ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

Comparison of Keyword Search and Ranked keyword Search in Cloud Computing

[1] Kavya H, [2] Prashanth Putta P, [3] Chethan R, [4] Divya D, [5] Vani Saptasagar,Associate professor ise department
R R institute of technology. RR layout Chikkbanavara , Bangalore.

***Abstract*— Cloud computing otherwise known as on demand computing. It provides the services over the internet. It has the provision of facilitating users to store and access their data in and from cloud server by sitting anywhere and on any device. Storing data in cloud server also opens up so many security threats as data is accessed over internet and client has no direct control over data once uploaded into cloud server. We first implement a basic idea for the Single Keyword Search Over Encrypted Data And then Multi-keyword Ranked. Search over Encrypted cloud data (MRSE) based on secure inner product computation and efficient similarity measure of coordinate matching, i.e., as many matches as possible, in order to capture the relevance of data documents to the search query, then we give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Assignment of anonymous ID to the user to provide more security to the data on cloud server is done. To improve the search experience of the data search service, further extension of the two schemes to support more Search semantics is done.**

***Index Terms*— Cloud computing, Encryption, Inner product similarity, Single Keyword Search, Multi-keyword , search ranking.**

I INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources.

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. C which includes ciphering, providing index etc . cloud computing enables cloud customers to remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources.

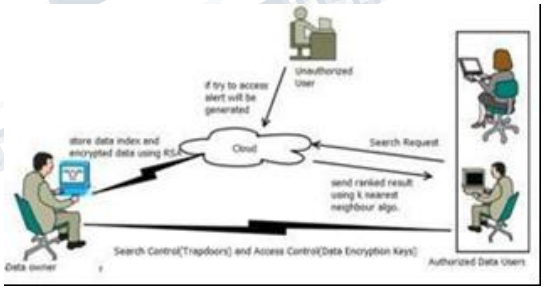

Fig1. Architecture of the search over encrypted cloud Data

(Mell and Grance 2010). The benefits brought by this new computing model include but are not limited to relief of the burden for storage management, universal data access with independent geographical location, and avoidance of capital expenditure on hardware, software, and personnel maintenances. (Griffith, joseph, Katz, Konwinski , Lee,Patterson, Rabkin, Stoica, and Zaharia 2009). With the increase the use of cloud services, more and more sensitive information are being centralized into the cloud servers, such as emails, personal health records, bank details, private videos and photos, company financial data, government documents, etc.

Popular services of cloud computing is data outsourcing through internet. For reasons of cost and convenience,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

public as well as private organizations can now outsource their large amounts of data to the cloud and enjoy the benefits of remote storage. At the same time, confidentiality of remotely stored data on untrusted cloud server is a big concern because of speculations. Although encrypted data storage protects remote data from unauthorized access, it complicates some basic, yet essential data utilization services such as plaintext keyword search. A simple solution of downloading the data, decrypting and searching locally is clearly inefficient since storing data in the cloud is meaningless unless it can be easily searched and utilized. Thus, cloud services should enable efficient search on encrypted data Researchers have investigated this problem quite extensively in the context of encrypted documents. wrapping of data plays a important role. Solutions generally involve building an encrypted searchable index such that its content is hidden from the remote server yet allowing the corresponding documents to be searched. These solutions differ from each other mostly in terms of whether they allow single keyword search or multi-keyword search and the types of techniques they use to build the trapdoor function. However, these techniques either do not allow searching on multiple keywords and ranking the retrieved document in terms of similarity scores or are very computationally intensive. In this work, we propose a novel secure and efficient multi-keyword similarity searchable encryption scheme that returns the matching data items in a ranked order. Our contributions can be summarized as below:

1. We present a secure searchable encryption scheme that allows multi-keyword query over encrypted document corpus and retrieves based on search.

2. We construct the searchable encryption scheme that is CKA2-secure in the random oracle model . Our scheme achieves semantic security against adaptive adversaries that choose their search queries as a function of previously obtained trapdoors (which computes in one direction) and search outcomes

3. We present a construction that achieves the optimal search time. Unlike all previous schemes that are glued to the linear search complexity, our search is sublinear to the total number of documents that contain the queried set of keywords. We show that this type of searchable encryption scheme can be extreme-efficient.

