A SECURED INFORMATION SHARING USING MULTI-OWNER KEYWORD SEARCH TECHNIQUE IN CLOUD ENVIRONEMENT

A. Chaitanya Sravanthi,

Assist. Prof., Department of MCA, QIS College of Engineering and Technology, Ongole,

K. Pavani,

Final Year Student of Master of Computer Applications, QIS College of Engineering and Technology, Ongole

Abstract**:** *In first, the greater parts of the current plans just think about the situation with the single information proprietor. Second, they need secure channels to ensure the safe transmission of mystery keys from the information proprietor to information clients. Third, in certain plans, the information proprietor ought to be online to help information clients when information clients mean to play out the hunt, which is badly arranged. Accessible encryption permits cloud clients to redistribute the enormous scrambled information to the remote cloud and to seek over the information without uncovering the touchy data. Numerous plans have been proposed to help the watchword look in an open cloud. In any case, they have some potential constraints. To empower clients to rapidly deal with the data of premiums from extensive scrambled information, accessible encryption has been proposed and enhanced by numerous plans. Rather than decoding the entire information, these plans enable clients to seek over the encoded information and just unscramble the comparing documents. Accessible encryption plans have been proposed to tackle the issues caused when the information proprietor imparts the information to different clients.*

Keywords**: *keyword search; cloud security; Secure channels; proxy re-encryption***

I. INTRODUCTION

The fast development of cloud clients has certified that distributed storage administrations are turning into the indistinguishable piece of individuals' life. Clients can appreciate an increasingly helpful and cost effective capacity condition than keeping up a nearby capacity framework. Regardless of the way that cloud capacity administrations give gigantic comfort to clients, information secrecy and security will be put in danger when clients re-appropriate the information to a remote cloud server. Normally, scrambling the information before redistributing is an answer for ensure information protection. In any case, this will make information usage, for example, catchphrase seek, a very testing errand [1].

To empower clients to rapidly deal with the data of interests from extensive encoded information, accessible encryption has been proposed also, improved by numerous plans [2-4] of unscrambling the entire information, these plans enable clients to seek over the scrambled information what's more, just unscramble the relating records. In this way, some after accessible encryption plans [5-9] have been proposed to take care of the issues caused when the information proprietor imparts the information to various clients. This situation, alluded to as multi-client setting, requires the information proprietor to designate the hunt capacity to information clients by means of secure channels. Other than that, these plans improve the functionalities of accessible encryption, such as fluffy watchword look [5], positioned catch phrases seek [6], multi-catchphrase looks [7], and so on. Moreover, a few plans [8, 9] improve the accessible encryption by joining two or more functionalities together. In any case, these plans share a few impediments.

To start with, a large portion of the current plans as it were think about the situation of a solitary information proprietor. As opposed to just a single information proprietor, generally cloud suppliers actually serve various information proprietors who can impart their information to one another. Since the information sharing is ending up progressively imperative on the client side, how to let information clients rapidly and safely discover the data of interests from numerous information proprietors' information turns into a test issue. Due to the monstrous transmissions of mystery keys, it is not sensible to straightforwardly expand the current plans from one information proprietor to numerous information

