ISSN: 0976-3104
SPECIAL ISSUE: COMPUTER SCIENCE

ARTICLE

IMPROVEMENT IN SEARCH TIME USING MULTI-KEYWORD SEARCH OVER ENCRYPTED DATA IN CLOUD COMPUTING

Anagha Ramnath Kadve, S. B.Vanjale

Dept of Computer Engineering, Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune, INDIA

ABSTRACT

Background: *The enrichment of the network and the growth of vast knowledge, also the distantly out-sourced the data to the cloud, which evades local organization of information.* ***Methods:*** *The system decreases the needed hardware cost. However, some subtle information, like individual healthcare info and private property info should be encoded first then subcontracted to the cloud. The system will shield confidential information. However, the encoded files on the cloud will rise the problem of the data recovery.* ***Results:*** *T the host cross from the cloud, which can end in large communication calculation upstairs.* ***Conclusions:*** *Very first the owner of the data has to keep online in single owner theme for generating entrances (Encrypted keywords) which can have an impression of usability and suppleness of search system.*

KEY WORDS
Cloud Computing, Privacy Preserving, Encryption/Decryption, Ranking, Relevance Score Find, Top-k Monitoring, Security

Received: 28 Nov 2017
Accepted: 03 Jan 2018
Published: 10 Jan 2018

***Corresponding Author**
Email:
anaghakadve92l@gmail.com
Tel.: +91-9762445248

INTRODUCTION

Cloud Computing is a revolutionary technology which is changing the entire approach of software hardware designing and purchasing. Cloud Computing has numerous benefits including fast distribution, simple access, and malleable ability management and decreased costs, etc. The action of all sizes can influence the cloud to enhance collaboration and innovation. There are huge advantages of Cloud Computing technology; due to this for privacy concern many organizations and individual upload their sensitive and confidential documents to the cloud. This helps in preserving the data security from unauthorized users [1].

Cloud Service Providers (CSPs) would guarantee to assure holders information safety using mechanisms like virtualization and firewalls. Data owner's information secrecy from the CSP itself does not protect by the mechanisms. Therefore the CSP acquire full management of cloud holder's information, software, and hardware. Encoded on conscious information before subcontracting can conserve information secrecy alongside Cloud Service Provider. However; encryption of data crafts the traditional information usage service entirely based on plain text keyword pursuit which is an extremely exciting problem. An incidental answer to the issue is to take all the encoded files and decode them narrowly. The technique is certainly impossible since it will damage a vast conversation volume upward. Consequently, building a secure examine examination of encoded cloud data is of supreme significance. Safe pursuit above encoded information has newly engrossed the importance of various scholars. The system defines and solves the problem of safe examine over encryption of data. Formation of searchable encryption proposes by the system, which is a cryptographic primeval that the main contributions of the paper are as follows:

- The issue of safe fuzzy keyword search will consider by the system.
- Create a dynamic key using fuzzy logic

The Cloud Service Provider may be a distinct object. Thus Cloud Computing has several privacy problems, especially, the info safety is vitally necessary and is as well the foremost doubtless to impend the consumer's secrecy. To check the information, the files may be encoded and outsourced to the cloud. Though, this may lead to a problem of information recovery.

RELATED WORK

The system has explained benefits of the approach with different algorithms. For an explanation of the proposed work techniques and algorithms such as indexing, trapdoor generation, re-encryption of the trapdoor and top-k file display.

In the paper [1] conveys some trouble for information search. Searchable encoding permits users to search for the encrypted data on cloud storage to retrieve the associated information without decryption. The files recovered if, as long as user's feature satisfies the access policy, and so the required keywords accept as true with the file keyword. Also, the removed user cannot search over again although he/she plots with one of the servers. The existing author improves the system model of searchable encoding by victimization two non-colluding cloud servers.

