IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Key Aggregate Searchable Encryption for Group Data Sharing along with Duplication Detection on Cloud

Soniya L. Barkade[1], Nagaraju Bogiri[2]

Student, Computer Dept., KJCOEMR, Pune, India[1]

Professor, Computer Dept., KJCOEMR, Pune, India[2]

Abstract: Data sharing is an critical functionality in cloud garage. In this article, we display a way to securely, efficiently, and flexibly share information with others in cloud garage. We describe new public-key cryptosystems which produce steady-size ciphertexts such that green delegation of decryption rights for any set of ciphertexts are possible. The novelty is that possible aggregate any set of secret keys and lead them to as compact as a single key, however encompassing the electricity of all of the keys being aggregated. In other phrases, the secret key holder can launch a constant-size mixture key for flexible alternatives of ciphertext set in cloud storage; however the different encrypted files outside the set stay private. This compact mixture key can be conveniently despatched to others or be saved in a clever card with very limited comfortable storage. We offer formal security evaluation of our schemes inside the trendy version. We additionally describe other utility of our schemes. In precise, our schemes provide the first public-key patient-controlled encryption for bendy hierarchy, which turned into but to be acknowledged.

Keywords: Searchable Encryption, Data Sharing, Cloud Storage, Data Privacy.

I. INTRODUCTION

Cloud storage has emerged as a promising solution for imparting ubiquitous, handy, and on-call for accesses to massive amounts of facts shared over the Internet. Today, hundreds of thousands of customers are sharing personal information, along with pix and films, with their buddies thru social community packages based totally on cloud storage on a every day foundation. Business users also are being attracted by way of cloud storage due to its numerous benefits, including decrease price, more agility, and higher resource utilization.

Although combining a searchable encryption scheme with cryptographic cloud garage can achieve the fundamental protection requirements of a cloud storage, imposing the sort of device for massive scale applications involving hundreds of thousands of customers and billions of files may also nevertheless be hindered by means of practical problems involving the efficient management of encryption keys, which, to the great of our know-how, are in large part omitted inside the literature.

First of all, the want for selectively sharing encrypted facts with one-of-a-kind customers (e.g., sharing a photo with sure pals in a social community utility, or sharing a enterprise report with sure colleagues on a cloud power) generally demands exclusive encryption keys to be used for distinctive files. However, this means the range of keys that need to be dispensed to users, both for them to go looking over the encrypted documents and to decrypt the documents, could be proportional to the quantity of such documents. Such a big number of keys.

II. LITERATURE SURVEY

- Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing.

Cloud computing is develop computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As to assure as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource annoyed data for sharing on cloud servers, which are not within the same trusted influence, as data owners.

To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by to cause to appear data decryption keys only to authorized users. The problem of simultaneously accomplish fine grained access, scalability, and data confidentiality of access control actually still remains not resolved.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

- Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing.

Success of data forensics in cloud computing is based on secure place that records ownership and process history of data objects. But it is the still challenging issue in this paper. In this paper, they proposed a new secure provenance scheme based on the bilinear pairing techniques .As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud. Secure authentication on user access, and place tracking on disputed documents is provided in this paper. With the provable security techniques, this paper formally demonstrates the proposed scheme is secure in the standard model.

- Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud.

In this paper character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Due to the frequent change of membership sharing data in multi-owner manner while preserving data and identify privacy from untrusted cloud is still a challenging issue.

III. EXISTING SYSTEM

There may be a wealthy literature on searchable encoding, together with sou'-sou'-east schemes and PEKS schemes. In difference to the ones current paintings, in the context of cloud storage, keyword seek underneath the multi-tenancy putting may be a additional not unusual scenario. In one of these state of affairs, the data proprietor would really like to percentage a document with a gaggle of licensed customers, and every user World Health Organization has the access right will provide a trapdoor to perform the keyword search over the shared file, namely, the "multi-person searchable encryption" (MUSE) situation.

Some recent paintings attention to one of these MUSE situation, even though all of them adopt unmarried-key combined with get right of entry to management to realize the intention. In MUSE schemes square measure made by means of sharing the file's searchable encoding key with all users World Health Organization will get entry to it, and broadcast encoding is employed to realise coarse-grained access management. In characteristic based totally encoding (ABE) is implemented to recognize fine-grained get entry to control aware key-word search.

IV. PROPOSED SYSTEM

In this paper, we will be inclined to address this venture by using providing the radical concept of key-mixture searchable encoding (KASE), and instantiating the concept via a concrete KASE theme.

The planned KASE subject matter applies to any cloud garage that supports the searchable cluster understanding sharing practicality, which indicates any consumer might with the aid of selection proportion a group of distinctive documents with a group of certain customers, whereas allowing the latter to perform key-word seek over the previous.
To aid searchable cluster know-how sharing the maximum needs for not pricey key management a twofold. First, an information owner entirely has to distribute one combination key (in place of a gaggle of keys) to a user for sharing any range of documents. Second, the person solely has to put up one aggregate to the cloud for activity key-word seek over any variety of shared documents.

We initial define a fashionable framework of key mixture searchable encoding (KASE) composed of 7 polynomial algorithms for protection parameter setup, key generation, encryption, key extraction. We will be predisposed to then describe each useful and protection needs for making plans a legitimate KASE subject.

We then instantiate the KASE framework by way of planning a concrete KASE subject. When imparting elaborated constructions for the seven algorithms, we will be inclined to investigate the efficiency of the theme, and set up its protection via elaborated analysis. We speak varied sensible problems in constructing partner actual cluster knowledge sharing machine supported the deliberate KASE subject, and degree its performance. The analysis confirms our device will meet the performance wishes of realistic packages.