proprietors. Second, the information proprietor needs to set up a protected channel for every datum client, which is used to keep the transmitted mystery data from being uncovered. Since assets of the information proprietor are restricted, it is costly to build up a lot of secure channels if the number of information clients is substantial. A few plans [10-12] dependent on open key encryption have been proposed to expel secure channels from accessible encryption. Regardless of the expulsion of secure channels, these arrangements are still far from being conveyed in a genuine open cloud. In these plans, the information proprietor needs to encode every watchword for every client, which will significantly increment the assets utilization at the point when the quantity of information clients is expansive. Other than that, some current plans [13, 14] require the information proprietor to remain online to help information clients seek over the remote encoded information. It is exceptionally badly designed that information clients can't perform catchphrase seek in their time of necessities when the information proprietor is disconnected, even on the off chance that they have mystery keys or trapdoors [16]. Additionally, on the off chance that numerous information clients ask for the hunt at a similar time, the information proprietor will embrace substantial calculation and correspondence load. It is extremely unreasonable on the grounds that the assets of any client are considered as constrained in cloud. To take care of the previously mentioned issues, we propose a novel accessible plan which considers the situation in multi-proprietor [17]-[20], setting without secure channels. Every datum proprietor can appreciate sharing his own information and appointing the capacity of pursuit to information clients in the cloud without [18], sending mystery key to every datum client. Rather, the cryptographic crude called intermediary re-encryption is used to support information proprietors delegate the capacity of hunt to information clients by means of the cloud server, without uncovering any extra data. More than that, our plan is a non-intelligent catchphrase seeks arrangement [21], which implies that there is no communication between information proprietors and information clients. All the more exactly, in the entire procedure of our plan, every client just needs to convey with the cloud server. We abridge our fundamental commitments as pursues [22]. To start with, we think about the situation of various information proprietors and propose a novel plan to empower watchword look in a gathering. Each part in the gathering could be an information proprietor, just as an information client. In the interim, our plan underpins dynamic client change in gathering, counting client expansion and client denial. Second, our proposed plan does not depend on verifies channels. Neither mystery keys nor trapdoors will be transmitted in our plan. Also, our plan can even now ensure the secure watchword seek under shaky channels. Besides, our plan ends cooperations between information proprietors and information clients, which will significantly improve the client experience. Third, we assess the execution of our plan, which is recognized from the majority of the open key based catchphrase look plans.

II RELATED WORK

Since Song et al. [2] presented the first practical searchable encryption scheme, many follow-up schemes have been proposed in the literature [3, 4, 20-22]. This entire scheme only allows the data owner to search over the encrypted data, which are not inappropriate for data sharing services in the cloud. In light of this problem, some schemes [5-9, 19] have been proposed to support multi-user searchable encryption, implying that the data can also be searched by authorized users. To delegate the search ability, the data owner requires a secure channel to transmit some secret information, such as the secret key or the trapdoor, to each data user. Considering the cost of building the secure channels, Beak et al. [10] proposed the first scheme, referred to as secure channel free searchable encryption (SCFPEKS), aiming to remove the secure channels from searchable encryption. Rhee at al. [11] introduced an enhanced security model and constructed a scheme in this model. To improve the efficiency, Gu et al. [12] presented a novel SCF-PEKS scheme without pairing operation. If there are many data owners who are willing to share their data with each other, a new searchable encryption is required. For the solutions with secure channels [13], each data owner has to establish a secure channel with a data user, and transmits the secret information via the channel. It means that the both the computation overhead and communication overhead increase with the number of data owners. For the SCF-PEKS schemes, each data [14], owner has to encrypt each keyword for each data user. The computation overhead and storage overhead will increase not only with the number of data users, but also with the number of keywords. Therefore [15], it is significant to design a searchable encryption without secure channels in multi-owner setting.

EXISTING SYSTEM:

In existing system, most of the existing schemes only consider the scenario of a single data owner. Rather than only one data owner, most cloud providers in reality serve multiple data owners who are able to share their data with each other. Since the data sharing is becoming increasingly important on the user side, how to let data users quickly and securely find out the information of interests from multiple data owners' data becomes a challenge problem. Due to the massive transmissions of secret keys, it is not reasonable to directly extend the existing schemes from one data owner to multiple data owners.