In the paper [2] explains the multi-keyword search mechanism that the users will search within the cloud simply per their quest. In planned system, new public-key cryptosystems are planned to securely, with efficiency, and only share data with others in cloud storage. The primary method is that one will aggregate any set of secret keys and build them as compact as one key. However, all keys should be collective. The

IIOAB JOURNAL
ISSN: 0976-3104

methodology is more versatile than ranked key assignment. The method is extremely convenient and shares information in a particular way. A limitation in work is time-consuming for decrypting files and therefore the space for storing for keys extended in future work. Multi-keyword search mechanism explains that the users can search among the cloud merely per their search. The methodology is extremely convenient and shares information in a particular method. A limitation of the system is time-consuming for decrypting files.

In the paper [3] explains the enhancement of the network and a massive expansion of data. The information holder used to distantly outsources the records to the cloud, which could escape the native info managing and scale back the native hardware worth. The supply of encrypted info to the cloud can raise the matter of the information recovery. As a result of knowledge holder or illegal operators can't find the records properly which was a need, and also the unfeasible to send all of the data to the native side from the cloud, that is in a place to guide to huge communication a computation overhead.

In the paper [4] the existing author tends to consider a more complicated model, wherever the cloud server would most likely behave deceitfully. Based on the model, the author explores the problem of result verification for the secure ranked keyword search. Entirely different from previous information verification scheme, the existing author proposed a unique deterrent based system. With the carefully devised verification information, the cloud server cannot understand that information holder, or how many information owners exchange anchor data which can use for confirming the cloud server's misbehavior.

In the paper [5] system propose schemes to deal with secure ranked multi-keyword search in a multi-owner model. To permit cloud servers to implement safe search without understanding the original information of both trapdoors and keywords, the existing author systematically constructs a new reliable pursuit protocol. To rank the quest results and conserve the security of related scores between files and keywords, the existing author proposes a novel Additive Order and Privacy-Preserving Function family. To enable the cloud server to operate safe search among multiple owners data encrypted with different secret keys, the existing author systematically constructs a new secure search protocol. Following are the key contributions of the paper:

- The existing author defines a many-holder model for safe keyword pursuit above encoded cloud documents, which formulae a quicker phase to actuality.

- The existing author consistently develops a different safe pursuit protocol that not only implements the cloud storage to complete safely rated keyword pursuit without understanding the original information of together trapdoors and keywords but also confesses information holder to encode keyword through authorized data users and self-chosen keys to request without perceptive the keys [6].

MATERIALS AND METHODS

The proposed system [Fig-1] is presenting an appropriate explanation for the target problem during the paper. The proposed system tends to initial describe a corresponding risk model and a structure model. Then the system elucidates the planning objectives of the resulting structure and a listing of symbolizations utilized in next negotiations. In the paper, the system tends to recommend PRMSM, a secrecy-protective graded multiple-keyword quest protocol during a many-holder cloud model. To accomplish a safe search without perceptive the exact value of each trapdoor and keyword and to modify cloud storage, the structure consistently constructs a different safe pursuit protocol [7]. To rank the search results and preserve the privacy of relevancy scores among keywords and files, the system tends to propose a new additive order and protective privacy function; the family that helps the cloud server, come back the first relevant search results to information users without revealing any sensitive data.

Advantages of Proposed System

Data Subcontracting Safety

Cloud will store the user's information, as a result of users now not physically possess this information. Hence, the reliability of the information will be in danger. The handlers' secrecy is below risk because the CSP manage all of the information [6], [7]. To evade the matter that information is clear to the Cloud Service Provider, the information has been encoded such a source to the cloud. The information can stay encoded once storing in the cloud.

Subcontracting Safety of Computation

Computation jobs and the native host data organization will reduction using the cloud. The cloud procedure information is not clearly sufficient to operators because of industrial clouds are not entirely reliable. Additional inspirations may result in the improper outcomes square measure recovered to the handlers [7].

IIOAB JOURNAL
ISSN: 0976-3104

Access Control

There is several user's storage information within the cloud. Solely the data holder and approved end users will recover the info. To make sure the privacy or shield the subtle data, the data typically authorized to the cloud in a coded format and therefore the encoded information should release the cryptography key solely to approved holders.

