ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

EFFICIENT SEARCHING WITH MULTIPLE KEYWORD OVER ENCRYPTED CLOUD DATA BY BLIND STORAGE

K.Santhi*[1], M.Deepa[2], M.Lawanya Shri[3], M. B. Benjula Anbu Malar[4]
[1,2,3,4] School of Information Technology VIT University, TamilNadu, India.
Email: ksanthi@vit.ac.in

Received on 28-07-2016 Accepted on 01-09-2016

Abstract

In Cloud Computing, a basic application is to source the knowledge to outside cloud servers for climbable knowledge storage. The outsourced knowledge, however, have to be compelled to be encrypted because of the privacy and secrecy issues of their owner. This leads to the well-known difficulties on the accurate search over the encrypted cloud knowledge. To tackle this issue, during this paper, we have a tendency to develop the searchable coding for multi-keyword hierarchal search above the storage knowledge. The main aim of this paper is to preserve the outsourced data in cloud through gateway encryption and blind storage, and to implement multi keyword ranked search over the encrypts data in a safe way by NLP method without has download and decrypts the entire group of member file contents.

Keywords: RSA algorithm, Base64 algorithm, Cloud, NLP Technique.

1. Introduction

Research in Cloud Computing is getting plenty of interest from each educational and industrial world. In cloud computing, users will foundation their calculation and storage to servers (also known as clouds) mistreatment web. Clouds will offer many sorts of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon’s EC2, Eucalyptus, Nimbus), and platform to support developers write applications (e.g., Amazon’s S3, Windows Azure). Abundant of the information grip on in clouds is particularly aware, for instance, medical records and social networks. Security and privacy square measure therefore vital problems in cloud computing. In one hand, the user ought to evidence itself before initiate any group battle, and the opposed hand, it should be ensured that the cloud doesn't tinker with the information that's outsourced. In order to lo k in cloud, some necessities is required, search over encrypted information ought to maintain the subsequent 3 functions. First, the searchable secret writing schemes ought to maintain multi-keyword search, and supply a similar user expertise as looking in Google search with totally different keywords; single-keyword search is much from satisfactory by solely returning terribly restricted and inaccurate search results. Second, to quickly determine most related results, the look for user would usually like cloud servers to kind the came back search ends up in a connection-based classify hierarchal by the importance of the search request to the documents.

In existing system encryption of the documents are done in cloud server. All the files uploaded by the user are encrypted in cloud and stored in fixed memory locations. Hence Multi keyword search is not possible on the encrypted cloud data. In order to create a search, the existing system downloads all the encrypted files and then decrypt for content based searching which is the conventional way to search.

In SSE-searchable symmetric encryption schemes, large sum of papers, search results should be reclaim in an order of the relevancy with the searched keywords using TF-IDF method.

In Proposed system, we introduced an efficient and reliable methodology for search over encrypts data which is spited in to multiple blocks and then stored in blind storage. Here the encrypts multi keyword search pre compute the resulting search data for the input query from users through Natural language processing Technique which is implemented on gateway (client side) on user file upload.

Hence the matching documents which is pre compute the before searching the encrypted cloud contents are retrieved from cloud. Here we does not pull all the encrypted data's from cloud for probing, which is time consuming and hopeless. The matching documents memory locations on blind storage are retrieved from the serializable objects which is stored in the gateway. User can download the resulting documents after getting the keys from the group owner. Asymmetric kind of encryption for key re-encryption and is more secured.

2. Literature Review

[1] Bing Wang, Shucheng Yu Empowering watchword seeks specifically over scrambled information is an alluring method for compelling use of encoded information outsourced to the cloud. Existing arrangements give multi keyword precise inquiry that does not endure watchword spelling mistake, or single catchphrase fluffy hunt that endures grammatical errors to certain degree. The ebb and flow fluffy inquiry plans depend on building an extended record that spreads conceivable catchphrase incorrect spelling, which prompt essentially bigger file document size and higher pursuit unpredictability. In this paper, we propose a novel multi keyword fluffy hunt plan by misusing the area touchy hashing

method. Our proposed plan accomplishes fluffy coordinating through algorithmic outline as opposed to growing the list document. It likewise wipes out the need of a predefined word reference and adequately underpins various watchword fluffy inquiry without expanding the list or pursuit intricacy. Broad examination and trials on certifiable information demonstrate that our proposed plan is secure, productive and exact. To the best of our insight, this is the main work that accomplishes multi-catchphrase fluffy inquiry over scrambled cloud information.