Disadvantage

1. It is not efficient.
2. Shared data will not be secure.
3. Multi-owner sharing data in one user only.

III PROPOSED SYSTEM

In this paper, we propose a novel searchable scheme which supports the multi-owner keyword search without secure channels. More than that, our scheme is a non-interactive solution, in which all the users only need to communicate with the cloud server. Furthermore, the analysis proves that our scheme can guarantee the security even without secure channels. Unlike most existing public key encryption based searchable schemes, we evaluate the performance of our scheme, which shows that our scheme is practical. We provide secure and privacy-preserving access control to users, which guarantees any member in group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

Advantage

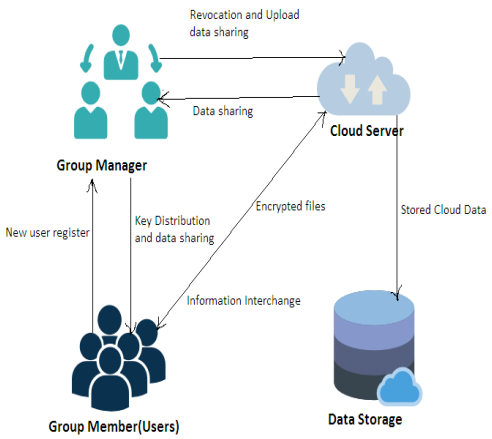
1. Decryption key should be sent via a secure channel and kept secret.
2. It is an efficient public –key encryption scheme which supports flexible delegation.

Table 1: Notations

Notation	Semantic
k_{UM}	the secret key of UM
e	the encryption key for record encryption
$qk_u, ComK_u$	user u's query key and her complementary key, respectively
U-ComK	a list of 2-tuples $(u, ComK_u)$ maintained by $Serv$

IV METHODOLOGY

Architecture:



Compoents:

Group Manager Module:

(a). In our scheme, we consider that the manager is an initiator who creates a group.

(b). the manager takes charge of the group management, including adding a new user and removing a revoked user.

(c). each user in the group is consideredas an authorized user, which means thatthe user simultaneously plays two roles: a dataowner and a data user. As a data owner, theuser can share his encrypted data with otherauthorized users in the group.

Group Member Module:

(a). As a data user, the user can search over the encrypted data of others in the group. After the manager permits a new user to join the group, the new user needs to upload the public key to the cloud server.

(b). Then the manager publishes a notification to the cloud server, which informs each authorized user to download the public key of the new user and generate a re-encryption key for the new user.

(c). After that, the new user can enjoy searching over the encrypted data of others in the group.

Cloud Module:

(a). The rapid growth of cloud users has affirmed that cloud storage services are becoming the inseparable part of people's life.

(b). Despite of the removal of secure channels, these solutions are still far from being deployed in a real public cloud. Most cloud providers in reality serve multiple data owners who are able to share their data with each other.

(c). the cryptographic primitive called proxy re-encryption is utilized to help data owners delegate the ability of search to data users via the cloud server, without revealing any additional information.

Admin Module:

(a). User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

Algorithm:

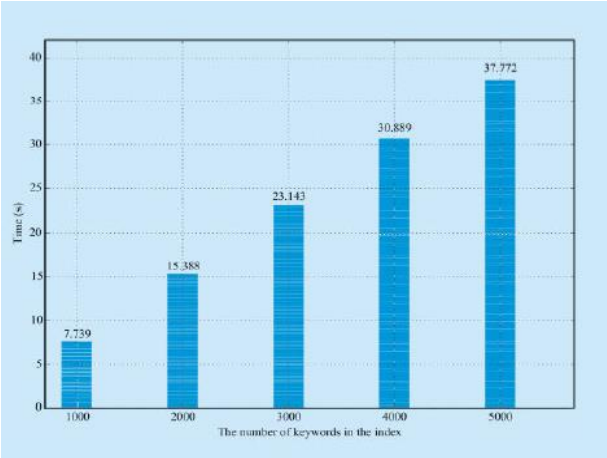
1. **SKE.Gen** ($1k$) $\rightarrow K$: Inputs a security parameter $1k$, the key generation algorithm **SKE.Gen** outputs a key K.

2. **SKE.Enc** (*K*, *m*) →*c*: Inputs a key *K* and a message *m*, theencryption algorithm **SKE.Enc** outputs a ciphertext.