Truthful Service Metering

To make sure the CSP's revenue, the restrained facility included in all summarization which is very important. The return is that the industrial clouds primary resolve finally. Notwithstanding CSP charge to the customers within which ways, like computing source or supported time. The systematic procedures should be reliable and truthful. The cloud computing is see-through to the operators [7]. Therefore the service-metering mechanism should assurance the quantity of incomes that operators expended are accurate.

Safety of Multi-tenancy

The end users will use a virtual machine or share virtual machines when the cloud sometimes virtualizes the corporal structure. However extreme usage can affect alternative operators, and fewer end users in an exceedingly only one virtual machine could be a liberal usage. Operators someday measure operating in varied surroundings, as a result of some free net has petite protection or an entire firewall. Hence, one users' setting can affect the traditional use of the server or alternative users [7].

Security of Virtual Substructures

In cloud computing, virtual substructures are infrastructure-level objects. The effective objects give sources to end users openly. Virtual networks and virtual machines (VMs) sometimes represent the effective objects. However, the side-channel outbreaks can portend the Virtual Machines. Additionally, different assaults like malware will attack the border Virtual Machines (VMs).

Security of Identity

To guard the user's secrecy, the subtle data in recovery should establish the consumer's uniqueness and therefore the characteristic data can similarly the offensive objective. Therefore the privacy conserving in knowledge extraction and distinctive private data should be secure, protocols or the trustworthy third party may be accepted to unravel the problem.

Server Accessibility

Several shoppers' usage the cloud to store private information or information, once various end users demand or regain at a similar, typically this may harm network jamming. Throughout the paper, the author tends to review the secrecy protecting cloud information recovery systems and supply an appraisal of them with relation to the fundamental ethics of secrecy secured and search [7]

The main contributions of the paper are as follows:

- The system consistently develop a new safe quest protocol, which not only enables the cloud server to operate safe ranked keyword pursuit without understanding the physical information of both trapdoors and keywords but also grant data owners to encrypt keywords with self-chosen keys
- The system proposes a Preservative Demand and Secrecy Conserving Purpose family which confess information holders to prevent the security of related grooves by various purposes rendering to the reference, though granting the cloud server to abundant the files exactly.

