VERIFIABLE AND MULTI-KEYWORD SEARCHABLE ATTRIBUTE BASED ENCRYPTION SCHEME FOR CLOUD STORAGE

[1]Aravind T, [2]Praba G, [3]Sowndarya K, [4]Susma Reddy N

[1] (Asst. prof/CSE, Muthayammal Engineering College, Rasipuram, Email: aravind.t.cse@mec.edu.in)

[2] (Student/CSE, Muthayammal Engineering College, Rasipuram, Email: prabaganesan44@gmail.com)

[3] (Student/CSE, Muthayammal Engineering College, Rasipuram, Email: sonucse1620@gmail.com)

[4] (Student/CSE, Muthayammal Engineering College, Rasipuram, Email: susmaengcse@gmail.com)

Abstract: In an attribute-based searchable encryption (ABSE) scheme, data owners will encrypt their data with access policy for the purpose of security consideration, and encrypt keywords to get keyword index for privacy keyword search, and data users will be able to search interesting keyword on keyword indexes by keyword search trapdoor. In many existing searchable encryption schemes it only supports single keyword search and most of existing attribute-based encryption (ABE) schemes have high computational costs at user client. In this paper, we propose a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme for cloud storage, in our new scheme multi-keyword can be searched and also the search privacy is protected. That is, the cloud sever can search the multi-keyword with keyword search trapdoor but it doesn't know any information of the keywords searched. within the proposed scheme, many computing tasks are outsourced to the cloud proxy server, which greatly reduces the computing burden at user client. Besides, the scheme also supports the verification of the correctness of outsourced private key.

Keywords: ABSE, verifiable outsourcing, adaptive security, multi-keyword search

---

I. INTRODUCTION

The development of cloud computing, many of the information can be shared through computer networks. Variety of services, such as outsourcing commission calculations and data storage can be provided for the users by cloud server(CS). Users can store their large amounts of data to the CS and share data with other users. For the purpose of the security of storage data and user's privacy, data is usually stored in encrypted form in CS.

The searchable Encryption (SE) is a cryptographic technology that has been developed from many years, and it also supports users' keyword search in cipher text. In the meanwhile, it can also save a lot of network and computational overhead for the user, and take advantage of huge computing power of CS. The SE technology mainly solves the problem of how to use the server to complete the search for interesting key-words when the data is encrypted and stored in CS, but CS is not completely trusted. How to improve the efficiency of keyword search

while reducing local computing load is still a major problem to be solved.

In most of the existing schemes single keyword search is supported. Single-keyword search will waste network bandwidth and computing resources, as this search method returns a major number of results, this means that the search result is not proper. In order to solve this problem, we propose multi-keyword search. Most of the existing attribute-based encryption (ABE) schemes results in high computational costs at user client. These problems greatly limit the applications of ABE schemes in real time practice. We proposed a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme to solve the problems of network bandwidth waste and high computational cost, for cloud storage in this many computing tasks are outsourced to cloud proxy server to reduce local computing burden.

II. LITERATURE SURVEY

Attribute-based Keyword Search Efficiency Enhancement Via an Online/Offline Approach [1]

AUTHOR: Qiuxiang Dong, Zhi Guan

Searchable encryption is a primitive, which not only protects data privacy of data owners but also enables data users to search over the encrypted data .Cloud instances are isolated in the network from other instances for improved security. The data owners needs to use every authorized user's public key to encrypt data and the application is restricted in real environment. New attacks which recovers the contents of individual user queries by assuming no leakage from the system except the number of results is presented [3].

By exploiting the behavior of specific applications, we can immediately have an attack without making further assumptions like prior work does about the underlying system.

Practical Techniques for Searches on Encrypted Data [2]

AUTHOR: Dawn Xiaodong Song David

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. They are secure and they provide provable secrecy for encryption, which means that the un-trusted server cannot learn anything about the plaintext given by the cipher text [7]. It is impossible to learn about the plaintext than the search result by the un-trusted servers. The current security mechanism poses a risk for organizations that outsources their data management to the un-trusted servers. Encrypting and decrypting sensitive data at the client side is the common approach in this situation but it has high communication and computation overheads if only a subset of the data is required, for example, selecting records in database table based on the keyword search. New cryptographic schemes are been proposed that support encrypted queries over encrypted data but all depend on a single set of secret keys, this implies that the single user access or share keys among multiple users, with key revocation requiring costly data re-encryption.