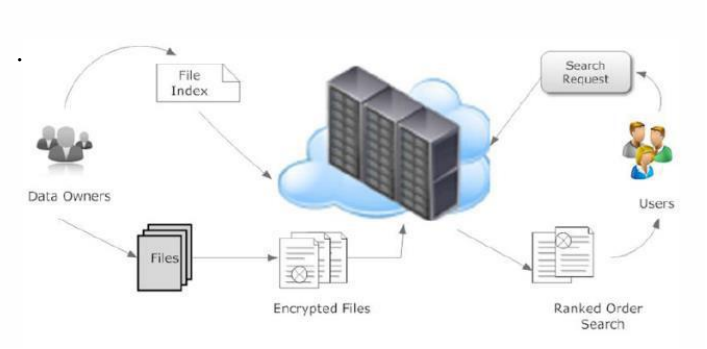

Fig. 2 Architecture of search over cl

II .RELATED WORK

2.1 Secured Multi-keyword Ranked Search over Encrypted:

In cloud compute data possessor are aggravated to farm out their multifaceted data organization systems from local sites to the marketable public cloud for superior give and economic savings. To make sure safety of stored data, it is have to to encrypt the data before storing. the cloud. In these existing systems the algorithms used are cryptographic. Organizations, companies store more and more valuable information is on cloud to protect their data from virus, hacking. The benefits of the new computing model include but are not limited relief of the trouble for storage administration, data access, and avoidance of high expenditure on hardware mechanism, software, etc. Ranked search improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency),As directly outsourcing relevance scores will drips a lot of sensitive information against the keyword privacy. We proposed asymmetric encryption with ranking result of queried data which will give only expected data.

2.2 Privacy Preserving Keyword Searches on Remote:

Encrypted Data: Consider the problem: a user U wants to stock up his files in an encrypted form on a far-flung file server S. afterward the user U wants to professionally get back some of the encrypted files contain exact keywords, keeping the keywords themselves clandestine and not to cause danger to the security of the tenuously store files. For example, a user may want to store old e-mail post encrypted on a server manage by Yahoo or one more large vendor, and later regain certain messages while travelling with a mobile device. In [2], solutions for this problem under well-defined safety requirements are obtainable. The idea of that scheme is to build an index of keywords for each file using a Bloom filter [B70], with pseudorandom functions used as hash functions.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

When U submits a document to S, he also submits the corresponding Bloom filter. We suspect that the security model defined in [G04] is insufficient, as the scheme cannot resist certain attack. Specifically, because the number of 1's of a Bloom filter is (roughly) proportional to the number of the distinct keywords of a document, some information is immediately leaked from the Bloom filters themselves, and we believe that statistical analysis based on this (and related) facts can compromise the security of the encrypted files.2 On the other hand, one inherent problem with this Bloom-filter-based approach is that Bloom filters inevitably induce false positives, which would potentially cause mobile users may download extra files not containing the keyword. While sufficiently rare false positive might be acceptable, we note that our scheme avoids this problem

2.3 Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data:

On one pass, users who do not unavoidably have prior knowledge of the encrypted cloud data, have to post process every retrieved file in arrange to find ones most matching their interest; On the other hand, invariably retrieving all files containing the query keyword further incur unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud archetype. This paper has definite and solved the problem of effectual yet safe and sound rank keyword search over Encrypted cloud data [2]. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency) thus making one step closer towards sensible consumption of privacy-preserving data hosting services in Cloud Computing. For the first time, the paper has defined and solved the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE) [2], and establish a set of strict privacy requirements for such a protected cloud data utilization system to become a reality. The proposed ranking method proves to be efficient to go back extremely relevant documents corresponding to submitted search terms. The idea of proposed ranking method is used in our future system in order to enhance the security of information on Cloud Service Provider.

2.4 Single Keyword Search over Encrypted data on cloud:

Obtainable searchable encryption scheme consent to a user to firmly look for over encrypted data through keywords without first decrypting it, these techniques support only conventional Boolean keyword search, without capturing any relevance of the files in the search result. When directly applied in large joint data outsourcing cloud environment, they go through next shortcoming.

1) The Most Significant Single-keyword Search (MSSS) scheme over encrypted cloud storage data reduces search time over large data sets on cloud.

2) The Most Significant Single-keyword Search algorithm reduces the index generation time to O (NT × 3) and supports single-keyword top-k retrieval over encrypted cloud data.

3) A new mathematical model is developed for secure 2 encryption search over index, without learning anything about queried keyword from unauthorised entities.