IIOAB JOURNAL
ISSN: 0976-3104

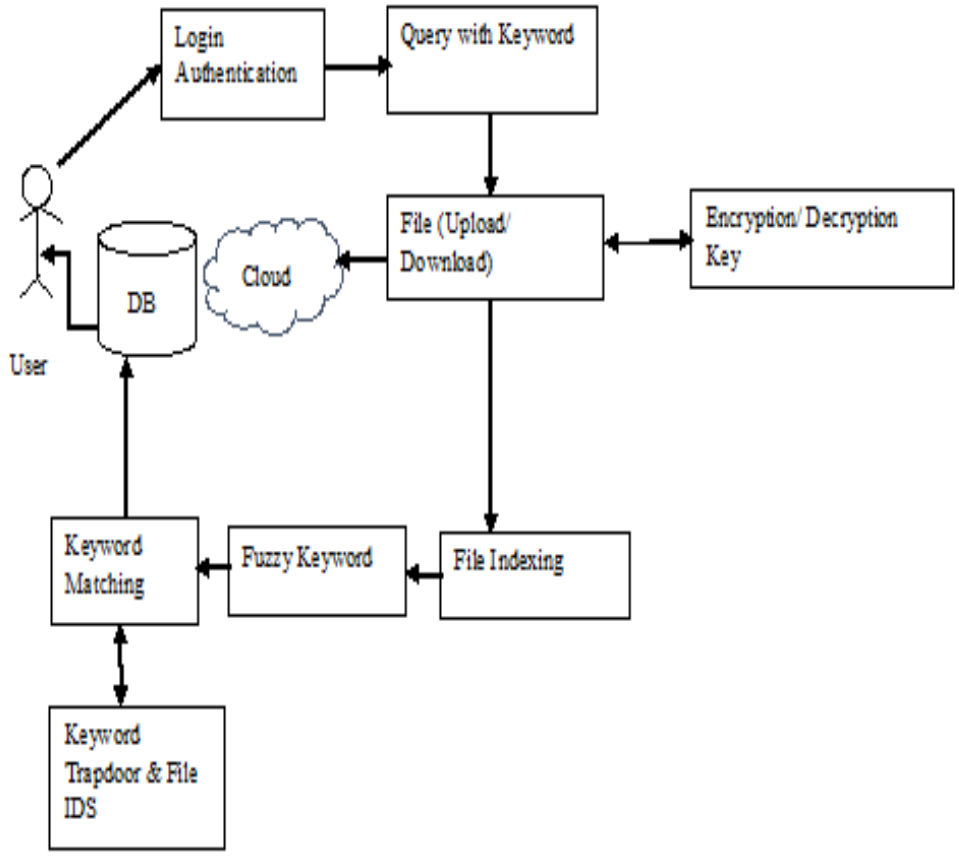

Fig. 1: System architecture

Modules

Algorithm use to Implement Fuzzy Keyword Search over Encrypted Data in Cloud Computing

1. Login- Data Owner Authentication
2. Data owner upload file using multiple fuzzy keyword
3. Encrypted file upload on cloud with keywords and upload Date-Time.
4. Data owner view user request- Accept or Delete request,
5. Data owner view uploaded files- File Upload Date-Time, File size, Total time to upload a file, Delete or Download own files
6. Login- Data User Authentication
7. Data user search file using multiple fuzzy keyword and also Search by Date-Time of uploaded file.
8. System shows the minimum search time with file information like file size, File uploaded, Date-Time
9. Files view in a top ranking format using TFIDF.
10. Data user send the request to data owner for download the file
11. When data owner accept the request then data user download that file which is in decrypted format.

Mathematical Equations use in the system implementation

I. Authentication-secure key creation: In the validation phase, user login to the system by providing his credentials. The system authenticates the user by verifying this powers. The secreted key generated to give the authenticated user. Algorithm- hash function and secret key generation.

II. Indexing: This is the second module of the proposed system. Indexing completed the uploaded and downloaded file. Indexing completed for file reference. Context-based indexing using Term Frequency and Inverse Document Frequency.

IIOAB JOURNAL
ISSN: 0976-3104

III. Encryption: Following are the few conditions which would be satisfied for encrypting keyword, first is data owner's needs to utilize their secret key for encryption. Secondly, the secreted key must be encrypted to different cipher text every time for the same keyword [7].

Given,
hth is the keyword of records holder Oi,
That is, wi; h
Encryption of wi; h is as follows:
wi;h = (gki;w • ro • H(wi;h), gki;---------- (1)
Where ro is a randomly created digit every period,
The equation will help to increase the safety of ˆwi; h
For understanding and simple explanation, let know
E′a =gki;w • ro • H(wi;h)
And
Eo = gki;w • ro .
The data holder transmits Ea′ and Eo to the cloud server of administration, and then this server will re-encrypt Ea' by using ka1 and ka2 secret key and finally gets Ea.
Ea = (Ea′ • gka1) ka2 ---------- (2)
Therefore ˆwi;h = (Ea, Eo).
ˆwi;h submitted to the server by administrative server. A reminder that the official servers simply do the calculation on encrypted data, the central server can't learn secret information from this encrypted data without knowing data owners secret key.

IV. Trapdoors calculation: The system must gratify following two conditions to make end user of data to create encoded keywords (trapdoors) conveniently, efficiently and securely [7]:

The data user doesn't require asking several information holders for secure keys to produce accesses.
Every time the created trapdoors must be changed for the same keyword. To meet that conditions, the generation of trapdoor performed in two steps: Firstly, the user of data produces trapdoor which based on users search keyword as well as random number. Assume a user of data needs to examine keyword wh′, so the system will encrypt files as follows:
T′ Wh = (gH (wh ′) • ru, gru) ---------- (3)
Where ru is a randomly created numeric for every phase. The system has seen while generating the trapdoor the secreted key of data owner is not needed. Furthermore, by using the random variable ru system should produce two trapdoors which are different.