V. IMPLEMENTATION

Data owner and user will be provided with registration and login. User will fill all details in registration form. User will get login credentials. Data owner can view all coming request from user. User will enter group name and public key as shown in fig. 1

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

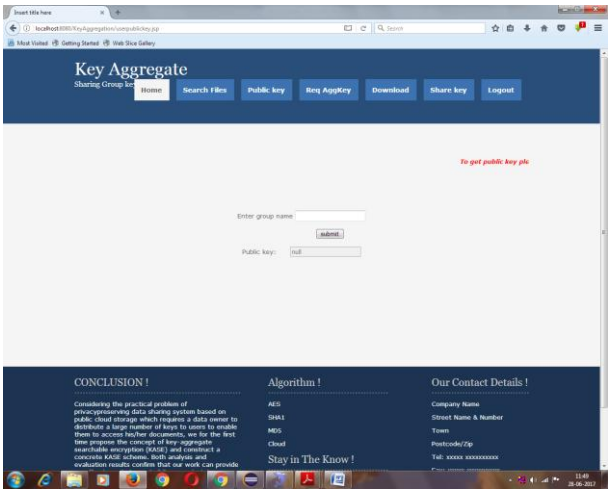


Fig. 1

Further, user will enter file name which to be encrypt, keyword and email_id. It is shown in fig. 2

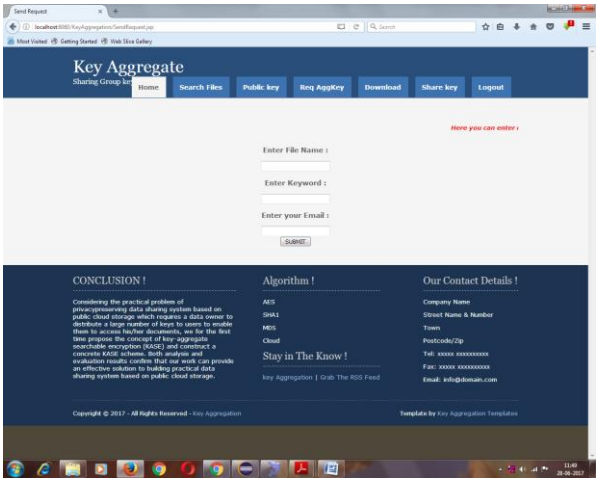


Fig.2

For decrypting file, data owner will send aggregate key to user via mail. User will receive key through mail as shown in fig. 3

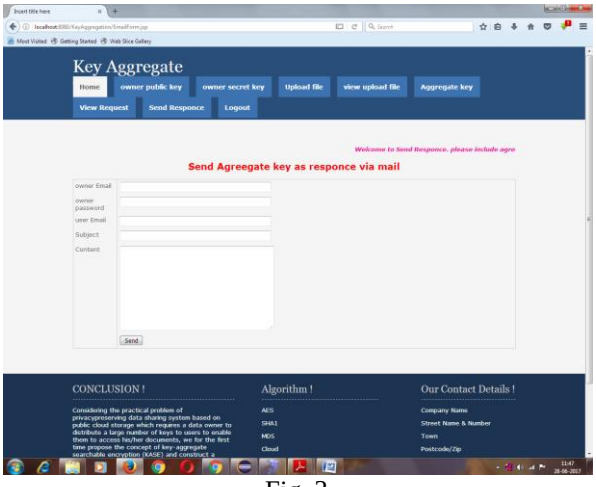


Fig. 3

Using these aggregate key, user will decrypt file.

DOI10.17148/IJARCCE.2017.6672

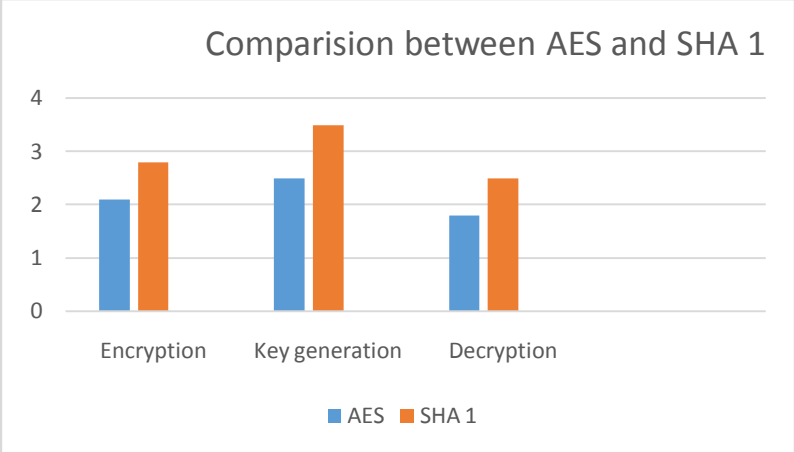
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

VI. RESULT

Encryption between AES and SHA 1 is performed. We have compare these two algorithm using various parameter i.e encryption, key generation, decryption.



VI. CONCLUSION

Mulling over of the practical issue of protection safeguarding information sharing framework in view of open distributed storage which is require an information proprietor to dispense an expansive number of keys to clients to allow them to get to the archives, In this proposed idea of key-total accessible encryption (KASE) and build a solid KASE plot. It can give a proficient answer for building viable information sharing framework in view of open distributed storage. In a KASE conspire, the proprietor needs to circulate a solitary key to a client while contributing a considerable measure of records with the client, and the client needs to present a solitary trapdoor when they inquiries over all archives shared by a similar proprietor

REFERENCES

[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 Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.
[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric 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 efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.