ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

Efficient Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage

Niraj Jaywant Bankar, Prof. Kore Kunal Sidramappa

P.G. Student, Department of Comp Engineering, SPCOE Otur Pune, India

Professor, Department of Comp Engineering, SPCOE Otur Pune, India

ABSTRACT: Data sharing is vital functionality in cloud storage.To address user concerns over possible unused quality facts lets loose in cloud storage a common way in is for the facts owner to encrypt all the facts before uploading them to the cloud, such that later the encrypted facts may be got back and decrypted by those who have decryption keys. A key question to designing such process of changing knowledge into a secret form design slices in the good at producing an effect of business managers of process of changing knowledge into a secret form keys. This also suggests the need of safely making distribution to users a complex number of keys for both process of changing knowledge into a secret form in look for and user will have to safely store the received key and put forward an equally greatly sized number of keywords trapdoors to the cloud in order to act look for over the shared data. The practical problem of right not to be public keeping safe facts having the same system based on public cloud storage which has need of a facts owner to make distribution a complex number of keys to users to make able them to way in his/her Documents. While addressing this practical problem, which is largely neglected in the literature, we propose the novel concept of major overall search encryption (KASE) in which the owner of the facts only for a single complex document and user's user. The user needs the same key delivery. For a complex number of shared documents, go to the single on the cloud for a question Out of necessity.

KEYWORDS: Searchable Encryption, Data Sharing, Cloud Storage, Data security, Trapdoor Mapping.

I. INTRODUCTION

Cloud storage has come out of as a hoping answer for making ready present every-where, right, and on-request ways in to greatly sized amounts of facts shared over the net. Today, millions of users are having the same personal facts, such as pictures by camera and videos, with their friends through grouping network applications based on cloud storage on a daily base. Business users are also being get attraction for by cloud storage because of, in relation to its great number of helps, including lower price, greater quick-moving and better resource utilization.However, while getting pleasure out of the toilet of having the same facts via cloud storage, users are also increasingly had a part in about not through design, by chance facts lets loose in the cloud. Such facts lets loose, caused by a bad person fighting against one or a behaving badly cloud operator, can usually lead to serious over-rules of personal right not to be public or business secrets (e.g. the near in time high outline small event of noted person pictures by camera being leaked in icloud).To remove users' concerns over potential data leaks in cloud storage, the data is for the user to encrypt all data before uploading it to the cloud, such as later encrypted data can be retrieved Can be decrypted and have decryption which has decryption. Such cloud storage is often called cryptographic cloud storage.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

II. LITARATURE SURVEY

AccordingAccording to KaipingXue [1] providing a more efficient access control scheme with single-point performance barrier problem and auditing mechanism. Our framework employs many specialty authorities to share the load of user validity verification. In the meantime, in our plan, a CA (Central Authority) is started to generate secret keys for verified users.Unlike many multi-authorization access control schemes, each officer of our plan personally manages the entire set of features. To increase security, we also offer an auditing mechanism to ascertain that the AA (attribute authority) has performed the validity verification process incorrectly or maliciously.

Kan Yang and et. Al.[2], proposed Apply a reciprocal multi-authorization CP-ABE plan, and as a built-in technique to design data access control plan. The law can achieve both security and backward security efficiently. This system also creates an expensive, efficient, and reversible data access control plan for multi-authority cloud storage systems. many authorities are in co-existence and each authority is capable of releasing the features independently.

The system [3] proposed without any secure third-party channels, anti-collusion is a safe way to deliver key, and users can safely obtain their own private key from the owner of the group. Second, this method may propose fine grained access control, any user in the group can use the source in the cloud and after the cancellation, and the user cannot access the cloud again.Collision can attack the plan by attack; it means that the cancelled users cannot get the actual data file, even if they combine without the cloud. In this approach, by exploit polynomial capability, framework can complete a safe client negation conspires, finally, this plan can accomplish fine efficiency, and which means that the previous customers do not need to refresh their cancellation from the group.

