International Journal of Research
Available at https://edupediapublications.org/journal
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Data sharing between different users by using Single key by Searchable encryption

Aenugu Hareesha[1],Ch. SeshaGopalarao[2]

[1]M. Tech Dept.:-CNIS, GNarayanamma institute of technology and science Shaikpet,hyd

Mail ID: -hareeshaanugu@gmail.com

[2]ProfessorDept.:-IT,GNarayanamma institute of technology and science Shaikpet,hyd

Mail ID: - seshagopalaraoch@yahoo.co.in

Abstract:

The ability of specifically offering scrambled information to diverse clients by means of open distributed storage might extraordinarily ease security worries over unintentional information spills in the cloud. A key test to planning such encryption plans lies in the productive administration of encryption keys. The wanted adaptability of imparting any gathering of chose reports to any gathering of client's requests diverse encryption keys to be utilized for distinctive archives. On the other hand, this additionally infers the need of safely conveying to clients an extensive number of keys for both encryption and seeks, and those clients will need to safely store the got keys, and present a just as substantial number of catchphrase trapdoors to the cloud to perform look over the common information. The inferred requirement for secure correspondence, stockpiling, and multifaceted nature unmistakably renders the methodology unfeasible. In this paper, we address this down to earth issue, which is generally disregarded in the writing, by proposing the novel idea of Single-Key Explore encryption and instantiating the idea through a solid SKEE plan, in which an information proprietor just needs to disseminate a solitary key to a client for sharing countless, and the client just needs to present a solitary trapdoor to the cloud for questioning the mutual reports. The security examination and execution assessment both affirm that our proposed plans are provably secure and for all intents and purposes productive.

Keywords: -cloud storage, Searchable encryption, data sharing & privacy, Single Key

1. INTRODUCTION:

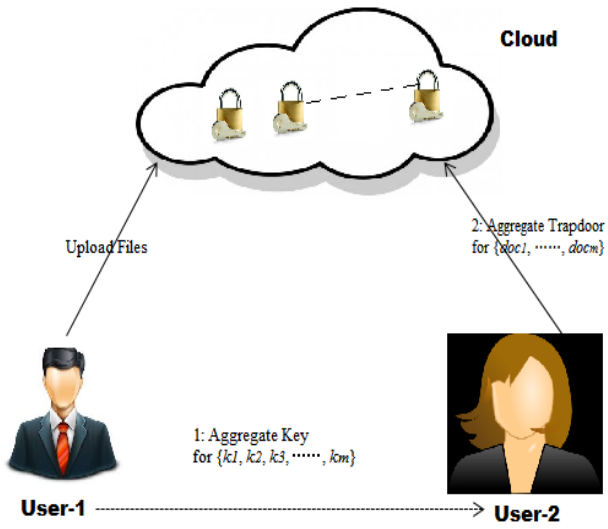
Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos

and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization. However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud). To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such a cloud storage is often called the cryptographic cloud storage. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable encryption (SE) scheme in which the data owner is required to encrypt potential keywords and upload them to thecloud together with encrypted data, such that, for retrieving data matching a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search over the encrypted data.

Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, implementing such a system for large scale applications involving millions of users and billions of files may still be hindered by practical issues involving the efficient management of encryption keys, which, to the best of our knowledge, are largely ignored in the literature. First of all, the need for selectively sharing encrypted data with different users (e.g., sharing a photo with certain friends in a social network application, or sharing a business document with certain colleagues on a cloud drive) usually demands different encryption keys to beused for different files. However, this implies the in this paper, we address this challenge by proposing the novel concept of key aggregate searchable encryption (KASE), and instantiating the concept through concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the

former. To support searchable group data sharing the main requirementsfor efficient key management is twofold.

2. SYSTEM ARCHITECTURE



We first define a general framework of key aggregatesearchable encryption (KASE) composedof seven polynomial algorithms for security parameter setup, key generation, encryption,key extraction, trapdoor generation, trapdooradjustment, and trapdoor testing. We thendescribe both functional and security requirementsfor designing a valid KASE scheme.After providingdetailed constructions for the seven algorithms,we analyze the efficiency of the scheme,and establish its security through detailed analysis.

