Data Seclusion in Multi-Owner Model using Dual-Encryption Method in Cloud Computing

M. Anusha[1]

[1]Second year M.Tech (CSE), R.V.R & J.C College of Engineering, Chowdavaram, Guntur. A.P, India

ABSTRACT: *- Cloud Computing is a new era in today's data sharing approach. Due to the availability of Public Cloud Servers (PCS) many of the Data Owners are willing to outsource their data by using PCS, there are many reasons to do so such as reduction in storage and maintenance cost, opportunity to choose the required hardware and software depending upon their necessity, easiness in adaptability of this technology…. etc.*
On the other side of the coin many organizations and individuals are still hesitant to outsource their sensitive information, the reason for this unwillingness is once the data is outsourced in a public cloud the owner loses the sole control of the data. Even though the CSPs (Cloud Service Providers) promise the owner to protect their data from the attackers but the data is no longer secluded from the CSP's itself, since the CSP possesses full control of cloud hardware, software and owner's data.

Here data security is the main consideration before outsourcing the data. To relate to privacy, safe searches over encrypted cloud data have inspired more research works under the individual owner model. However, most cloud servers in real do not just handle particular owner; instead, they support several owners to share the benefits of cloud computing. Having a huge amount of data files in the cloud server, it is crucial to give multi-keyword based search service to the data user.

To facilitate cloud server to perform a safe search without knowing the real data of keywords and to rank the search result the privacy of related scores between keywords and files has to be kept alive. For preventing the unauthorized persons from monitoring secret keys and pretending to be authorized data users submitting searches and downloads. In this paper, we suggest a new method for data storage firmly in cloud server using different encryption algorithms along with the secure search for data and fetching the data depending upon keywords and rank, using dynamic private key generation method and new user authentication procedure.

Keywords: *Cloud Computing, PCS (Public Cloud Server), CSP (Cloud Service Provider), Encryption, Key Generation, Authentication.*

I. INTRODUCTION: -

In today's world cloud computing is an emerging technology. Clouds provide access to inexpensive hardware, software and storage resources, and are based on a pay-per-use model [5]. People are becoming comfortable with data storing remotely in the environment of cloud. so, clouds are being increasingly used by many users.

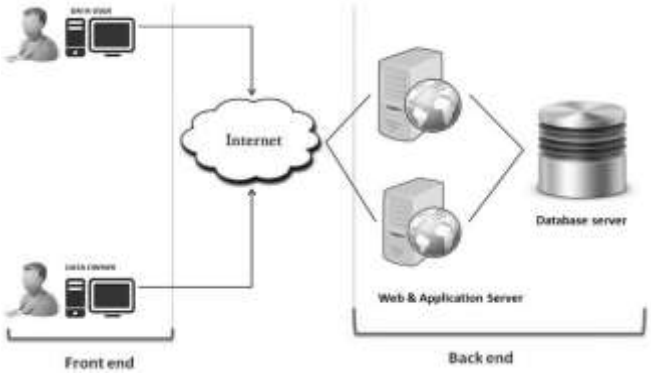

FIG.1. GENERAL SYSTEM ARCHITECTURE OF CLOUD COMPUTING

Figure 1. shows the general system architecture of cloud computing, there are two parts front end and back end. In the front end, there are users (data owner's/data users) and in backend database for storing the data.

II. ISSUES FACING BY CLOUD USERS

Nowadays all the data owners are moving towards the cloud. The outsourced nature of the cloud and the inherent loss of control that goes along with that means the sensitive data must be carefully monitored to ensure it is always protected.

- Privacy, Security & Compliance become shared statutory responsibility between the cloud provider and the data user, but, ultimately, it is the customer that is responsible. It's important to remember that once sensitive data is placed in the cloud, the data owner no longer has full control.
- With a huge amount of data files stored in the cloud server, it is important to provide multi-keyword based search service to the data user.

- Unauthorized access could be by attackers. The weak access, authentication & authorization controls could lead to unauthorized access [2]. Based on the type of Cloud Computing service, the clients / customers might have finite or nil rights to define the controls to prevent unauthorized access. Various approaches are used to minimize the risk of unauthorized access and sharing.

