Dual Encryption Scheme with Owner & User Control over Cloud Data

Suriya A
IFET college of engineering
Suriya0419@gmail.com

Abstract--**Cloud is playing an important role in the recent years. Cloud computing is the delivery of computing services over the network. We can store and process data using cloud. The data should be encrypted and stored in the cloud for the security purpose. Due to lack of security, the attackers or intruders may hack the data which is stored in the cloud .In the existing system, the encrypted text key is maintained by either cloud administrator or file owner. The proposed method uses dual encryption scheme, so as to give more data security. In this concept, one key is handled by the file owner and another key by the administrator. Here, attribute based AES (Advanced Encryption Standard) algorithm is used to encrypt and decrypt the data. User can access data in cloud using the encryption key; the key will be changed automatically once the access is over.**

Index Terms--**Cloud computing, Encryption Key, Cloud Administrator, Automatically Regenerated, Dual Encryption.**

INTRODUCTION

Cloud can be used as a public cloud, private cloud or hybrid cloud. Public cloud services can be offered over the internet and cloud offer space to store and process data in it. In private cloud, the infrastructure is dedicated to a particular organization and not shared with other organization. The usage of both public and private cloud is called hybrid cloud. Cloud computing has many challenges when data owner and data users are involved to store data in the offsite location. When it comes to cloud computing security and privacy of personal information is extremely important. The need for data encryption is related to data ownership, guarantee towards quality of service are some of the challenges faces by the cloud users.

This paper introduces dual encryption scheme. The first encryption is done on owner side and another encryption done under the cloud. Dual encryption scheme enhances security on cloud data. The encrypted key is changed automatically in cloud once the access is over. The data owner can get notification of each and every process can occur in cloud. Using this automatic key generation process the data can be more secure in cloud, when compared the previous work.

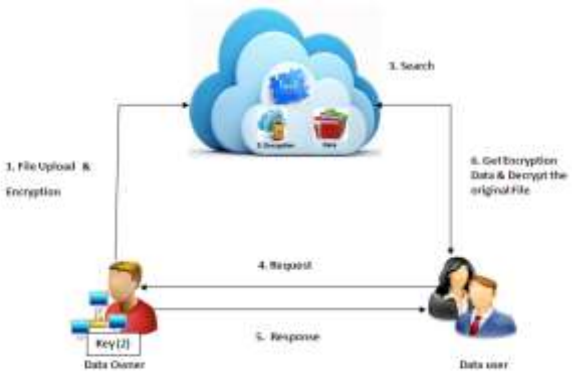
Related Work:

Major security challenges are the generation, distribution, and usage of encryption keys in cloud systems. One of ways to provide security, proxy re-encryption scheme is proposed, in which a semi-trusted proxy transforms a cipher-text for data sender into a cipher-text for data receiver without seeing the underlying plaintext. This paper proposes a new re-encryption scheme for secure data sharing, which is based on a trusted authority.

Updation and deletion of data should be handled by data owner only and generated encrypt key is given by the data owner. They used single encryption and this handled by cloud administrator. Secret key is given by data owner so security system maintains public key for encrypted data. They used multilayered encryption scheme to encrypt the original data

Multiple data owners and multiple data users are used for secure multikeyword search. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, they construct a novel secure search protocol. Additive Order and Privacy Preserving Function (AOPPF). Security measure is inefficient due to multiple data owner. Authorization of data owner and privacy confidentiality are not focused. Efficient privacy-preserving search method over encrypted cloud data that utilizes minhash functions. This method is the capability of multi-keyword search in a single query using minhash Algorithm for preserving privacy for multi-keyword search and Inverse document frequency for keyword search. minhash function takes much of computation time to process for user queries. It occupies large amount of space to store keyword of documents. It rising lot of questions on process when data size increase.

THE SYSTEM ARCHITECTURE:



(a)The Architecture of Dual Encryption Scheme and Automatic key Generation over cloud data.