V. Display Top-k file: The system must fulfill conditions given next for ranking the significance groove whereas maintaining its secrecy.

This purpose must save data order that supports cloud server for determining which data is extra appropriate to a particular keyword, affording to the encrypted importance scores. Unique data holders must have special purposes such that illuminating the coded data owner cost would not result in the leak of encrypted values of another data holders [7].

Ranking algorithm Apriori

The Apriori Algorithm: it is a basic algorithm for common mining itemsets and Boolean association rules.

Key Concepts: Common Itemsets: The sets of an item which has minimum support (denoted by Li for ith-Itemset).

Apriori Property: Any subset of the constant itemset must be usual.

Join Operation: To find L, k, a set of candidate k-itemsets has generated by entering Lk-1 with itself.

RESULTS

In the paper, the system further calculates the significance score of a keyword to a file. The keyword frequency and file size of the data set can be gotten. MRSE grieves a quadratic evolution with the size of keyword glossary rises when PRMSM and SRMSM are impervious to the measure of the keyword vocabulary for index structure.

The system observes that PRMSM spends a little more time than SRMSM on trapdoor generation; the reason is that PRMSM presents an extra variable to ensure the randomness of trapdoors. Fig shows the how to increases no of files size on keyword similarity and TFIDF trapdoor varies rapidly, jaccar keyword similarity shows decreases slowly. As the system can see from [Fig. 2], the extra keywords are present in the cloud storage. The extra time needed for combining process.

IIOAB JOURNAL
ISSN: 0976-3104

Keyword Similarity

Table-1 and Fig. 2 show the Keyword similarity match using Jaccard Algorithm and TFIDF Algorithm. Jaccard Algorithm is better than TFIDF Algorithm because Jaccard Algorithm search keyword similarity fast than TFIDF:

Table 1: Keyword Similarity

No of Files	Using Jaccard Algorithm	Using TFIDF Algorithm
1	0.4	2.4
2	0.2	1.3
3	0.8	3.6
4	0.6	1.7
5	0.3	2.5

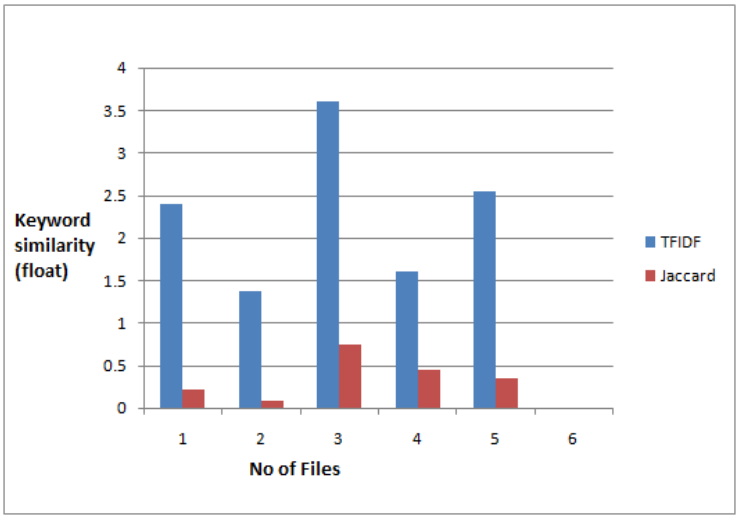

Fig. 2: Keyword similarity using Jaccard and TFIDF Algorithm

Searching Time Difference

Table-2 and Fig. 3 show the Search time using by keyword and date-time. The file search fast using date-time than search by the keyword.

Table 2: Time Difference by Keyword and Date

No of Files	By Keyword	By Date-Time
1	87	95
2	83	54
3	64	39
4	67	45
5	78	69

CONCLUSION

Implementing the multi-owner theme as compared to the only owner has many problems. Very first the owner of the data has to keep online in single owner theme for generating entrances (Encrypted keywords) which can have an impression of usability and suppleness of search system. The second issue is performance arts appropriate, capable and safe looking for encoded knowledge by entirely different secret keys.

