ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Achieving Secure, Scalable, Data Group Sharing Using Key Aggregate Searchable Encryption

Rajeshree K. Duratkar, Prof. Sonali A. Patil

M.E Student, Department of Computer Engineering, JSPM's B.S.I.O.T.R, Wagholi, Pune University, India

Asst. Professor, Department of Computer Engineering, JSPM's B.S.I.O.T.R, Wagholi, Pune University, India

ABSTRACT: Data sharing is a very essential practicality in cloud storage. This article usually have a tendency to reveal the way too firmly, expeditiously, and flexibly proportion understanding with others in cloud garage. The energy of preferentially sharing encrypted knowledge with no longer like users thru public cloud garage may additionally extremely ease safety misery, with the aid of threat understanding disclose in the cloud. a key check to style such coding plan lies inside the nicely-prepared control coding keys. The popular flexibility of allocating any cluster files with any cluster of users by accomplishing weight age totally exclusive coding keys to be used for diverse files. On the alternative hand, this includes the requirement of firmly distributing to users by way of an outsized style of keys for every coding and search, and people customers were given to get to save the received keys. For the duration of this paper, we have a propensity to target this practical downside, by means of suggesting the unconventional construct of key combination searchable coding (KASE) and instantiating the idea thru a true KASE subject matter, throughout which an facts proprietor wishes to proportion out one key to a user for distributing an outsized type of documents, and therefore the user has to present one trapdoor to the cloud for wondering the shared files facts deduplication is a method for putting off reproduction copies of facts, and has been widely used in cloud garage to reduce garage space and upload bandwidth. But, there may be only one replica for each document saved in cloud even though any such report is owned by using a huge number of users. As a result, deduplication device improves storage utilization while reducing reliability. Moreover, the assignment of privacy for touchy data additionally arises whilst they're outsourced with the aid of users to cloud.

KEYWORDS: Public key encryption, master key, cloud computing, web based services, data sharing.

I.INTRODUCTION

With growing dependency on net for globalization, fee for owning it infrastructure, sources have multiplied. Cloud computing is a new concept that typically is an on call for leasing carrier for net programs and it assets. in step with nist definition, “cloud computing is a model for allowing ubiquitous, convenient, on-demand network access to a shared pool of configurable computing assets (e.g., networks, servers, storage, programs, and offerings) that can be unexpectedly provisioned and launched with minimum management attempt or provider interplay”. Cloud computing reduces big upfront investments and habitual ongoing maintenance fee because of its principle of “pay for what you use”. In cloud computing, the assets may be in a person else’s premises or network commonly referred to as companies. The sources can be leased and are accessed remotely by using cloud users or cloud carrier customers via internet or community. All request acquired by way of the cloud servers are processed and the output is despatched lower back as ordinary system. In this paper, we suggest the novel concept of key-combination searchable encryption (KASE), and instantiating the concept thru a concrete KASE approach. the proposed KASE scheme relates to any cloud storage that supports the searchable group data sharing characteristic, which means any consumer might also opt to distribute a set of files that are selective with a set of selected users, at the same time as allowing the very last to perform key-word search above the sooner. To preserve searchable group statistics sharing the main desires for efficient key control are double. Typically, a information proprietor wants to allocate a single mixture key (rather than a collection of keys) to a

DOI: 10.15680/IJIRCCE.2016. 0412151

consumer for sharing any number of documents. Subsequent, the person wishes to submit a unmarried combination trapdoor to the cloud for appearing keyword search over any amount of shared documents. KASE scheme can guarantee both requests. Data de-duplication is a specialized records compression method for putting off duplicate copies of repeating information. Associated and extremely synonymous phrases are intelligent (statistics) compression and single-instance (information) garage. This approach is used to enhance garage utilization and also can be carried out to network records transfers to reduce the wide variety of bytes that ought to be sent.