SKE.Dec (*K*, *c*) →*m*: Inputs a key *K* and a ciphertext *c*, the decryption algorithm **SKE.Dec** outputs a message.

V ANALYSIS

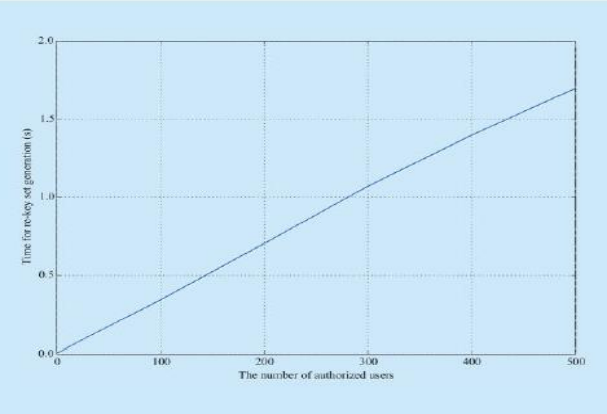
We compare our theme with Beak et al. [10] and Rhee et al. [11]. Assume that there is n licensed user United Nations agency will search over the file with m keywords. Noting that we have a tendency to solely consider one get in the comparison. Let E be one exponential operation, P be one pairing operation, be the length of the component in, and be the length of the component. As shown in Table two, the time complexness of the index generation is O(n) in our theme, which is O(m·n) in [10] and [11]. The extra storage within the comparison is that the size of both the index and also the re-encryption key set. In addition, we appraise our planned scheme employing a world dataset referred to as Enron Email Dataset [16]. The experiment is dead on a portable computer running Ubuntu Linux with 2.5 GHz Intel Core i5 processor and four G memory. 2 C languages based mostly supply libraries area unit wont to implement our scheme: Pairing-Based cryptographical (PBC) library [17] and OpenSSL library [18].



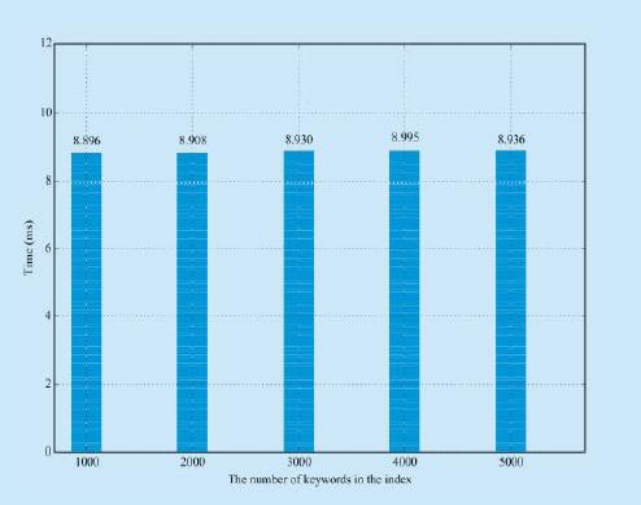
The average time for the tokens generation with the different number of keywords

in the index

To make the cryptographic setting, we have a tendency to adopt the sort A elliptic curve with 160-bit cluster, which can provide 1024-bit separate exponent security. All the communication prices aren't thought-about for the instant in our analysis. Except that the results of the index generation is that the average price of ten trials, others experimental results area unit the typical values generated from 100 trials. Re-encryption Key Computation: we have a tendency to first appraise the time consumption by the information owner to get the re-encryption key set, which is illustrated in Figure one. We assume that the information owner has already downloaded the public keys of licensed users from the cloud server.



The average time for generating the re-encryption key set with the different number of authorized users



The search efficiency with the different number of keywords in the index

VI RESULT

Searchable encryption schemes allow users to perform keyword based searches on an encrypted database. Almost all existing such schemes only consider the scenario where a single user acts as both the data owner and the querier. However, most databases in practice do not just serve one user; instead, they support search and write operations by multiple users. In this paper, we systematically study searchable encryption in a practical multi-user setting. Our results include a set of security notions for multi-user searchable encryption as well as a construction which is provably secure under the newly introduced security notions.

