

Reducing Key Space Using KASE and Searching Multi Keyword for Multiple Data Owners in Cloud Computing

M. Gowthami*, T. Praveen, V.S. Vinitha, G. Nandhini

Department of Computer Science and Engineering Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Tamilnadu

*Corresponding author: E-Mail: gowthamimailme@gmail.com

ABSTRACT

The encrypted data for selectively sharing to a multiple user by the public cloud storage may concerns over unintended data leaks in the cloud .when sharing selected group of documents to multiple users demands random encryption keys for those group of documents. However it is used to distribute large number of key for both encryption and search .Then the user should store the received key and submit keyword trapdoor to cloud for performing shared data .We propose a new concept of KASE(key Aggregate Searchable Encryption).In which the data owner needs to distribute a single key for sharing group of documents to a user .Then the single trapdoor will submit by the user to the cloud for query the shared document .From our proposed scheme it is provably secure and practically efficient.

KEY WORDS: KASE, Trapdoor, Data User, Data Owner, Encryption Key, Keyword.

1. INTRODUCTION

Distributed storage has developed as a promising lot of information shared over the Internet. Today a substantial number of customers are sharing individual data, for instance, photos and recordings, with their associates through interpersonal association applications in light of appropriated stockpiling each day. Business clients are likewise being pulled in by distributed storage because of its various advantages, including lower cost, more prominent dexterity, and better asset usage.

Nonetheless, while getting a charge out of the accommodation of sharing information by means of distributed storage, clients are likewise progressively worried about incidental information spills in the cloud. Such information spills, brought on by a vindictive enemy or a getting into mischief cloud administrator, can more often than not prompt to genuine ruptures of individual protection or business mysteries (e.g., the current prominent occurrence of superstar photographs being spilled in iCloud). Such conveyed stockpiling is consistently called the cryptographic disseminated stockpiling. In any case, the encryption of data makes it striving for customers to interest and a short time later particularly recoup only the data containing given watchwords.

A regular course of action is to use a searchable encryption (SE) scheme in which the data proprietor is required to encode potential watchwords and exchange them to the cloud together with mixed data, to such a degree, to the point that, for recouping data planning a catchphrase, the customer will send the relating watchword trapdoor to the cloud for performing look for over the encoded data.

2. RELATED WORK

Searchable encryption: The soonest endeavour of searchable encryption was made by Tune et al. In, they propose to scramble every word in a record freely and permit the server to discover whether a solitary questioned watchword is contained in the document without knowing the correct word. This proposition is a greater amount of theoretic interests in light of high computational expenses. Goh propose building a watchword list for every record and utilizing Bloom channel to quicken the pursuit. Curtmola (2006), propose building records for every watchword, and utilize hash tables as an option way to deal with searchable encryption.

The primary open key plan for watchword seek over scrambled information is displayed in. The creators and further advance the look functionalities of searchable encryption by proposing plans for conjunctive watchword look. The searchable encryption thinks for the most part about single watchword look or Boolean watchword seek. Expanding these systems for positioned multi-catchphrase hunt will bring about substantial calculation and capacity costs.

Secure Keyword Search in Cloud Computing: The protection worries in distributed computing spur the contemplate on secure watchword look. Wang (2013), initially characterized what's more, understood the safe positioned watchword seek over encoded cloud information and they proposed aconspire that profits the top-k pertinent records upon a solitary catchphrase seek. Their methodologies vectorize the rundown of catchphrases what's more, apply grid augmentations to conceal the real catchphrase data from the cloud server, while as yet permitting the server to discover the top-k applicable information documents.

Multi-watchword positioned question on scrambled information (MKQE) that empowers a dynamic watchword word reference and stays away from the positioning request being mutilated by a few high recurrence watchwords. Wang (2013), Proposed fluffy watchword look over encoded cloud information going for resistance of both minor grammatical mistakes and organization irregularities for clients' seek input. Additionally proposed

privacy assured comparability seek instruments over outsourced cloud information. In, we proposed a protected, productive, and conveyed catchphrase seek convention in the geo-conveyed cloud environment.

Order Preserving Encryption: The request saving encryption is utilized to keep the cloud server from knowing the correct pertinence scores of watchwords to an information document. The early work of Agrawal et al. proposed a request saving symmetric encryption (OPE) conspire where the numerical request of plain messages are safeguarded.

A perfect secure request protecting encryption plot. Kerschbaum what's more, Schroepfer further proposed a plan which is thought secure as well as an effective arrange saving encryption conspire. Be that as it may, these plans are not added substance arrange saving. As a reciprocal work to the past request saving work, we propose another added substance request and security safeguarding capacities. Information proprietors can uninhibitedly pick any capacity from an AOPPF family to encode their importance scores. The cloud server registers the whole of encoded pertinence scores and positions them in light of the whole.

System Architecture: In this system architecture diagram the data user will register into the database. Then only user can login to that site and authorization will be done. The data owner upload the files into cloud and it will be encrypted format and generates a private key stored in cloud securely. The data owner share the large number of files to the multiple users. After that the data owner send that private key to the user, then only the entire file will be converted into decrypted format. Finally the user will download that file. This process will share the files to multiple users securely.