III IMPLEMENTATION DETAILS

3.1 MRES System

For our organism, we choose the attitude of harmonize matching, to identify the correspondence amid search inquiry and data credentials. Particularly, we use internal data correspondence, i.e., the figure of query keywords appearing in a document, to appraise the similarity of that document to the search query in coordinate matching principle. Each document is connected with a binary vector as a sub index where each bit represent whether analogous keyword is contained in the document [6] The search reservation is also describe as a dual vector where each bit means whether corresponding keyword appears in this search request, so the similarity could be exactly measured by inner product of query vector with information vector. However, directly outsourcing data vector or query vector will infringe index privacy or search privacy To improve document retrieval accuracy, search result should be ranked by cloud server according to some ranking criteria. Cloud server only sends back top-k documents that are most relevant to the search query. Multi Keyword Ranked Search In this method searching of cloud data using Privacy Preserving Multi keyword Ranked Search (MRSE). Here basic concept is used is co-ordinate matching. Coordinate matching obtains the similarity between search query and documents. Inner product similarity is also used to describe the multi keyword ranked search over encrypted cloud data (MRSE). The features of this method are, multi keyword ranked search, privacy-preserving, high efficiency is eliminating unnecessary traffic and improve search accuracy. The steps of ranked search are shown below.

1. Data owner collects the file and generate the index by extracting the keyword from data files and published index and data files on cloud.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

2. After outsourced the data files user is enable to search and download the data files from cloud server.

3. User can search through single or multiple keywords that is encrypted and using this keyword one trapdoor is generated.

4. Using trapdoor the relevant keyword data files is searched using query and searched data is shown to the user.

This scheme introduces a lower overhead on both the computation and communication. Also explore other multi-keyword semantics over encrypted data, integrity check of rank order in search result and privacy guarantees in stronger threat model. In the wished-for organism the stream starts from the user. The user has to register in CSP to get the amenities. Once user data is stored in CSS it has no unswerving control above it. User has to hire any auditor called TPA who will very regularly check the user data in CSS . The TPA should be granted by the user to check the integrity for a specific data and for a unambiguous time without accessing the exact data. Below an algorithm is provide which describe how the TPA does the audit.

AES

In today's world most of the communication is done using electronic media. Data security plays a vital role in such communication. Hence there is a need to protect data from malicious attacks. This can be achieved by Cryptography. The earlier encryption algorithm is Data Encryption Standard (DES) which has several loopholes such as small key size and sensible to brute force attack etc. and it cannot be provide high level, efficient and exportable security. These loopholes overcome by a new algorithm called as Advanced Encryption Standard (AES). However, it is a very difficult to search the most suitable services or products for ordinary consumers, as there are so many services and products in cloud. Meanwhile, data outsourcing enables the data owner and the cloud service provider not in a same trusted domain, making the data owner not manage data in real time. It is a common practice to encrypt sensitive information before outsourcing. The plain text of 128 bits is given as input to encryption block in which encryption of data is made and the cipher text of 128 bits is throughout as output. The key length of l28bits, l92bits or 256bits is used in process of encryption. The AES algorithm is a block ciphers that user the same binary key for both encryption and decryption of data blocks.

1. Cryptography - Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. Generally speaking, it uses a cryptographic system to transform a plaintext into a cipher text. using most of the time a key. It has different Encryption and Decryption algorithms to do so.

2. Cipher Text - This is the scrambled message produced as output from Encryption algorithm. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts.

3. Encryption - Encryption is the process of converting data, in plain text format into a meaningless cipher text by means of a suitable algorithm. The algorithm takes secret key and plain text as input and produces cipher text.

4. Decryption - Decryption is converting the meaningless cipher text into the original information using decryption algorithms. The decryption algorithm is inverse of encryption algorithm. This takes key and cipher text as input and produces original plain text.

5. Symmetric Key Cryptography - It uses the same secret (private) key to encrypt and decrypt its data. It requires that the secret key be known by the party encrypting the data and the party decrypting the data for better use.

6. Asymmetric Key Cryptography – Asymmetric uses both a public and private key to compute. This allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key. To search over encryption data multiple search techniques are invented which are described below

AES Algorithm:
Notation and Definitions
1. The set of round keys from the cipher key.
2. Initialize state array and add
the initial round key to the
starting state array.
3. Round = 1 to 9 : Execute Usual Round.
Execute Final Round
i. Corresponding cipher text chunk output of
Final Round Step
ii. Usual Round Execute the following
operations which are described above.
1. Sub
Bytes
2. Shift

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

Rows
3. Mix
Columns
4. Add Round Key , using K(round)

iii. .Final Round:
Execute the following operations which are described above.
1.Sub Bytes
2.Shift Rows
3. Add Round Key, using K (10)

Algorithm

AES(K, W)	Encrypt W using the AES codebook with key K
AES-1(K, W)	Decrypt W using the AES codebook with key K
MSB(j, W)	Return the most significant j bits of W
LSB(j, W)	Return the least significant j bits of W
B1 | B2	Concatenate B1 and B2
K	The key-encryption key K
S	The number of steps in the wrapping process, = 6n
P[i]	The ith plaintext key data block
C[i]	The ith cipher text data block
A	The 64-bit integrity check register
R[i]	An array of 64-bit registers where i = 0, 1, 2, ..., n