[2] Muhammad Naveed, Manoj Prabhakaran**,** Dynamic Searchable Symmetric Encryption permits a customer to store a dynamic accumulation of scrambled records with a server, and later rapidly complete catchphrase seeks on these encoded reports, while uncovering negligible data to the server.

In this paper we show another element SSE conspire that is more straightforward and more effective than existing plans while uncovering less data to the server than earlier plans, accomplishing completely versatile security against fair yet inquisitive servers.

We executed a model of our plan and exhibited its productivity on datasets from earlier work.

Aside from its solid effectiveness, our plan is additionally less difficult: specifically, it doesn't require the server to bolster any operation other than transfer and download of information. In this way the server in our plan can be constructing exclusively with respect to a distributed storage administration, as opposed to a cloud calculation administration too, as in earlier work.

In building our dynamic SSE plan, we present another primitive called Blind Storage, which permits a customer to store an arrangement of records on a remote server in a manner that the server does not figure out what number of documents are put away, or the lengths of the individual documents; as every document is recovered, the server finds out about its presence (and can see the same document being downloaded along these lines), however the record's name and substance are not uncovered.

This is a primitive with a few applications other than SSE, and is of free hobby.

[3]Qin Liu, Chiu C.Distributed computing as a rising innovation pattern is relied upon to reshape the advances in data innovation. In this paper, we address two crucial issues in a cloud situation protection and effectiveness. We first survey a private catchphrase based document recovery plan proposed by Ostrovsky. At that point, taking into account a conglomeration and dissemination layer (ADL), we introduce a plan, termed productive data recovery for positioned

question (EIRQ), to advance diminish questioning expenses acquired in the cloud. Questions are grouped into different positions, where a higher located inquiry can improve a higher rate of coordinated documents. Broad assessments have been directed on an expository model to look at the adequacy of our plan.