In this paper, we are concentrating on the above said issues.

- Sensitive data protection for data owners.
- Multi keyword based search service to the data user.
- New way of authenticating the user.

III.PROPOSED SYSTEM

The Proposed System ensures to resolve the challenges that are facing by the cloud users (Data Owners & Data Users) by dealing with the following issues.

Issue 1: - Sensitive data protection for data owners.

Service providers of cloud would guarantee to owner's data security using phenomena like virtualization and firewalls. These phenomena do not protect owner's data privacy from the CSP itself since the CSP control whole of cloud hardware, software, and owners' data. Secluding the sensitive data before send outside can store data confidentiality against CSP.

Issue 2: - Multi keyword based search service to the data user.

We introduce secure ranked keyword search without knowing the real data of both keywords and secret keys, Ranked search greatly enhances system usability by enabling relevance ranking and search result instead of sending identical results and further ensures the file retrieval accuracy.

Issue 3: - New way of authenticating the user.

In the proposed system a new way of authenticating the user has been introduced. While registering the user on the site by sending an "Authentication password" to user mobile, later on, login user can change the password. If the user enters the secret key, then the only user is authorized.

In the proposed system as shown in figure 2, whenever a new data owner or data user gets registered then an activation request is send to the admin server while the cloud users (Data Owners and Data Users) are authenticated via SMS of secret key which should be provided at the time of the first login as a password.

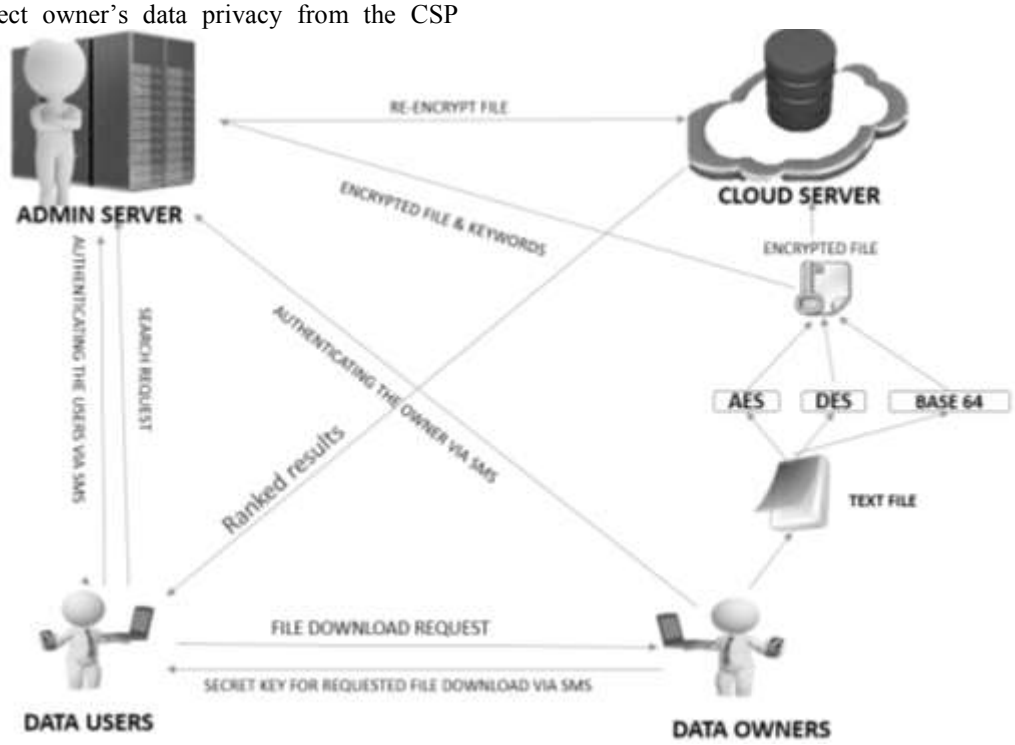

FIG.2. PROPOSED SYSTEM ARCHITECTURE

Figure 2. shows the proposed system architecture, it shows how does the owner's data secluded from CSP and how does the data owner and data user gets interacted for data sharing.