We discuss various practical issues in buildingan actual group data sharing system based onthe proposed KASE scheme, and evaluate itsperformance. The evaluation confirms our systemcan meet the performance requirements ofpractical applications.The rest of the paper is organized as follows. We then define the general KASE framework in SectionWe describe related work in SectionWenumber of keys that need to be distributed to users, must not only be distributed to users via securechannels, but also be securely stored and managed by the users in their devices. In addition, a largenumber of trapdoors must be generated by usersand submitted to the cloud in order to perform akeyword search over many files. The implied need forsecure communication, storage, and computationalcomplexity may render such a system inefficient andimpractical. Both for them to search over the encrypted filesand to decrypt the files, will be proportional to thenumber of such files. Such a large number of keys design a concrete KASE scheme and analyze its efficiencyand security in SectionWe implement andevaluate a KASE-based group data sharing system in Section.

3. RELATED WORK

Existing System

Consider a scenario where two employees of a company would like to share some confidential business data using a public cloud storage service (e.g., dropbox or syncplicity). For

instance, Alice wants to upload a large collection of financial documents to the cloud storage, which are meant for the directors of different departments to review. Suppose those documents contain highly sensitive information that should only be accessed by authorized users, and Bob is one of the directors and is thus authorized to view documents related to his department. Due to concerns about potential data leakage in the cloud, Alice encrypts these documents with different keys,and generates keyword ciphertexts based on department names, before uploading to the cloud storage.Alice then uploads and shares those documents with the directors using the sharing functionality of the cloud storage. In order for Bob to view the documents related to his department, Alice must delegate to Bob the rights both for keyword search over those documents, and for decryption of documents related to Bob's department. With a traditional approach, Alice must securely send all the searchable encryption keys to Bob. After receiving these keys, Bob must store them securely, and then he must generate all the keyword trapdoors using these keys in order to perform a keyword search. Alice is assumed to have a private document set {doci}n i=1, and for eachdocumentdoci, a searchable encryption key kiisused.Without loss of generality, we suppose Alice wants to share documents {doci}m i=1 with Bob. In this case,Alice must send all the searchable encryption keys{ki}m i=1 to Bob. Then, when Bob wants to retrievedocuments containing a keyword w, he must generatekeyword trapdoor Tri for each document dociwithkeykiand submit all the trapdoors {Tri}m i=1 to thecloud server. When m is sufficiently large, the key distribution and storage as well as the trapdoor generation may become too expensive for Bob's client-side device, which basically defies the purpose of using cloud storage.

Proposed System:

In this paper, we address this challenge by proposing the novel concept of key-aggregate searchable encryption (KASE), and instantiating the concept through a concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former.

To support searchable group data sharing the main requirements for efficient key management are twofold. First, a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing

any number of files. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files. We first define a general framework of key aggregate searchable encryption (KASE) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. We then describe both functional and security requirements for designing a valid KASE scheme.We then instantiate the KASE framework by designing a concrete KASE scheme. After providing detailed constructions for the seven algorithms, we analyze the efficiency of the scheme, and establish its security through detailed analysis. We discuss various practical issues in building an actual group data sharing system based on the proposed KASE scheme, and evaluate its performance. The evaluation confirms our system can meet the performance requirements of practical applications.

Advantages of proposed system:

- ❖ It is more secure.
- ❖ Decryption key should be sent via a secure channel and kept secret.
- ❖ It is an efficient public-key encryption scheme which supports flexible delegation.
- ❖ To the best of our knowledge, the KASE scheme proposed in this paper is the first known scheme that can satisfy requirements.

4. Implementation

1. Searchable Encryption

2. Data Group Sharing

Searchable Encryption:

Setup: This algorithm is run by the owner set up the scheme. It takes as input a security parameter 1 , and outputs the necessary keys.

Encrypt (k; m): This algorithm is run by the owner to encrypt the data and generate its keyword cipher texts. It takes as input the data m, owner necessary keys including searchable encryption key k and data encryption key, outputs data cipher text and keyword cipher texts Cm.

Trpdr(k; w): This algorithm is run by a user generate a trapdoor Tr for a keyword w using key k.