II.LITERATURE REVIEW

A. 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.

B. 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.

C. 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.ARCHITECTURAL DESIGN

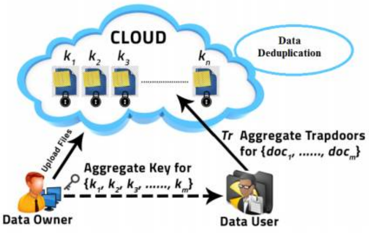
CLOUD
k_1 k_2 k_3 k_n
Data Deduplication
Upload Files
Tr Aggregate Trapdoors for $\{doc_1, ..., doc_m\}$
Aggregate Key for $\{k_1, k_2, k_3, ..., k_m\}$
Data Owner
Data User

Fig: KASE Architectural diagram

IV.PROPOSED SYSTEM

We will be predisposed to cope with this assignment by offering the novel idea of key-aggregate searchable encoding (KASE), and instantiating the concept via a concrete KASE subject. The planned KASE topic applies to any cloud garage that supports the searchable cluster understanding sharing practicality, which indicates any person may by way of selection percentage a gaggle of distinct documents with a bunch of targeted users, whereas permitting the latter to carry out key-word search over the previous. To help searchable cluster knowledge sharing the most needs for reasonable key control a twofold. First, a statistics owner completely has to distribute one aggregate key (in preference to a bunch of keys) to a user for sharing any range of files. Second, the user entirely has to put up one combination trapdoor (in preference to a group of trapdoors) to the cloud for pastime keyword seek over any variety of shared documents. Datadeduplication is a method for reducing the quantity of garage area an organisation wishes to keep its records. in most groups, the garage systems include reproduction copies of many pieces of information. for example, the equal document can be saved in numerous one of a kind locations by means of extraordinary users, or two or more documents that aren't same may additionally nonetheless consist of a good deal of the equal records. Deduplication gets rid of these more copies by means of saving simply one copy of the records and replacing the other copies with tips that lead back to the original replica. Agencies frequently use deduplication in backup and disaster recovery packages, but it could be used to unfasten up area in primary storage as nicely.

V.ALGORITHMS

1. AES

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

2. K-means

K-means is one of the simplest unsupervised learning algorithms that solve the well - known clustering problem. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed apriority. The main idea is to define k centres, one for each cluster. These centres should be placed in a cunning way because of different location causes different result. So, the better choice is to place them as much as possible far away from each other. The next step is to take each point belonging to a given data set and associate it to the nearest centre. When no point is pending, the first step is completed and an early group age is done. At this point we need to re-calculate k new centroids as barycentre of the clusters resulting from the previous step. After we have these k new centroids, a new binding has to be done between the same data set points and the nearest new centre. A loop has been generated.

VI.CONCLUSION

How to protect users' information privateness is a vital question of cloud storage. With greater mathematical tools, cryptographic schemes are getting extra versatile and regularly contain multiple keys for a single utility. Recollect the way to “compress” secret keys in public-key cryptosystems which support delegation of secret keys for special cipher text classes in cloud garage. Regardless of which one some of the electricity set of instructions, the delegate can usually get mixture key of steady size. Our method is more flexible than hierarchical key challenge which can only store spaces if all key-holders share a comparable set of privileges. An issue in our paintings is the predefined sure of the number of most cipher text training. In cloud storage, the wide variety of cipher texts typically grows hastily. So we have to reserve enough cipher textual content lessons for the destiny extension. Despite the fact that the parameter can be downloaded with cipher texts, it'd be better if its size is unbiased of the maximum variety of cipher text training. On the other hand, whilst one consists of the delegated keys round in a mobile tool without the usage of unique relied on hardware, the secret's set off to leakage, designing a leakage resilient cryptosystem. Also duplicated information are removed from cloud in order that storage can be stored.

REFERENCES

[1] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, "SPICE - SimplePrivacy-Preserving IdentityManagement for Cloud Environ-ment,"Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS),vol. 7341, pp. 526-543, 2012.
[2] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.
[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W.Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.
[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Dataon the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems ICDCS 2013. IEEE, 2013.
[5] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng,"Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,"in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.
[8] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.
[9] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.
[10] J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.
[11] C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114-127, 2011.
[12] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.
[13] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained AccessControl. Information Security and Cryptology, LNCS, pp. 406-418, 2012.
[14] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490- 502, 2012.

BIOGRAPHY

Rajeshree Kawdu Duratkar is a M.E student in the computer engineering Department, College of JSPM"s B.S.I.O.T.R, Wagholi, Pune University, Maharashtra, India. She received bachelor of Computer science and engineering (B.E) degree in 2010, from Sipna C.O.E.T, Amravati, MS, India. Her research interests in cloud computing.