The Admin server has user revocation authority which means, the admin can activate or deactivate a cloud user. Only the admin activated user can login to the cloud.

Data Owner while uploading the file into the cloud chooses any one of the three encryption technique such as AES, DES and BASE 64. The single encrypted file along with its keywords reaches the admin server and cloud. Until and unless the admin re-encrypts the file data user couldn't see the file in search result even though the file assigned keywords to match with the search request. The admin re-encrypted file will be placed in the cloud. Neither the cloud nor the admin ever comes to know about the real data of the file, hence, the owner's data is secluded from the CSP.

Data user submits a search request to admin server which forwards it to the cloud, whereas the cloud provides the results which match with search request keywords rank wise based on a number of downloads does the file got, while the highly downloaded file gets the top position in the result list. data user upon seeing the result list put a download request to the corresponding file owner and upon receiving the dynamic (one time) secret key from owner via SMS the user downloads the file, for every new download (even for the same file from same user) a new secret key is generated for security purpose. The Owner can either accept or decline the data user's download request.

IV.ALGORITHMS USED IN THE PROPOSED SYSTEM

The Encryption algorithms used in this paper for Data Seclusion are:

- **AES (ADVANCED ENCRYPTION STANDARD).**
- **DES (DATA ENCRYPTION STANDARD).**
- **BASE 64.**

AES (ADVANCED ENCRYPTION STANDARD):- AES is a symmetric key block cipher encryption algorithm designed by Vincent Rijmen and Joan Daemen in 1998. It is based on Feistel network and supports 128-bit block size and key length 128, 192 and 256 bits[4]. AES performs 10, 12 or 14 round and the number of rounds depends on the key. It means for 128-bit key length AES performs 10 rounds, for 192-bit key it performs 12 rounds and for 256-bit key it performs 14 rounds. In AES each round performs some steps. Key-expansion, Initial-round, Rounds and Final-rounds. In Rounds step, Sub-byte generation, Shift-rows, Mix-columns and Add-round key are performed whereas, in Final-rounds step, same functions are performed except Mix-columns function.

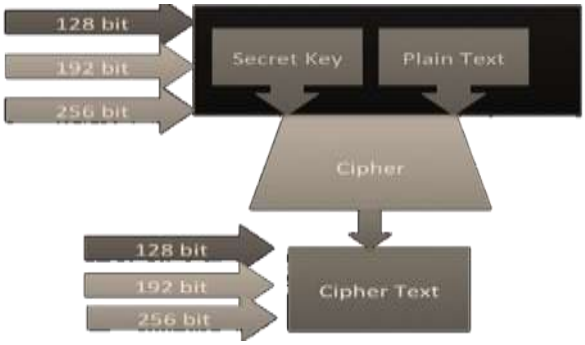

FIG.3. FLOW DIAGRAM OF AES

DES (DATA ENCRYPTION STANDARD): - DES is based on a cipher known as the **Feistel block cipher**. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure.

As with most encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is, therefore, a symmetric, 64-bit block cipher as it uses the same key for both encryption and decryption and only operates on 64-bit blocks of data at a time.

The key size used is 56 bits, however, a 64 bit (or eight-byte) key is actually input. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily and does not increase the security in any way[1]. All blocks are numbered from left to right which makes the eight bit of each byte the parity bit.

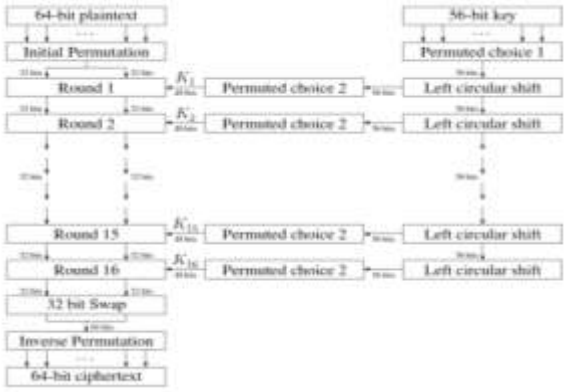

FIG.4. FLOW DIAGRAM OF DES ALGORITHM FOR ENCRYPTING DATA

Once a plain-text message is received to be encrypted, it is arranged into 64-bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. Multiple permutations and substitutions are incorporated throughout in order to increase the difficulty of performing a cryptanalysis on the cipher.