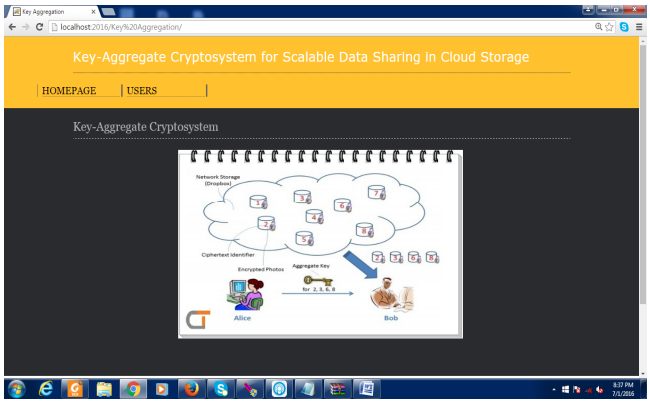
Test (Tr, C): this algorithm is run by the cloud server to perform a keyword search over encrypted data. It takes as input trapdoor Tr and the keyword cipher textsCm .Outputs whether Cm contains thespecified keyword.

Data Group Sharing:

In which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents.

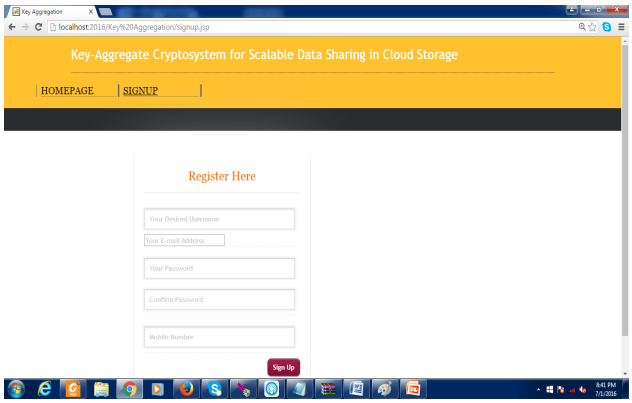
5. EXPERIMENTAL RESULTS

Home page:



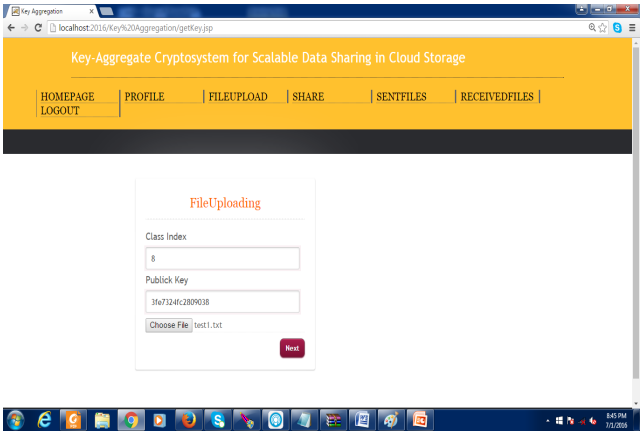
This screen is illustrating the home page of the application. And also this having links of User and Cloud Login Pages and Contact Page.All the Actors having login page links from this home page only.Another more thing is it also shows to us Architecture Diagram of the Application.

Registration Page:



This screen is illustrating the User Registration page of the application. And also this having fields all user required fields.A New user needs to fill this form for login credentials before entering into application.After successfully registering the user all fields values will be stored into specified database.

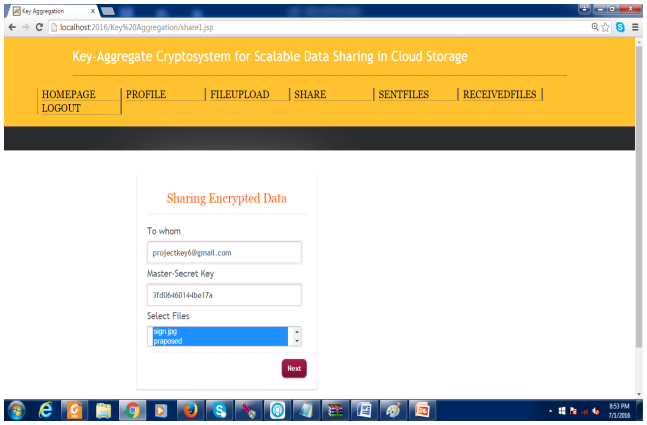
User File Upload Page:



Description:

User uploading a file to cloud having the fields of File Id and File Name and File Data.File Id Automatically taken by database it will having hidden on this page.For Browse File /Select file from system user click choose file ButtonAfter Press “Continue” Button.File will be uploaded along with file data.