Proposed method:

In dual encryption scheme, one key is stored in cloud and another will be used by the data owner. Two layer authentication can be used for users. One process is login and another one is file accessing under the cloud data. Data owner should know every processing on file. To view the file inn cloud, the users can give key request to the data owner. Data owner can accept the request or denial the request. The secret key will be regenerated automatically to the administrator to provide the data more secured in cloud.the two main thing can be proposed in this scheme ,

1.Dual Encryption is used to keep the data as more secured using private cloud data can stored in this process.

2.Automatically Encrypted key changed and it will regenerated to data owner.

Module description:

1. Encryption:

The dual encryption scheme is used in this work with AES (Advanced Encrypted Standard). While uploading the file, the first encryption will be done, the second is when storing the data into drive cloud account. Meta data should not be encrypted due to search scheme.by using 64 bit encoder to encrypt the data in cloud

2. Key generation:

This process is to generate the secret key in the independent manner. The key size is 256 bits, while uploading a file, two keys will be generated. One key is handled by the data owner while another by cloud account. Only private keys is allowed in this process.

3. Authentication and key distribution:

Authentication can be done using cloud account secret password with alert in the e-mail. The data owner sends the key to the requested user. He can accept or deny the key request. The key can be send only he accepts the request. The key can be sent through the email.

4. Decryption tool:

This tool is given by the cloud service provider. The data can be decrypted using online and offline tool. Authenticated users can downloaded the tool using their registered account. Java swing application is used in their work to decrypt the key.

5. FTP:

File transfer protocol (FTP) is used to communicate with drivehq cloud account. This protocol is used to store and receive the data.

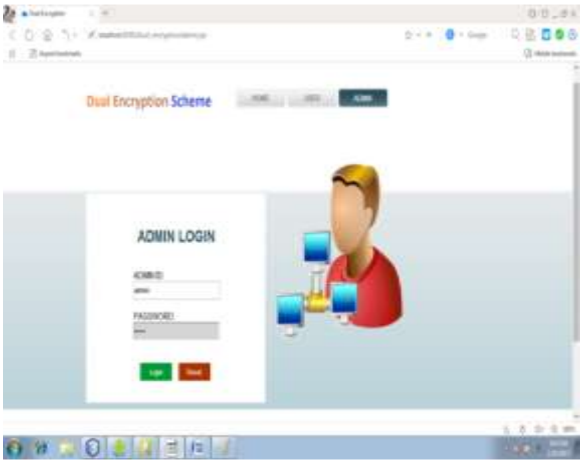
Algorithm Explanation:

Attribute based AES with dual encryption is used in this work to secure the data which is stored in the cloud. This algorithm use 256 bit auto generated secret key. The generation of key is either first or second encryption. The existing system used 12 to the rounds to encrypt and decrypt the data, but in this work, 16 rounds were used because of attribute based encryption. Attribute contains user data and file details.

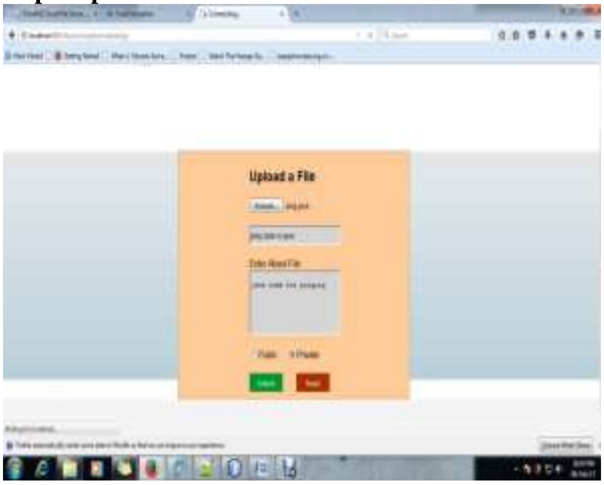
SAMPLE IMPLEMENTATION:

Step 1:Admin Login:

Admin can login with their Admin name and their password.