BASE 64: -Base64 encoding is used to convert binary data into a text-like format that allows it to be transported in environments that can handle only text safely[3].

The Base64 encoding process is to:

1. Divide the input bytes stream into blocks of 3 bytes.
2. Divide 24 bits of each 3-byte block into 4 groups of 6 bits.
3. Map each group of 6 bits to 1 printable character, based on the 6-bit value using the Base64 character set map.
4. If the last 3-byte block has only 1 byte of input data, pad 2 bytes of zero (\x0000). After encoding it as a normal block, override the last 2 characters with 2 equal signs (==), so the decoding process knows 2 bytes of zero were padded
5. If the last 3-byte block has only 2 bytes of input data, pad 1 byte of zero (\x00). After encoding it as a normal block, override the last 1 character with 1 equal signs (=), so the decoding process knows 1 byte of zero was padded.
6. Carriage return (\r) and new line (\n) are inserted into the output character stream. They will be ignored by the decoding process.

V. MODULES

In proposed system, there are four modules

- Data owners
- Data users
- Admin server
- Cloud server

Data Owners: The Data owner through sms receives a password for authentication when they get registered, later on, login owner can change the password. Data owner while uploading the file provides multiple keywords which help the users for feasible search and then chooses any one of the three encryption techniques such as AES,DES and BASE 64 for encryption of the file.The encrypted files and its keywords reach the admin server and cloud. Upon Receiving the request for the download of the file by data user, the owner can either accept or reject the request.If the data user file request is accepted then the owner sends a dynamic one-time secret key to the user via SMS to download the file.

Data User: The Data user through sms receives a password for authentication when they get registered, later on, login user can change the password. Data user searches the cloud for the file using multiple keywords.Upon receiving ranked search result having a highest downloaded file at the top of the list.The user sends a download request to the corresponding owner of the file.The user receives the one-time secret key via SMS if the owner accepts the request.The user downloads the file by entering the key.For every new download, a new key is required.

Admin Server: The Admin server gets activation request from data owner and data user when they get registered.Admin can either activate/deactivate the user or owner.Only the activated ones can log in to their account,by this admin performs an effective user or owner revocation.The data owner uploaded file will be re-encrypted and placed in cloud server by admin server.Before re-encryption user couldn't get to see the owner uploaded files in the search result list.Admin server forwards the data user file search request to the cloud server.

Cloud Server: The Cloud server produces the ranked search result list, where the list is in descending order of a number of downloads.The result list is displayed to the data user.Cloud server stores the encrypted files and keywords,it doesn't know the actual content of the file,so as secluding the owner's data not only from attackers but also from the cloud server.

VI. CONCLUSION

In this paper, we discussed the problem of secure multi-keyword search for several data owners and several data users in the cloud computing environment. And also our proposed method enable genuine data users to perform safe,proper and valuable searches over multiple data owners' data. A new user authentication procedure and dynamic private key generation method are proposed to efficiently authenticate data users and distinguish unauthorized users who get the private

key and perform unauthorized searches. To enable the cloud server to perform a secure search among multiple owners data which is encrypted. we suggest a new method for data storage firmly in cloud server using different encryption algorithms. To rank the search results and preserve the privacy of relevance scores between keywords and files, we suggested a secure search for data and fetching the data depending upon keywords and rank, using dynamic private key generation method. Hence, the data stored in the cloud is secluded for attackers.

REFERENCES:

1. "A Study of Encryption Algorithms for Security",Global Journal of Computer Science and Technology Network, Web & Security
2. W.Stallings, "Cryptography and Network Security 6th Ed," Prentice Hall , ,PP. 58-309 .
3. http://www.herongyang.com/Encoding/Base64-Encoding-Algorithm.html
4. "Performance Evaluation of Cryptographic Algorithms: DES and AES", 2013 IEEE Student's Conference on Electrical, Electronics and Computer Science
5. Cloud computing Application architectures, George reese.