Public Key Encryption With Keyword Search Based On Factoring [3]

AUTHOR: Wenjun Luo, Jianming Tan

Public key encryption with keyword search (PKES) enables senders to send encrypted data to F receiver like traditional public key encryption (PKE) schemes. The PKES used in the factoring scheme is secure and it is computationally efficient. The public parameters in the scheme is short, it is in need of public modules and a random element of

the set of integers. This problem is the focus of active research and several security definitions and the constructions which have been proposed. In this paper we are going to review existing security definitions, which point out their short- comings, and propose a new stronger definition which is proved to be equivalent. We then present the constructions which is secure under our new definitions. And also to satisfy stronger security guarantees, these constructions are more efficient than all previous constructions.

Fuzzy Keyword Search Over Encrypted Data in Cloud Computing [4]

AUTHOR: Li, Dong Zheng, Yinghui

The information is being centralized into the cloud and data is encrypted before outsourcing. It greatly enhances system usability by returning the matching file when user is searching. It only supports exact keyword search. And also to satisfy stronger security guarantees, these constructions are more efficient than all previous constructions. Further work on SSE only considers the setting where the owner of the data is capable of submitting search queries. The natural extension where an arbitrary group of parties other than the owner can submit search queries is considered in this process. The SSE in this multi-user setting, and present an efficient construction is defined.

III. SYSTEM ANALYSIS

A. Existing System

An encryption operation which takes one minute on a PC will take about half an hour to finish on a mobile device. The current solutions that we provide don't help in solving the problem of user privilege very well. This type of operation will result in very high revocation and computational cost. This is also not applicable for mobile devices as well. And even, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud.

B. Disadvantages

There is no proper mechanism for providing the security for data that is presented in the mobile cloud.User authentication and revocation cost will be high.Encryption strategies such so the populace authorization encryption are not anonymous. The adversaries reap the cipher texts, he do without problems are aware of the proprietor regarding the cipher text so nicely as whomever intention gets hold of the cipher text.They might also will according part records only including receivers who have certain attributes. Data carriers then receivers hold to affirm the truth concerning each lousy according to redact sure that data or the identity won't keep leaked out.The attributes additionally need according to keep protected.

C. Proposed System

In this process we are providing methods for efficient access of the data. Performance has been increased with the reduced cost. Random based key management service is practiced. This proposes a searchable encryption that is based on attributes and supports multi-keyword search. Searchable encryption is a primitive method; it not only protects data privacy of data owners but also enables data users to search over the encrypted data. Most of the existing searchable encryption methods are in the single-user setting. There are only few schemes in the multiple data users setting, which encrypt data with the help of sharing data.

D. Advantages

First proposed the notion about the privacy about the keys is high secure. The most recent approaches borrow ideas from attribute-based encryption to enable

attribute-based keyword search (ABKS).Achieving attributes authentication earlier than re-encryption, or ensuring the protection over the attributes and data. Receivers whoever are certified in imitation of know the information do use their keys in conformity with decrypt the cipher text, however others cannot, consequently data providers' privations be able stand protected. To perfect the current PRE system considered the scenario to that amount information companies may additionally need the records to stay conditionally shared.

IV. MODULE DESCRIPTION

A. Data owner

The data owner should have to be registered initially to get access about the profile. In the encrypted format data Owners will upload the file to the cloud server. Randomly the encryption key generator will be generated while uploading the file to the cloud.

B. Data user

Data User will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data User can access the file based on the key received from mail id. Based on the key received, the consumer can verify and decrypt the data from the cloud.

C. Semi-trusted server

In LDSS, proxy encryption server and proxy decryption server are introduced to assist users to encrypt and decrypt data so that user-side overhead can be minimized. In addition, the proxy servers will also be operated in the cloud. So, we consider that they are honest but actually they are curious just as the CSP.

