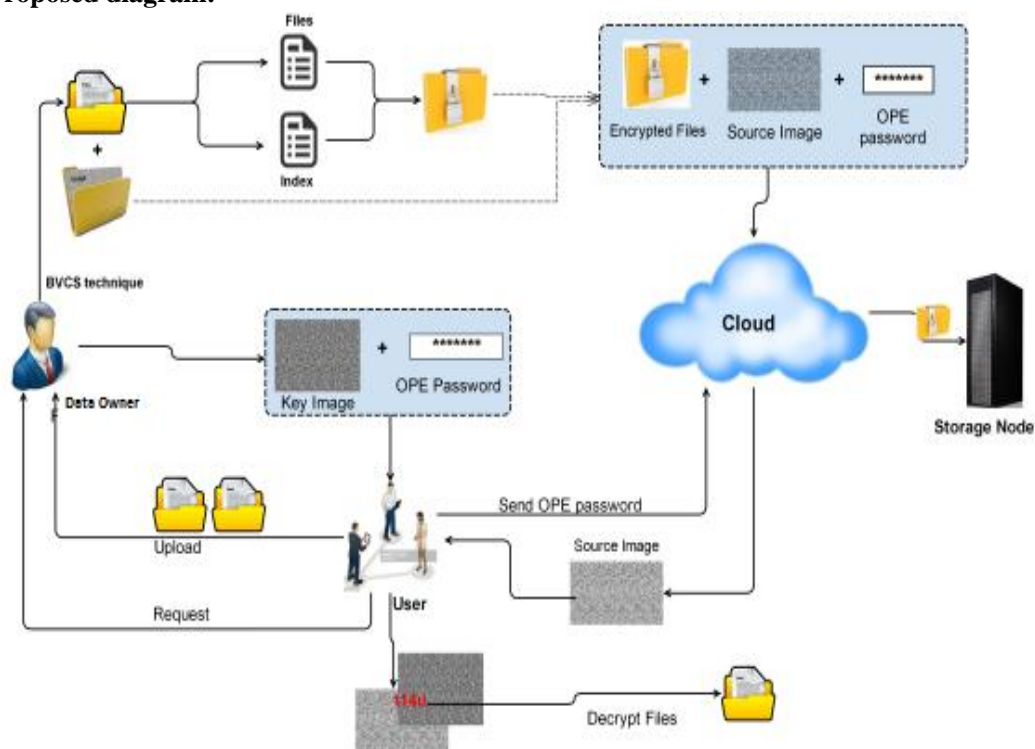
Accessing the files. The cloud matches the key image with the source image it already has. When both matches, it will send the file in the form of a cloud and it can be

downloaded. Hackers cannot hack the source image or key image and will be produced only when it is a valid user.

Advantages:

1. Reducing File Search and Retrieval Time
2. Reducing the Energy Consumption
3. Reducing Traffic Overhead
4. control the statistics information leak top-k relevant files searching algorithm.

Proposed diagram:



4.2. DESCRIPTION:

The software's that are used for the project are net beans and SQL. A net bean is used to build professional OS-independent desktop applications and SQL is used to update database, execute queries and manage permissions.

4.3. MODULES DESCRIPTION

An exclusively designed to have few implementation dependencies as probable. It is a high-level language. The Java program is both compiled and interpreted. With a compiler, you translate a Java program into an intermediate language called **Java**

byte codes – the platform independent codes interpreted by the Java predictor. With an predictor, each and every Java byte code instruction is parsed and run on the PC. The login credentials are secured by encryption and they are decrypted back by the server to avoid eavesdropping. User give their credentials to authenticate, System get their credentials and check with the Database if exists.

5. CONCLUSION

In this paper, the effects of An Professional Exploration Method above Encrypted Data on Mobile Cloud

Giving a model that expects the users' click points and their saliency value. Our main contribution is that we introduce. The provider verifies the user id and file request, later it will send OPE password and key image to user.

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).

REFERENCES:

- [1] **J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. j. Lou**, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March 2010.
- [2] **C. Liu, L. H. Zhu, L. Li, and Y. Tan**, "Fuzzy Keyword Search on Encrypted Cloud Storage Data with Small Index," in Proc. of IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), 2011, pp. 269-273.
- [3] **M. Islam, M. Kuzu, and M. Kantarcioglu**, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," In Proc. of NDSS'12, 2012.
- [4] **Z. Shen, J. Shu, and W. Xue**, "Preferred keyword search over encrypted data in cloud computing," In Proc. of 21st International Symposium on Quality of Service (IWQoS'13), 2013.
- [5] **Z. Fu, J. Shu, X. Sun, and D. Zhang**, "Semantic keyword search based on trie over encrypted cloud Data," in Proc. of SCC'14, 2014, pp. 59-62.