IIOAB JOURNAL
ISSN: 0976-3104

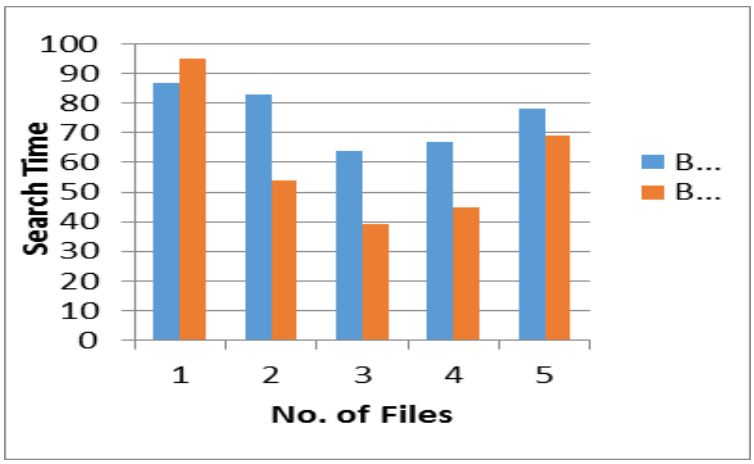

Fig 3: Searching time difference by Keyword and by date-time

CONFLICT OF INTEREST
There is no conflict of interest.

ACKNOWLEDGEMENTS
To prepare proposed methodology paper on "Multiple Fuzzy Keyword Search Over Encrypted Data Using Date And Time " has been prepared by Anagha Ramnath Kadve and Prof. Dr. S.B.Vanjale. Author would like to thank my faculty as well as my whole department, parents, friends for their support. Author has obtained a lot of knowledge during the preparation of this document.

FINANCIAL DISCLOSURE
None

REFERENCES

[1] Wang YJ, Zhao J, Shen J, Li KC. [2016] Fine-grained searchable encryption in multi-user setting, Soft Computing, 21(20): 6201–6212.
[2] Arthi G, et.al. [2016] Efficient search of Data in Cloud Computing using Cumulative Key, IJSTE- International Journal of Science Technology & Engineering, 2(9):299-302.
[3] Shen J. et.al. [2015] Privacy Preserving Search Schemes over Encrypted Cloud Data: A Comparative Survey,2015 First International Conference on Computational Intelligence Theory, Systems and Applications. Doi: 10.1109/CCITSA.2015.46
[4] Zhang W, et.al. [2014] Secure Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing, 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Doi: 10.1109/DSN.2014.36
[5] Zhang W, Lin Y. [2015] Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing, Member, IEEE Transactions on Cloud Computing, Doi: 10.1109/TCC.2015.2481389
[6] Kadve AR, Vanjale SB. [2016] A Survey on Multi-Keyword Search Tracking Based On Privacy Preserving in Cloud Computing, International Journal of Control Theory and Applications, 9 (44): 463-468.
[7] Kadve AR, Vanjale SB. [2017] Multiple Fuzzy Keyword Search over Encrypted Data Using Date and Time, JETIR, 4(11):85-89
[8] Kumar SN, Vajpayee A. [2016] A Survey on Secure Cloud: Security and Privacy in Cloud Computing, American Journal of Systems and Software, , 4(1):14-26
[9] Hashizume K, et al. [2013] An analysis of security issues for cloud computing, Journal of Internet Services and Applications, 4(5): Doi:10.1186/1869-0238-4-5
[10] Khatri SK et al. [2013] Multi-Tenant Engineering Architecture in SaaS, IJCA Special Issue on International Conference on Reliability, Infocom Technology and Optimization ICRITO:45-49
[11] Khana N, Al-Yasirib A, [2016] Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. Procedia Computer Science, 94, 485-490.
[12] Subashini SN, Kavitha V. [2011] A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1):1-11.