D. Trusted authority

A trusted authority (TA) is introduced. It is responsible for generating the public and private keys, and also for distributing attribute keys to users. We assume that the TA is entirely credible, and a trusted channel exists between the TA and every user. The purpose of TA is to transfer keys (in a small amount) securely between users. In addition, it keeps watching that the TA is online all the time because data users may access data at any time and need TA to update the attribute keys.

E. Secret sharing on lazy re-encryption

The cipher text controls the access of the data, data needs to be re-encrypted when some users' access privileges to the data to be revoked. However, frequent re-encryption brings heavy computational overhead, and the accessed plain text data may already be stored in these data users. Therefore, this paper adopts the lazy re-encryption method proposed. With lazy re-encryption, when a user's access privilege is revoked, data is not re-encrypted until the data owner updates the data the file of the access control policy that contains these attributes will be marked.

F. Data access control

The security of access control policy is that no participants can know about the specific content of the access control policy except data owners. LDSS introduces attribute description field so that access control policy is described by the corresponding attribute description bit. ESP and the Cloud can only get the relationships between different attribute description bits, but not the specific content of access control strategy, thus protecting the access control strategy.

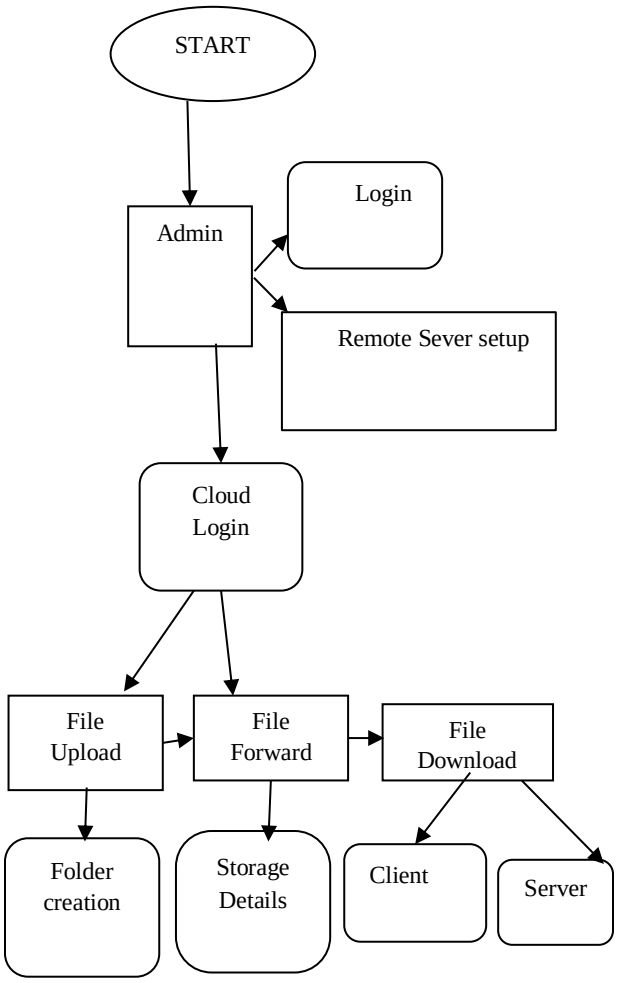

Fig: Flow Diagram

V. ALGORITHM

1. SYSTEM SETUP (λ , *U*) → *PP* , *MSK* . The setup algorithm is executed by *AA*. It inputs security parameters λ, attributes universal set *U*, outputs the public parameters *PP* and master secret key *MSK*.*AA* publishes *PP* and keeps *MSK* secretly.

2. KEY GENERATION (*PP* , *S*) → SK_o . The outsourcing private key generation algorithm is executed by *CPS*. It inputs *PP* and a set of attributes $_{S.}$ outputs outsource private key SK_o and sends SK_o to *AA* .

3. ENCRYPTION (*PP* ,= (*M* , ρ)) → *CT* ′ The outsource encryption algorithm is executed by *CPS* , the algorithm inputs *PP* , and access policy , outputs intermediate ciphertext *CT*.