3. System Architecture

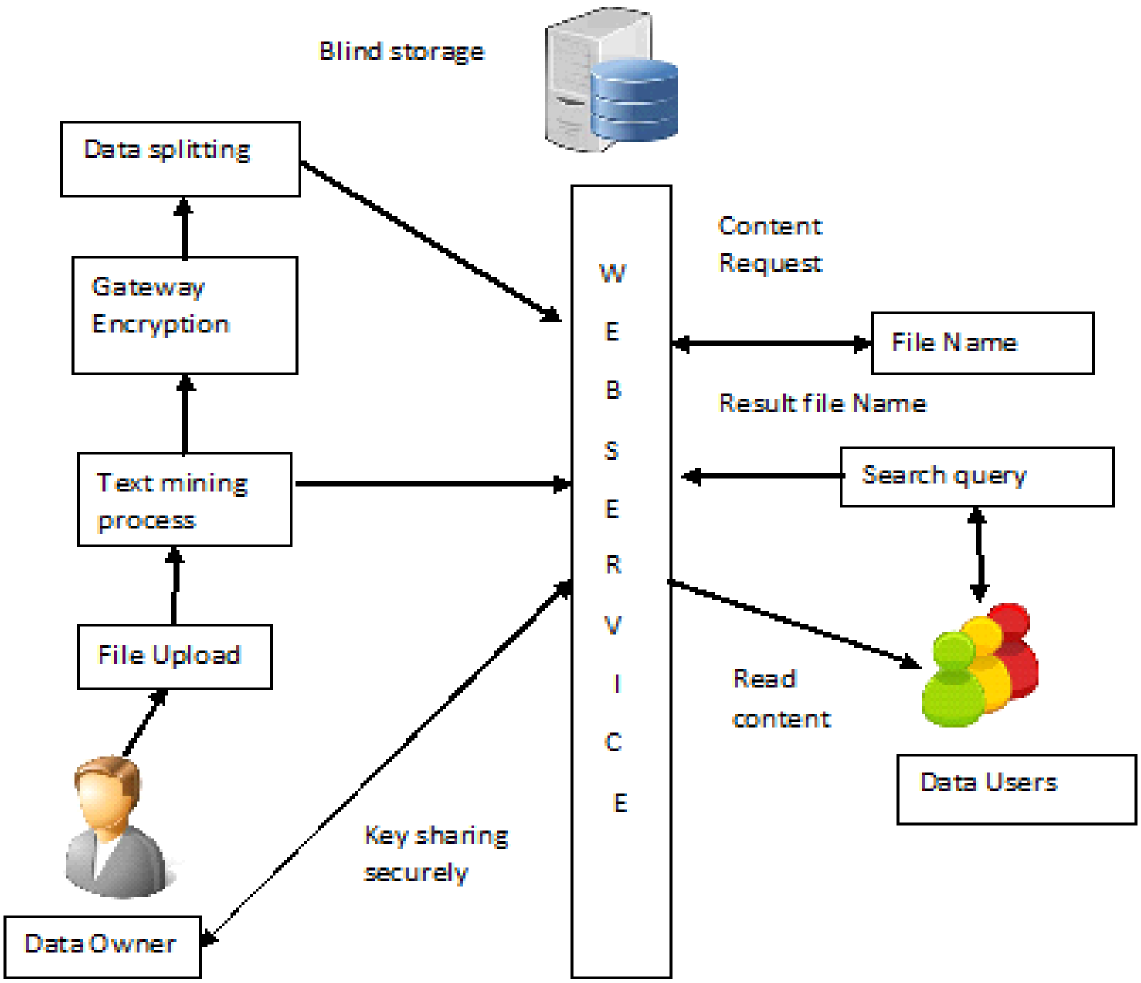


Fig 1: System Architecture.

4. Algorithms

1. Base 64

Example 1: Input data, 1 byte, "A". Encoded output, 4 characters, "QQ=="

Input Data A

Input Bits 01000001

Padding 01000001 00000000 00000000

\ \ \

```
Bit Groups   010000 010000 000000 000000

Mapping         Q     Q     A     A

Overriding      Q     Q     =     =
```

Example 2: Input data, 2 bytes, "AB". Encoded output, 4 characters, "QUI="

```
Input Data        A       B

Input Bits   01000001 01000010

Padding      01000001 01000010 00000000

             \     \     \

Bit Groups   010000 010100 001000 000000

Mapping         Q     U     I     A

Overriding      Q     U     I     =
```

Example 3: Input data, 3 bytes, "ABC". Encoded output, 4 characters, "QUJD"

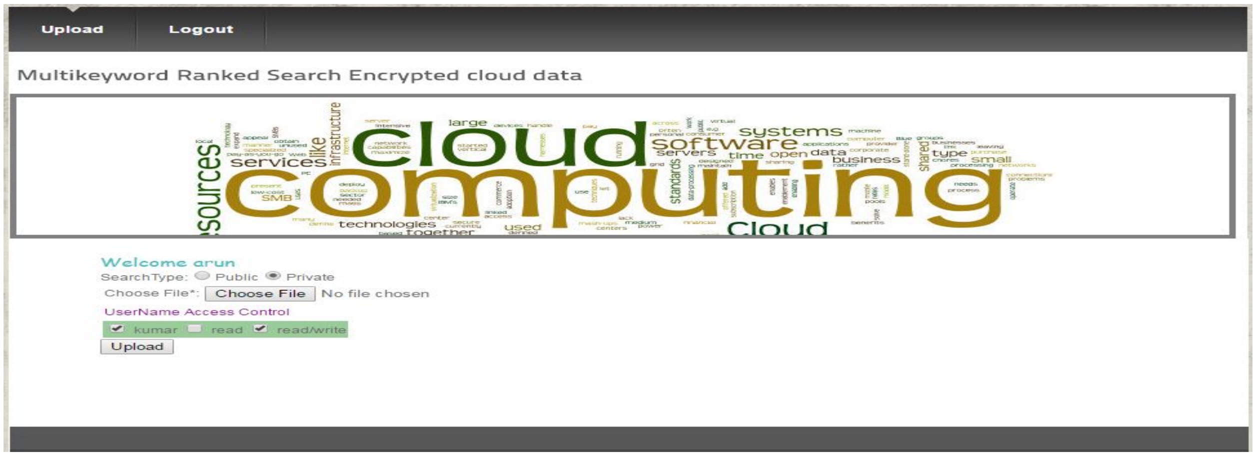
```
Input Data        A       B       C

Input Bits   01000001 01000010 01000011

             \     \     \

Bit Groups   010000 010100 001001 000011

Mapping         Q     U     J     D
```

RSA Algorithm

1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (phi) φ = (p-1)(q-1).
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi).
5. The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d. Other times we might write the key pair as ((N, e), d).]