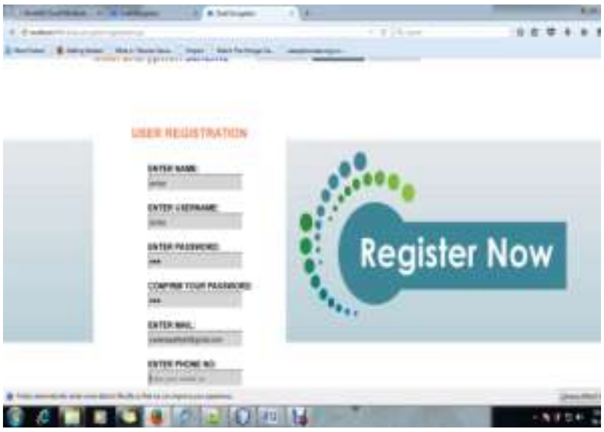


Step2:Upload a file:

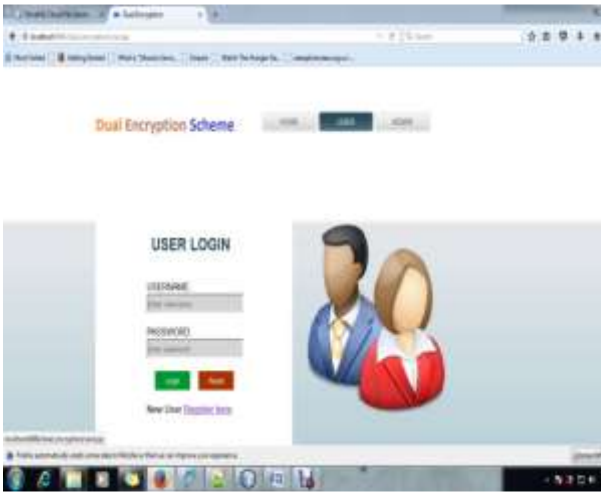


Step 3: Registration & User login:

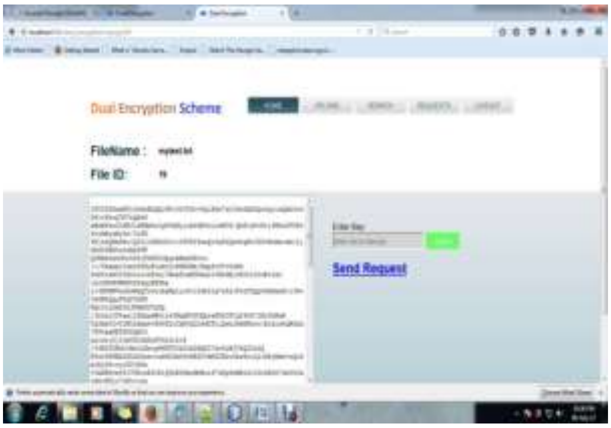
New user means they can register with required details.

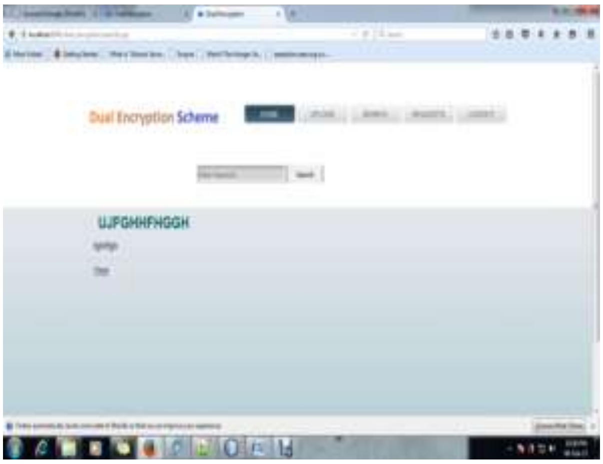


Then perform login operation in cloud with the user name and password

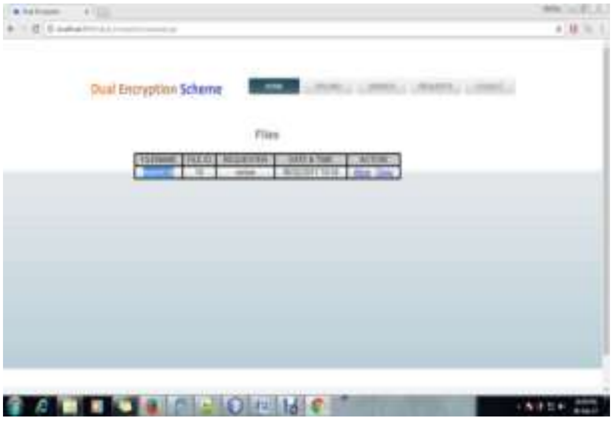


Step 4: User Search data in cloud:

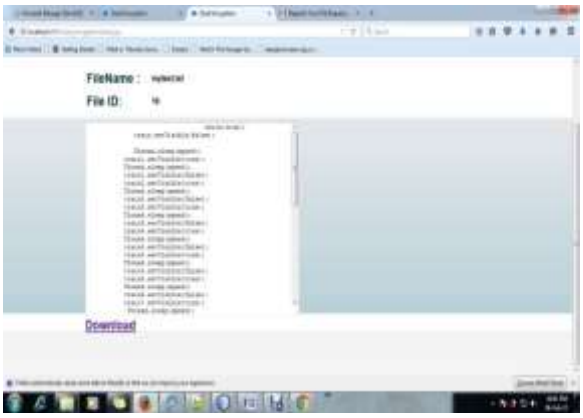




Step 5: Users Key Requests:



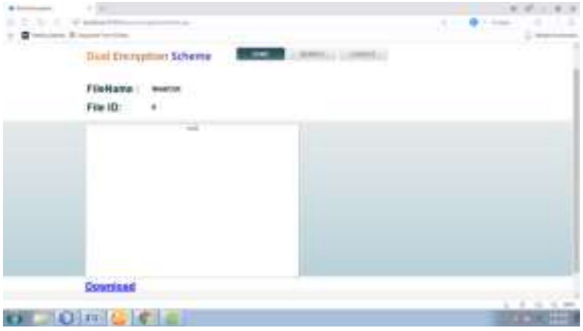
Step 6: Decrypt the data using Encryption Keys



FileName : [illegible]

File ID: [illegible]

Step: 7 Automatically Encryption Key changed:



FileName : [illegible]

File ID: [illegible]

User may access data in another time by using old encryption key without owner permission means it displays null message because encryption key is automatically changed.

Conclusion:

In this paper dual encryption method is proposed, which supports not only encryption but also automatic key generation method. In this process private method can be used to perform Encrypt the data in dual time. The first encryption done under owner side and second encryption is done under cloud admin by using AES algorithm. There are still many challenge problems in encryption schemes. In proposed scheme the data owner is responsible for generating encryption key updating information and sending them to the cloud server. Some data users are trustworthy. It is not practical and a dishonest data user will lead to many secure problems, like a dishonest data user may search the documents and distribute decrypted key to unauthorized ones. So that automatic key generation method is proposed for randomly key generated for separate data to handle these challenge problems.

References:

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,”IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan-Feb.2012.

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” inProc. Financ. Cryptography Data Secur., 2010, pp. 136–149.

[3] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2009.

[4] O. Goldreich and R. Ostrovsky, “Software protection and simulation on oblivious rams,”J. ACM, vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” inProc. Adv. Cryptol.-Eurocrypt, 2004, pp. 506–522.

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, “Public key encryption that allows pir queries,” inProc. Adv. Cryptol., 2007, pp. 50–67.

[7] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” inProc. IEEE Symp. Secur. Privacy, 2000, pp. 44–55.

[8] E.-J. Goh, “Secure indexes,”IACRCryptol.ePrint Archive, vol. 2003, p. 216, 2003.

[9] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” inProc. 3rd Int. Conf. Appl. Cryptography Netw.Secur., 2005, pp. 442–455.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun.Secur.,2006, pp. 79–88.

[11] N. Leavitt, “Is Cloud Computing Really Ready for Prime Time?” Computer, vol. 42, pp. 15–20, January 2009.

[12] J. Brodkin, “Gartner: Seven Cloud-Computing Security Risks,” Network World, July 2008.

[13] G. Srilakshmi, M Preethi, “Security Schemes in Distributed Data Storage Using Proxy Re-encryption,”International Journal of Advanced Research in Computer Science and Softward Engineering, vol. 4, no. 11, pp. 743-474, 2014.