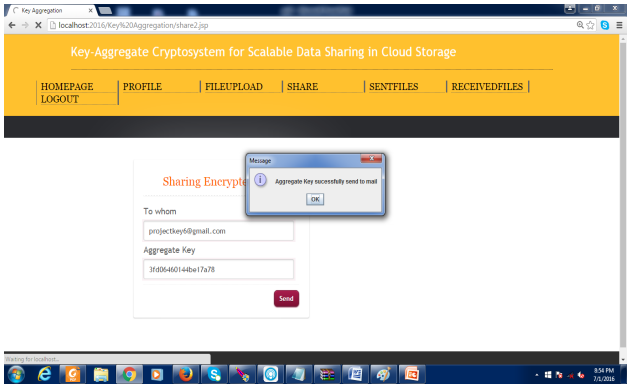
Before upload File with Keyword Ciphertext Page:



Description:

File will uploaded along with encrypted format of the system.And also ciphertexts of the file will also having file encrypted format of the application.Except file name file data and keyword ciphertexts all having encrypted format for security purpose.Finally having Upload button to upload file.

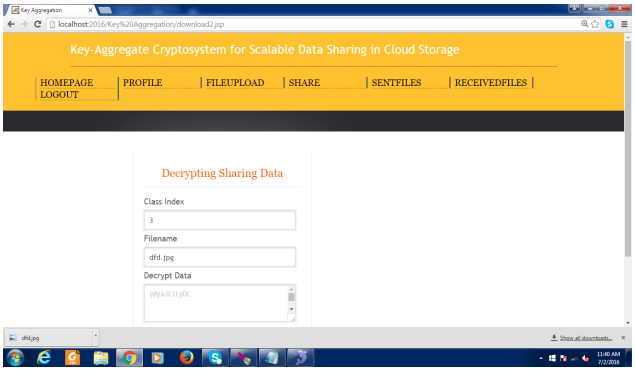
Data Sharing Page:



Description:

The Above screen describes user sharing the file from user to user of the application.

Data Share with Master Key:



Description:

After Selecting to User from user will generate "Master Key".After Master key successfully generated select multiple files from the cloud to share.After click on "GetAggreagateKey" button.

6. CONCLUSION:

Considering the practical problem of privacypreserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of key aggregate searchable encryption (KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage. In a KASE scheme, the owner only needs to distribute a single key to a user when sharing lots of documents with the user, and the user only needs to submit a single trapdoor when he

queries over all documents shared by the same owner. However,if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multi-owners setting is a future work. Moreover, federated clouds have attracted a lot of attention nowadays, but our KASE cannot be applied in this case directly. It is also a future work to provide the solution for KASE in the case of federated clouds.

7. REFFERENCESS:

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing",Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance:The Essential of Bread and Butter of Data Forensics in CloudComputing", Proc. ACM Symp. Information, Computer and Comm.
Security, pp. 282-292, 2010.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiownerdata sharing for dynamic groups in the cloud", IEEETransactions on Parallel and Distributed Systems, 2013, 24(6): 1182-
1191.

[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystemfor Scalable Data Sharing in Cloud Storage", IEEE Transactionson Parallel and Distributed Systems, 2014, 25(2): 468-477.

[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searcheson encrypted data", IEEE Symposium on Security and Privacy,IEEE Press, pp. 44C55, 2000.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchablesymmetric encryption: improved definitions and efficient constructions",In: Proceedings of the 13th ACM conference on Computer
and Communications Security, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen."Computationally efficientsearchable symmetric encryption", Secure Data Management, pp.87-100, 2010.

[8] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchablesymmetric encryption", Proceedings of the 2012 ACM conferenceon Computer and communications security (CCS), ACM, pp. 965-976, 2012.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryptionwith Keyword Search", EUROCRYPT 2004, pp. 506C522,2004.

[10] Y. Hwang, P. Lee. "Public Key Encryption with ConjunctiveKeyword Search and Its

Extension to a Multi-user System", In:Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

[11] J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypteddata in cloud computing", Proc. IEEE INFOCOM, pp. 1-5,2010.

[12] C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard searchover encrypted data", Secure Data Management. LNCS, pp. 114-127, 2011.

[13] C. Dong, G. Russello, N. Dulay."Shared and searchable encrypteddata for untrusted servers", Journal of Computer Security,pp. 367-397, 2011.

[14] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword SearchScheme for Secure Data Sharing with Fine-Grained AccessControl. Information Security and Cryptology, LNCS, pp. 406-418,2012.

[15] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine Grained Access Control in HybridCloud", In: Network and System Security 2012, LNCS, pp. 490-
502, 2012.