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

5. Implementation



Multikeyword Ranked Search Encrypted cloud data

Welcome arun

SearchType: ○ Public ● Private

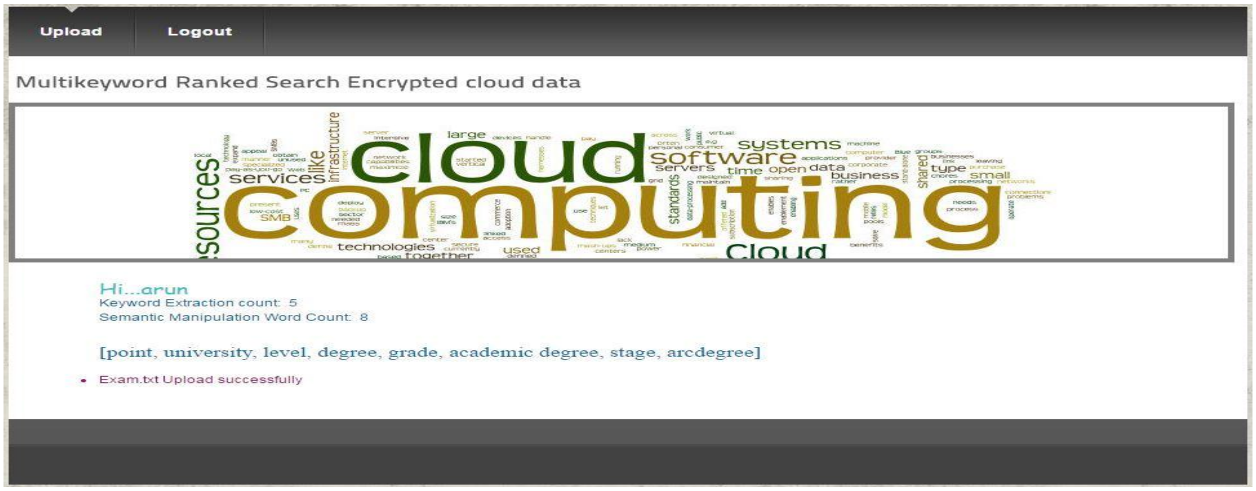
Choose File*: Choose File No file chosen

UserName Access Control

☑ kumar □ read ☑ read/write

Upload

Fig 2: Uploading a file.



Multikeyword Ranked Search Encrypted cloud data

Hi...arun

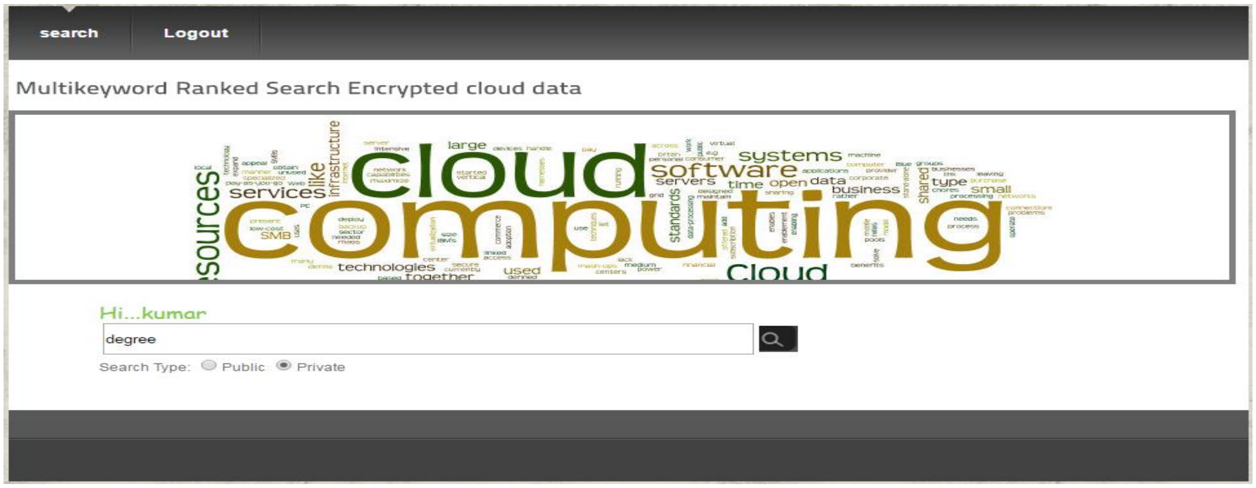
Keyword Extraction count: 5

Semantic Manipulation Word Count: 8

[point, university, level, degree, grade, academic degree, stage, arcdegree]

- Exam.txt Upload successfully

Fig: 3 Keyword Extractions.