VII CONCLUSION

In this paper, we propose a novel public key based keyword search scheme, which supports multi-owner keyword search without secure channels. Moreover, our scheme supports non-interactivity, which means that each data owner and data user in the group can complete his individual tasks without interacting with each other. Instead, each of users in the group only needs to interact with the cloud server. Furthermore, although the removal of secure channels, our scheme can still guarantee the secure keyword search, which will not reveal any additional information to the cloud server nor the eavesdropper. Finally, the experimental results demonstrate that our scheme is an efficient public key based solution.

VIII REFERENCES

[1] W.H Sun, W.J Lou, Y.T Hou, and H Li, "Privacy-preserving keyword search over encrypted data in cloud computing," in Secure Cloud Computing. Springer, 2014, pp. 189–212.

[2] D.X Song, D Wagner, and A Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[3] D Boneh, C.G DI, R Ostrovksy, and G Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.

[4] R Curtmola, J Garay, S Kamara, and R Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[5] J Li, Q Wang, C Wang, N Cao, K Ren, and W.J Lou, "Fuzzy keyword search over encrypted data in cloud computing." in Computer Communications (INFOCOM), IEEE, 2010, pp. 1-5.

[6] C Wang, N Cao, J Li, K Ren, and W.J Lou, "Secure ranked keyword search over encrypted cloud data," in IEEE 30th International Conference on Distributed Computing Systems (ICDCS), 2010, pp. 253–262.

[7] M Li, S.C Yu, N Cao, and W.J Lou, "Authorized private keyword search over encrypted data in cloud computing," in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 383–392.

[8] N Cao, C Wang, M Li, K Ren, and W.J Lou, "Privacy preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[9] W.H Sun, B. Wang, N Cao, M Li, W.J Lou, Y.T Hou, and H Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 2013, pp. 71–82.

[10] J Baek, R Safavi-Naini, and W Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications–ICCSA 2008. Springer, 2008, pp. 1249–1259.

[11] H.S Rhee, J.H Park, W Susilo, and D.H Lee, "Improved searchable public key encryption with designated tester," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009, pp. 376–379.

[12] C.X Gu, Y.F Zhu, and H Pan, "Efficient public key encryption with keyword search schemes from pairings," in Information security and cryptology. Springer, 2008, pp. 372–383.

[13] W.H Sun, X.F Liu, W.J Lou, Y.T Hou, and H Li, "Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data," in IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2110–2118.

[14] B Wang, W Song, W.J Lou, and Y.T Hou, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," in IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2092–2100.

[15] F Bao, R.H Deng, H.F Zhu, "Variations of diffie-hellman problem," in Information and Communications Security. Springer, 2003, pp. 301–312.

[16] "Enron Email Dataset," https://www.cs.cmu.edu/~./enron/.

[17] "Pairing-based Cryptographic Library," https://crypto.stanford.edu/pbc/.

[18] "OpenSSL," https://www.openssl.org/.

[19] B Wang, S Yu, W.J Lou, Y.T Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud." In INFOCOM, 2014 Proceedings, 2014, pp. 2112-2120.

[20] E.J Goh. "Secure Indexes." IACR Cryptology ePrint Archive, pp. 216, 2003.

[21] P Golle, J Staddon, and B Waters. "Secure conjunctive keyword search over encrypted data." In Applied Cryptography and Network Security, 2004, pp. 31-45.

[22] S Kamara, C Papamanthou, and T Roeder, "Dynamic searchable symmetric encryption." In Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp. 965-976.

Authors Profile

Ms. **A. Chaitanya Sravanthi** is currently working as an Assistant Professor in Department of Master of Computer Applications in QIS College of Engineering & Technology with the Qualification MCA.

Ms. **K. Pavani** pursuing MCA 3rd year in Qis College and Engineering and Technology in Department of Master of Computer Applications, Ongole.