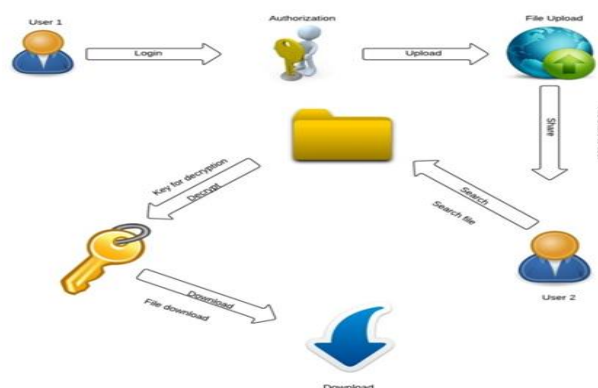


Figure.1. System architecture

Implementation: In this project we identified our project as four modules which is listed below

- Authentication and Authorization.
- File upload and download.
- File sharing.
- Key generation

Authentication and Authorization: In this module the User need to enroll to start with, then just he/she needs to get to the information base. After enlistment the client can login to the site. The approval and validation prepare encourages the framework to secure itself what's more it shields the entire component from unapproved usage .The Registration includes in getting the points of interest of the clients who needs to utilize this application.

File upload and download: Document transfer to cloud after encryption handle. The client can download the record by decoding key. While transferring to the Cloud the record got scrambled by utilizing AES (Advanced Encryption Standard) Algorithm and creates Private key. Again the Encrypted Data is converted as Binary Data for Data security and Stored in Cloud.

File Sharing: In this module, the transferred documents are shared to the companions or clients. In this, the Data Owner set an ideal opportunity to lapse the information in Cloud. The Private key of the Shared Data will be send through Email.

Key generation: In this module the key will be create haphazardly and send to the client for document decoding. The key will be produced while sharing the record to client.

3. EXPERIMENTAL RESULT



Figure.2. Home Page

The home page contains register, admin and login. With the help of home page the user entered to the database.

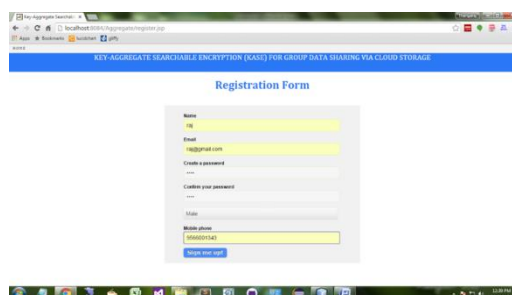
A screenshot of a web browser displaying a registration form. The form is titled "Registration Form" and includes fields for Name, Email, Create password, Confirm your password, and Mobile phone. A "Sign Up" button is at the bottom.

Figure.3. Registration

Initially the user register their details in the registration form for who are involved in this site.

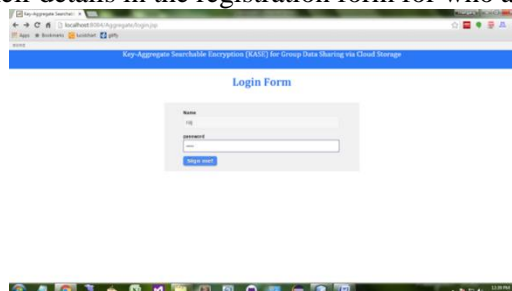
A screenshot of a web browser displaying a login form. The form is titled "Login Form" and includes fields for Name and password. A "Sign In" button is at the bottom.

Figure.4. Login

After registration the data owner verify whether the authorized person is involved in this site then only the user can login to that site.

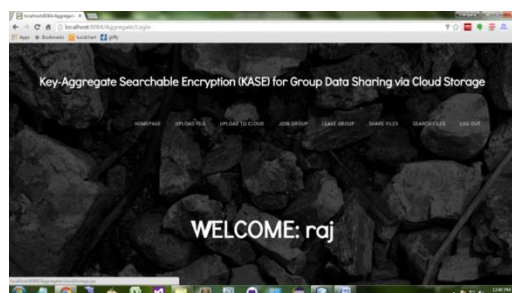


Figure.5. User home

Here the user home page will be displayed after login to that site.



Figure.6. Upload file

The data owner upload the files for sharing those files to multiple users securely.



Figure.7. File upload to cloud

The files uploaded to the cloud and it will be in encrypted format for protect the files from unauthorized users. Then private key will generate, stored in cloud.

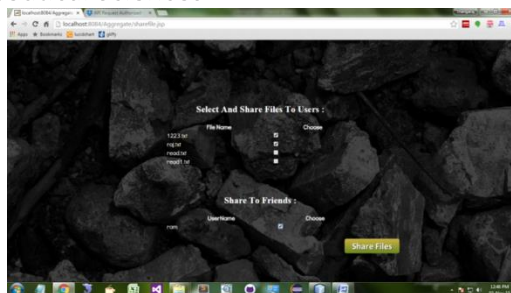


Figure.8. Share files

After uploading the files to cloud, data owner share files to multiple users using share files option. These multiple users selectively selected by the data owner.