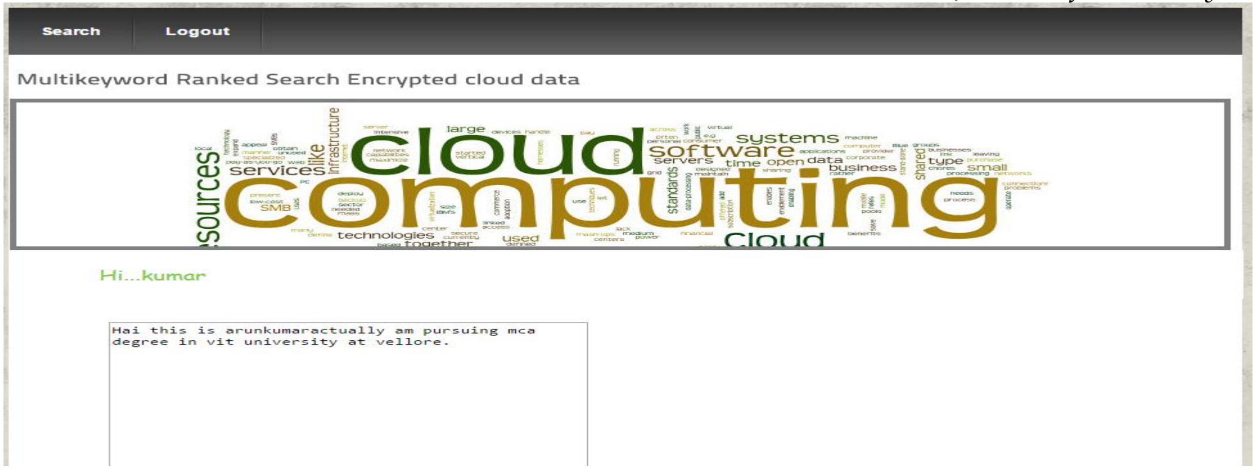
Multikeyword Ranked Search Encrypted cloud data

Hi...kumar

degree

Search Type: ○ Public ● Private

Fig 4: Searching file.



Multikeyword Ranked Search Encrypted cloud data

Hi...kumar

Hai this is arunkumaractually am pursuing mca degree in vit university at vellore.

Fig: 5. Decrypted Content.

6. Conclusion

Hence we developed an efficient search in multi keyword through blind storage which enable accurate, well-organized and secure search over encrypted data. Privacy is preserved for data in cloud while storing in blind Storage, and also achieved access control for each user.

References

1. B.Wang, S.Yu,W. Lou, andY. T. Hou, ``Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in *Proc. IEEE INFOCOM*, Apr./May 2014, pp. 2112_2120.
2. Muhammad Naveed, Manoj Prabhakaran, Carl A. Gunter,” Dynamic Searchable Encryption via Blind Storage”, 2015.
3. Qin Liu, Chiu C,” Efficient Information Retrieval for Ranked Queries in Cost-Effective Cloud Environments”, International Conference on Computer Communications: Mini-Conference IEEE,2012.
4. M. M. E. A. Mahmoud and X. Shen, ``A cloud-based scheme for protectingsource-location privacy against hotspot-locating attack in wirelesssensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10,pp. 1805_1818, Oct. 2012.
5. Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo, ``Exploiting geo distributed clouds for a e-health monitoring system with minimum servicedelay and privacy preservation," *IEEE J. Biomed. Health Inform.*, vol. 18,no. 2, pp. 430_439, Mar. 2014.

6. H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, ``An SMDP-based service model for inter domain resource allocation in mobile cloud networks,"*IEEE Trans. Veh. Technol.*, vol. 61, no. 5, pp. 2222_2232,Jun. 2012.

7. H. Li, Y. Dai, L. Tian, and H. Yang, ``Identity-based authenticationfor cloud computing," in *Cloud Computing*. Berlin, Germany:Springer-Verlag, 2009, pp. 157_166.

8. W. Sun, *et al.*, ``Privacy-preserving multi-keyword text search in the cloudsupporting similarity-based ranking," in *Proc. 8th ACM SIGSAC Symp.Inf., Comput. Commun. Secur.*, 2013, pp. 71_82.

9. Lawanya Shri, M., Subha, S.," An implementation of E-learning system in private cloud", International Journal of Engineering and Technology, 2013.

10. K.Santhi, M.Deepa, M.Lawanya Shri, M. B. Benjula Anbu Malar,” Approach for Secure Authorized eduplication using Hybrid Cloud” IJAER ,2016.

Corresponding Author:

K.Santhi*

Email: *ksanthi@vit.ac.in*