4. TRAPDOOR GENERATION (w j ′ , SL) → TD . The user provides the input as SK L and the keyword set WD′ that he wants to be queried and generates a trapdoor TD and sends it to CS.

5. SEARCH (*I* ,*TD*) → 0 *or* 1 . The *CS* takes trapdoors *TD* and index *I* as input. If the trapdoor and index can match successfully, the algorithm outputs 1, otherwise outputs 0.

6 .DECRYPTION (*PP* , *IK* , *CT*) → *E* . The algorithm performs decryption of ciphertext *CT* through *CPS* under the access policy (**M**,)ρ . It inputs the *PP* ,*IK* and corresponding ciphertext *CT* . If the attribute does not satisfy the access policy, the algorithm outputs ⊥ . Otherwise, it outputs partially decrypted ciphertext *E* and sends it to *U*.

VI. CONCLUSION

In this article we proposed VMKS-ABE scheme. In our scheme, we combine the verifiable of the correctness of outsourced private key with multi-keyword search based on attribute encryption. In the general group model, the security of keyword index is proved. Under the random oracle model, the cipher text is proved to be selectively secure. As the security in the general group model is much weak than in the standard model, this is worth constructing verifiable and multi-keyword searchable scheme in the standard model.

Future extraction: Construction secure against an adaptive adversary stems from the difficulty of simulating in advance an index for the adversary that will be consistent with future unknown queries. The broadcast encryption scheme and the assumption that the server is honest-but-curious, is what

prevents users from performing successful searches once they are revoked. The formal treatment of the security of the multi-user scheme is enhanced for the future work.

REFERENCES

[1] K. Tuan Anh Nguyen, D. Dugki Min, J. Eunmi Choi, S. Todorovic, and A. Tran Duc Thang.(2019). “Reliability And Availability Evaluation For Cloud Data Center Networks Using Hierarchical Models” Computer. Netw., vol. 51, no. 18, pp.2891282.

[2] H. Junfeng Tian, J. C. S. Xuan Jing, and D. K. Yau.(2019). “A Lightweight Secure Auditing Scheme For Shared Data In Cloud Storage” in Proc. IEEE Int. Conf, pp. 2916889.

[3] Qiuxing Dong, Zhi Guan, and Zhong chen,``Attribute-based keyword search efficiency enhancement via an online/offline Approach," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130_2145, Jun. 2015. doi: 10.1109/JIOT.2018.2825289.

[4] Wenjun Luo, Jianming Tan,``Public key encryption with keyboard search based on factoring," *Comput. Netw.*, vol. 133, pp. 157_165, Mar. 2018. doi: 10.1016/j.comnet.2018.01.034.

[5] F. Kalyani Sonawane and C. Mitra Mandal.(2017,Oct) “Multi-Keyword Ranked Search Over Encrypted Cloud Data With Multiple Data Owners” in Proc. IJEDR, Volume 5, Issue 3, ISSN:2321-9939.

[6] Jeet Vyas, Prashant Modi. (2017, May). “Providing Confidentiality And Integrity On Data Stored In Cloud Storage By Hash And Meta Data Approach” in International Journal of Research Technology,Vol.4, Issue 5, ISSN:2394-2444.

[7] Jinli,Gian wang, Con Wang and Wenjing Lou, ``Fuzzy keyword search over encrypyed data in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 1187_1198, Apr. 2010doi: 10.1109/TPDS. 2014.2355202.

[8] J. Li, H. Wang, Y. Zhang, and J. Shen, ``Cipher text policy attribute-based encryption with hidden access policy and testing," *KSII Trans. Int. Inf. Syst.*, vol. 10, no. 7, pp. 3339_3352, Jul. 2016.

[9] R. Nitya Lakshmi, R. Lavanya, M. Meenakshi, and Dr.C. Suresh GanaDhas.(2015, Mar). “Analysis Of Attribute Based Encryption Schemes” in International Journal Of CSE, Vol.3 Issue 3, ISSN: 2347–8586.