Figure.9. Search file

While sharing the files, data owner wants to know the exact file name then can search that file by trapdoor technique.

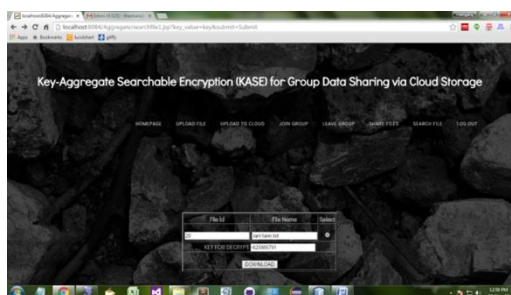


Figure.10. File Download

Here the data owner send the private key to the user through email. This key is used to decrypt entire file, then the user can download that file.

4. CONCLUSION

Considering the practical issue of security ensuring data sharing system in perspective of open disseminated stockpiling which requires a data proprietor to course a generous number of keys to customers to enable them to get to his/her reports, we curiously propose key-add up to searchable encryption (KASE) and fabricate a strong KASE plot. Both examination and appraisal happens assert that our work can give a capable response for working sensible data sharing system in perspective of open dispersed stockpiling. In a KASE plot, the proprietor simply needs to scatter a single key to a customer when offering clusters of records to the customer, and the customer simply needs to exhibit a lone trapdoor when he inquiries over all chronicles shared by a comparative proprietor. In any case, if a customer needs to address over files shared by various proprietors, he ought to deliver distinctive trapdoors to the cloud. Well ordered guidelines to diminish the amount of trapdoors under multi-prorietors setting is a future work. Furthermore, bound together fogs have pulled in an extensive measure of thought nowadays, however our KASE can't be associated fogs for this circumstance particularly. It is also a future work to give the response for KASE by virtue of consolidated fogs.

REFERENCES

- Boneh D, Di Crescenzo G, Ostrovsky R and Persiano G, Public key encryption key word with search, in Advances in Cryptology- Eurocrypt 2004, Springer, 2004, 506–522.
- Bosch C, Brinkma R, Hartel OP, Conjunctive wildcard search over encrypted data, Secure Data Management. LNCS, 2011, 114-127.
- Chen X.F, Li J, Huang X.Y, Li J.W, Xiang Y, Secure Outsourced Attribute-based Signatures, IEEE Trans. on Parallel and Distributed Systems, 2013.

Chu C, Chow S, Tzeng W, Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage, IEEE Transactions on Parallel and Distributed Systems, 25 (2), 2014, 468-477.

Cloud, In: Network and System Security 2012, LNCS, 2012, 490- 502.

Computing, Proc. ACM Symp. Information, Computer and Comm. Security, 2010, 282-292.

Curtmola R, Garay J, Kamara S and Ostrovsky R, Searchable symmetric encryption, Improved definitions and efficient constructions, in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, 79–88.

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

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

Dong C, Russello G, Dulay N, Shared and searchable encrypted data for untrusted servers, Journal of Computer Security, 2011, 367-397.

Hwang Y, Lee P, Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System, In: Pairing-Based Cryptography C Pairing 2007, LNCS, 2007, 2-22.

Kamara S, Papamanthou C, Roeder T, Dynamic searchable symmetric encryption, Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, 2012, 965- 976.

Li J, Kim K, Hidden attribute-based signatures without anonymity revocation, Information Sciences, Elsevier, 180 (9), 2010, 1681-1689.

Li J, Wang Q, Wang C, Fuzzy keyword search over encrypted data in cloud computing, Proc. IEEE Infocom, 2010, 1-5.

Liu X, Zhang Y, Wang B and Yan J, Mona, secure multi owner data sharing for dynamic groups in the cloud, IEEE Transactions on Parallel and Distributed Systems, 24 (6), 2013, 1182- 1191.

Lu R, Lin X, Liang X and Shen X, Secure Provenance, the Essential of Bread and Butter of Data Forensics in Cloud
Song X, Wagner D, Perrig A, Practical techniques for searches on encrypted data, IEEE Symposium on Security and Privacy, IEEE Press, 2000, 44-55.

Van P, Sedghi S, Doumen JM, Computationally efficient searchable symmetric encryption, Secure Data Management, 2010, 87-100.

Wang C, Chow S.S, Wang Q, Ren K and Lou W, Privacy-preserving public auditing for secure cloud storage, IEEE Trans. Comput, 62 (2), 2013, 362–375.

Wei Zhang, Yaping Lin, Sheng Xiao, JIE Wu, and Siwang Zhou, Privacy Preserving Ranked Multi keyword Search for Multiple Data Owner In Cloud Computing, IEEE Trans. Comput, 65 (5), 2016.

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

Zhao F, Nishide T, Sakurai K, Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control, Information Security and Cryptology, LNCS, 2012, 406-418.