According to [4] proposes the major of key-approach feature which is based on KP-ABE with reflection of non-monotonic access structures and with regular ciphertext size. System also proposes the first Key-Policy Attribute-based Encryption (KPABE) The method of allowing for non-fixed access structures (i.e., may contain negative attributes) and with continuous ciphertext size. To achieve this goal, the system first shows that a certain class of identity-based transmission encryption schemes generates monotonic KPABE systems in select set models. The system then describes a new efficient identification-based solution mechanism, which, combined with a special urgency of our normal monotonic construction, with the constant sized cipher-text, first gave birth to the expressive KP-ABE realization is.

According to F. Zhang and K. Kim [5] proposed an ID-based ring signature approach, both approaches has defined base on bilinear pairings as well as Java pairing library. Also system analyzes their security and efficiency with different existing strategies. The Java Pairing library (JPBC) has used for data encryption and decryption purpose. Some user access control policies has design for end users that also enhance the privacy and anonymity of data owner.
In approach [6], propose the first Identity-based threshold ring signature approach that does not support to java pairings. It propose the first Identity -based threshold verifiable ring signature strategy. System also analyze that the secrecy of the actual signers is maintained even against the PK generator (PKG) of the Identity -based system. Finally system shows how to add identity collusion and other existing base different schemes. Due to the dissimilar levels of signer inscrutability they support, the system proposed in this paper actually form a suite of Identity -based threshold ring signature method which is related to many real-world systems with varied anonymity needs.

According to system [7], the system proposed an efficient Encrypted Data Search(EnDAS) scheme As a mobile cloud service This innovative plan uses a lightweight (encrypted keyword) compression method, which optimizes the data communication process by reducing the size of the net for traffic efficiency. Customizable methods for searching the document, the Trapper Mapping Table (TMT) module and rank serial binary search (RSBS) algorithms are said to speed up the search time.

According to system [8] System Define and solve the challenging problem of privacy that maintains the search for multi-keyword rank on encrypted cloud data (MRSE). We establish a set of strict privacy requirements for such a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

secure cloud data usage system. In the various Multi Keyword Keywords, select the efficient coordination measure of "coordinate matching" to capture the relevance of the data documents in the search query, that is, several matches as possible. We further use "internal product similarity" to evaluate the measure of similarity. We first offer a simpleimpression for MRSE based on the compilation of secure internal product, and then offer two majorimprovements MRSE schemes to meet the severalrigid privacy requirements in two different risk models. According to the system [9], the system defines and resolves the problem of keyword search on secure rank on encrypted cloud data.

According to system [9] the system Protected rank on encrypted cloud data defines and resolves the problem of keyword search. Instead of sending a rank search, increasing the system usability by enabling search results relevancy ranking instead of sending undefined results, and ensures file retrieval accuracy ahead. In particular, we find statistical measurement approaches, i.e., relevant scores, to create a safe search index from information retrieval, and to develop a range of order-preservation mapping techniques to properly preserve those sensitive score information. We do.

According to Kan Yan [10], System proposed ciphertext-policy feature-based encryption (CP-ABE) is a promising technique for access control of encrypted data. The system has proposed an operational and protected data access control scheme with DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), efficient decryption and cancellation.Specifically, system construct a new multi-authority there is also a design of a CP-ABE scheme with efficient decryption and an efficient feature refrain process that can complete both further safety and recessive security.

OBJECTIVES OF SYSTEM

The Objective of the proposed application is as follows:

- TO implement a KASE algorithm in multi cloud environment.
- Provide multiple possible results with minimum time complexity.
- Generate minimum load on server side.
- Reduce searching time and maximize the accuracy on multi keyword search system.
- Successfully implement with Role Base Access Control (RBAC) and secure revocation.

III. PROPOSED METHODOLOGY

In the proposed research work to implement a system which can provide multi keyword search system over the AWS cloud.Generate the keyword index and use for searching the results, finally users get top k document for specific query.

- Data Privacy: one but the user can learn the actual retrieved data.
- Index Privacy: The search index or the query index do not leak any information about the corresponding keywords.
- Trapdoor Privacy) given one trapdoor for a set of keywords, the server cannot generate another valid trapdoor.
- Non-Impersonation: No one can impersonate a legitimate user.