IV. RESULT

In this section we present comparison result of Single Key word Search Ranked search and Multi Keyword Ranked Search Over A Encrypted Data On Cloud as shown in following figures .In this Result Each Ranked search and Multi Keyword Ranked Search Over A Encrypted Data On Cloud..In this Result Existing System is Single Keyword Search System and proposed System is nothing but MRES System

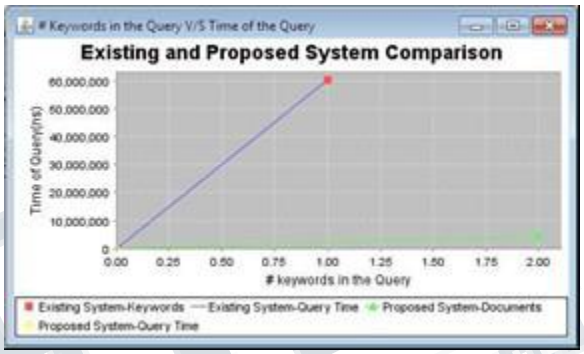

Fig 2: Comparison Graph- No. Of Documents V/S Query

Fig 2 is a Comparison graph of Existing System and Our System to see changes. The graph is plotted Number of Documents that the respective system's search result returned and Time required to return the documents; in respective System. As shown in the graph Our system requires less time which is less than around 5 ns with most specific result of number of document equal to one which is less than the documents returned by existing system which are three and time required is around 6ns only

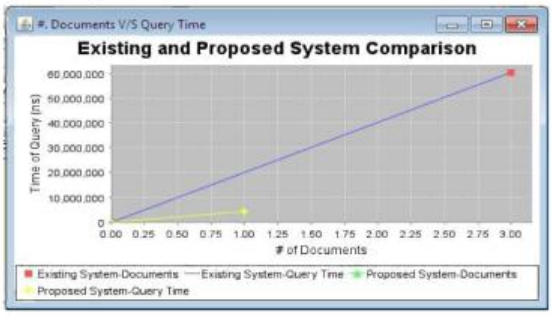

Fig 3: Comparison Graph- No. Of Keywords V/S Query Time

The graph is plotted against Number of Keywords fired in the respective system's search and Time required in respective System. As shown in the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

graph our system requires less time which is less than around 5 ns with multiple Keyword Query and existing system requires around 6ns even though a single Keyword query is fired. So Our System Works Better in each and every aspect then existing System. Which gives the better performance when compared.

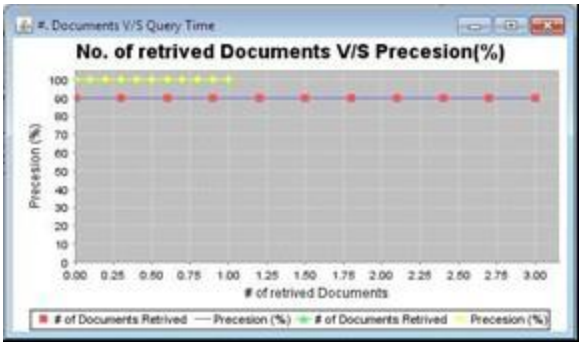

Fig 4: shows The Comparison graph of Existing System and Our implemented System plotted against No of Documents returned by respective system V/S percentage Precision(Perfectness). Our system gives much better precession than existing system as shown in graph above.

In this method the major merits are:
(1) Data security by encryption.
(2) Privacy shield through trapdoor.
(3) Auditing details to the data owner.
(4) Audit aptitude aware data scheduling at this time we are going to evaluate the performance of our projected scheme in terms of the computation introduce by each operation. Request and resources are taken as the computing parameter. When the numbers of requests increase at the same time, it is to check whether they are served within a particular time with the correct output. The waiting time is measured for each request for further computation.

V. CONCLUSION

In our future work, the software executes successfully by fulfilling the objectives of all the project needs. Further extensions to this system can be made required with minor modifications. This project presents to design and develop an efficient service to protect users' data privacy is a central question of cloud storage. The invention can be implemented in digital electronic circuitry or in computer hardware, firmware, Software or in combinations of them. Apparatus of the invention can be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor and method steps of the invention can beperformed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output successfully.

VI .REFERENCES

1. Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. Of INFOCOM, 2010.

2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley

3. R. Carmela, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, pp. 79–88, Oct. 2006.

4. R. Agarwal, J. Kiernan, R. Srikanth, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD'04, Paris, France, pp. 563–574, Jun. 2004.

5. D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," EUROCRYPT, vol. 43, pp. 506–522, 2004