.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

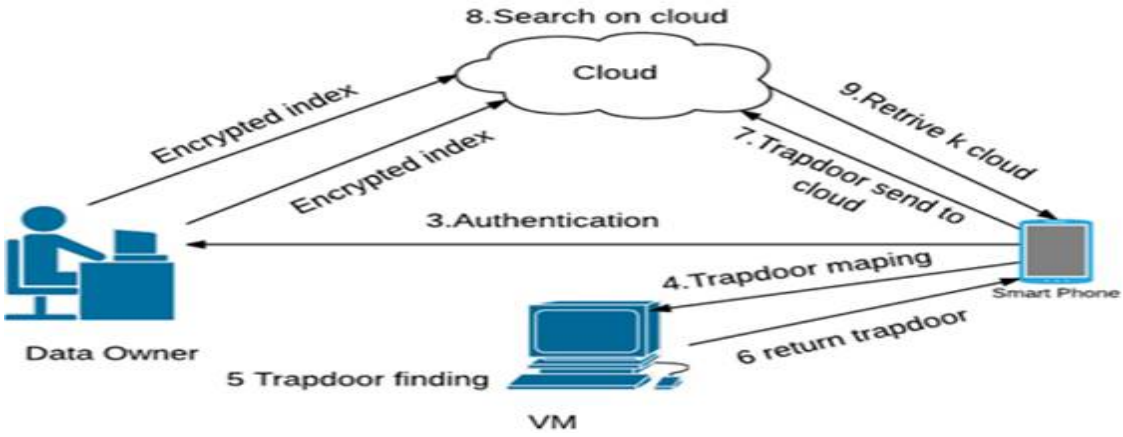

Figure 1 : Proposed System Architecture

1: First provider can upload the file and encrypt the file as document and save into cloud.
2: Here same time data owner can encrypt the index for specific file and save into cloud.
3: This step user authentication has done by provider.
4. If it is valid user then give access of system.
5. User can send the keyword to VM.
6: In VM we create the Slot allocation and trapdoor mapping, it can be find base on keywords.
7: Trapdoor mapping system returns Trapdoors to user.
8: The same Trapdoors (encrypted keyword) user resend to cloud server
9: Then cloud system search on index table
10: Then retrieve the documents similar to index
11: Return the entire document list to user.

The Proposed framework is composed of seven algorithms. Specifically, to establish this plan, the cloud server will produce the system's public parameters through the setup algorithm, and these public parameters can be reused to share their files with various data owners. For each data owner, it should produce a public / master-secret pair through the keygen algorithm. Keywords for each document can be encrypted with encrypted encryption with a unique searchable encryption key. Then, the data owner can use the master-secret key to create the total search encryption key for a group of selected documents via the extracted algorithm. The overall key can be safely distributed (eg, through secure e-mail or secure devices) authorized users, who need access to those documents. After that, as shown in Fig.1.1, an authorized user can produce a keyword trapeador through the Trapador algorithm using this total key, and store the trapper in the cloud. After obtaining the fraud, to perform a keyword search on the specified set of documents, the cloud server will run the adjusted algorithm for generating the correct traffic for each document, and then test the algorithm that the keyword contains the keyword or notSystem provides the below features these are below

Multi-keyword Ranked Search:
To design search plans that allow multi-keyword queries and provide similarity ranking for effective data retrieval rather than retrieving the resulting data.

Privacy-Preserving:
To avert the cloud server from learning bonus information from datasets and indexes, and to meet privacy requirements.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

Efficiency:
The above objectives should be achieved on efficiency and privacy.

Achieve Search Accuracy:
Search accuracy determines whether the search the results match users' search requests. The user will want the same search experience for encrypted data, which Google can provide.In particular, mobile users prefer multi-keyword search instead of single keyword search because single keyword search usually returns search results only.

IV. RESULTS AND DISCUSSION

For the system performance evaluation, calculate the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.8 GHz i3 processor and 4 GB RAM with public cloud Amazon EC2 consol. For the system evaluation we create 2 machines on physical environment with Wi-Fi and 10 VM with Amazon EC2 as public cloud environment. After implementing some part of system we got system performance on reasonable level. The below table 1 shows the proposed KASE algorithm performance for user plain text conversion as well encryption decryption.
First second experimentation system show the user verification time with different approaches. In current system we consider as four different authorities for runtime verification. The below Figure 3 shows the performance measures using different parameters with some existing approaches.

Table 1: System performance (Estimated)

Data Size in KB	Encryption time (Milliseconds)		Decryption time(Milliseconds)	
	Existing	Proposed	Existing	Proposed
5	120	92	155	142
10	235	186	305	270
15	345	285	470	415
20	475	375	610	560

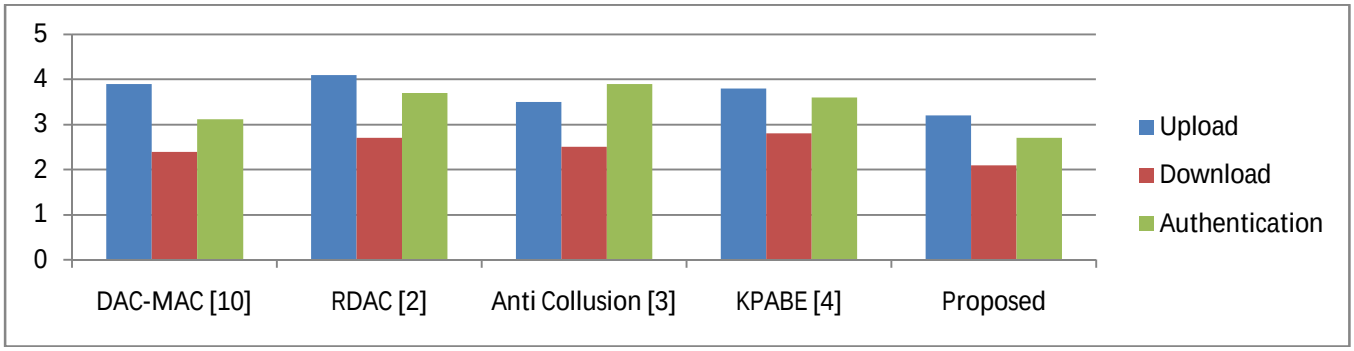

Figure 3: Accuracy of proposed system with existing systems

The proposed KASE algorithm provides the best accuracy as well as result than existing algorithms.
In the second experiment analysis system has evaluated with existing systems with [10], [2], [3], [4] etc. The three functionalities have done in each system like upload, download and authentication of user as well. In the proposed desired configuration system illustrates time complexity in milliseconds.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

V. CONCLUSION

This is a multipurpose cloud administration as an actual encrypted data search plan. Practical problem of confidentiality of maintaining data clouding based on public cloud storage, which requires users to have a large number of keys in order to be able to access their documents, we first use concept-key encryption (KASE) Key-aggregate) and creation of a solid KASE plan.

System also illustrates a Role Base Access Control (RBAC) data sharing scheme for untrusted environment in the cloud. In our scheme, the users can securely get their master and private keys from middleware authorities, VM provide and secure communication between multi parties. Also, our scheme is able to provide the secure revocation for untrusted user. The proxy key generation has also proposed in this work. When data owner revokes any specific end user system automatically expired the existing keys and generates new keys for all shared users. The system can achieve highest level security as well as privacy through such approaches

REFERENCES

[1]. Xue K, Xue Y, Hong J, Li W, Yue H, Wei DS, Hong P. RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage. IEEE Transactions on Information Forensics and Security. 2017 Apr;12(4):953-67.

[2]. Kan Yang and XiaohuaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[3] :Zhongma Zhu and Rui Jiang proposed A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 1, JANUARY 2016.

[4] N. Attarpadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in 2011.

[5] F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 533–547. Springer, 2002.

[6] J. Han, Q. Xu, and G. Chen. Efficient id-based threshold ring signature scheme. In EUC (2), pages 437–442. IEEE Computer Society, 2008.

[7] Ruhui Ma and At. Al. ,"EnDAS: Efficient Encrypted Data Search as a Mobile Cloud Service" IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING IEE 2015

[8] Ning Cao et. Al. "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data" 2014

[9] Cong Wang at. Al. " Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 8, AUGUST 2012.

[10]. Yang K, Jia X. DAC-MACS: Effective data access control for multi-authority cloud storage systems. InSecurity for Cloud Storage Systems 2014 (pp. 59-83). Springer, New York, NY.