International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Preserving Encryption Based Data Search

A.C.Southarraj[1], P. Ushman ali[2]
[1]*Assistant professor, Sri krishna arts and science college coimbatore-8.*
[2]*IV M.Sc. Software Systems, Sri krishna arts and science college coimbatore-8.*

Abstract:Computers have become an essential part of organizational information processing because of the power of technology and the volume of data to be processed. Through the technology, the manual process, defects and time consumption can be reduced. That's in all the area of business, computer technology is widely been implemented. Hence the inception of computers had a great role in reducing large tasks to simpler one
Keywords: Servers, Encryption, Indexes, cloud computing, keyword search

I. INTRODUCTION

Many techniques are developed so far now to search encrypted data over cloud such as searchable encryption, PEKS, OPE etc. To Searchable encryption is a technique to search encrypted cloud over the cloud. There are two types of searchable encryption one is searchable public key encryption abbreviated as SSE and searchable symmetric encryption abbreviated as SPE.

A. Distributed file systems for mobile clouds

Moreover, many studies about the storage systems for cloud environments that enable mobile client devices have been published. A new mobile distributed file system called mobiles has been proposed and implemented in which aims to reduce computing in mobile devices by transferring computing requirements to servers. Hyrax, which is a infrastructure derived from Hadoop support cloud computing on mobile devices. But Hadoops designed for general distributed computing, and the client machines are assumed to be traditional computers. In short, neither of related work targets at the clouds that have certain resource-limited client machines, for yielding attractive performance enhancements.

B. Searching Module

In practice, to realize effective data retrieval on large number of documents, it is necessary to perform relevance ranking on the results. Ranked search can also inefficiently reduce network traffic by sending back only the most relevant data. In ranked search, the ranking function plays an important role in calculating the relevance between files and the given searching query. The most popular relevance score is defined based on the model of, where term frequency is the number of times a term (keyword) appears in a file and inverse document frequency (IDF) is the ratio of the total number of files to the number of files containing the term. There are many variations of -based ranking functions, and in [16], the following one is adopted. *Score* Herein, *w* denotes the keyword and *denotes* the TF of term *w* in file *denotes* IDF whereis the number of files that contain term *w* and *is* the total number of documents in the collection; andis the number of indexed terms containing in file the length

C. Cryptography Modul

The order preserving property means that if the plaintexts have such a relationship as then the corresponding ciphertexts and satisfy. Random order-preserving function (ROPF), bucket is determined by a binary search based on a random HGD sampler. In, the procedure of binary search is described as Algorithm 1, where is a random coin generator.

D. Encryption and Decryption Module

File bench which allows generating. A large variety of workloads to assess the performance of storage systems. Besides, File bench is quite flexible and enables to minutely specify a collection of applications, such as mail, web, file, and database servers. We chose File bench as one of benchmarks, as it has been widely used to evaluate file systems by emulating a variety of several server-like applications. I Ozone, which is a micro-benchmark that evaluates the performance of a file system by employing some collection odds with regular patterns, such as sequential, random, reverse order, and stride. That is why we utilized it to measure read data throughput of the file systems with various prefetching schemes, when the workload has different access patterns.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

E. File Sharing Module

Applications of privacy preserving keyword search, if a determinist is used to encrypt relevance scores, the ciphertexts will share exactly the same distribution as its plain counterpart, by which the server can specify the keywords. Therefore, Wang et al. modified the original OPE to a probabilistic one, called "One-to-Many OPE".

F. Problem Description

The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk, the cloud server may leak data information to unauthorized entities or even be hacked. It follows network traffic, which is abslutely undesirable in today's pay-as-you-use cloud paradigm. In short, lacking of effective
mechanisms to ensure the file retrieval accuracy is a significant drawback of existing searchable encryption schemes in the context of Cloud Computing. Nonetheless, the state of the art in infortion retrieval (IR) community has already been utilizing various scoring mechanisms to quantify and rank order the relevance of files in response to any given search query. Our contribution can be summarized as follows
Thorough security analysis shows that our ranked searchable symmetric encryption scheme indeed enjoys "as strong-as-possible" security guarantee compared to previous searchable symmetric encryption (SSE) schemes.
Extensive experimental results demonstrate the effectiveness and efficiency of the proposed solution.

II. PROPOSED SYSTEM

To meet the effective data retrieval, the result must be returned based on some ranking criteria based on one to many order preserving encryption(OPE). It also improves system performance.

A. The system architecture involves five special Models:

1) The Cloud Holder: A person or the company, they are the Owner of the cloud.
2) The Cloud superintendent: The responsible person, he has the right to controls over all the operations of the cloud server.
3) The cloud server: It provides huge storage space and remote access to all its users
4) The data Holder: Owner of the data, it may be a person or company they may have collection of data.
5) The data user: A user or the customer, they can search, view the data.
6) Hackers: Here Hackers are the unauthorized persons their main job is to hack the data. The advantages of this proposed system methods are, To provide a data privacy and data security, Decrease the computational overhead, Provide accurate ranked search result, Increase the communication capacity, Increase the performance by decreasing network traffic to improve the system usability.

B. Block Diagram

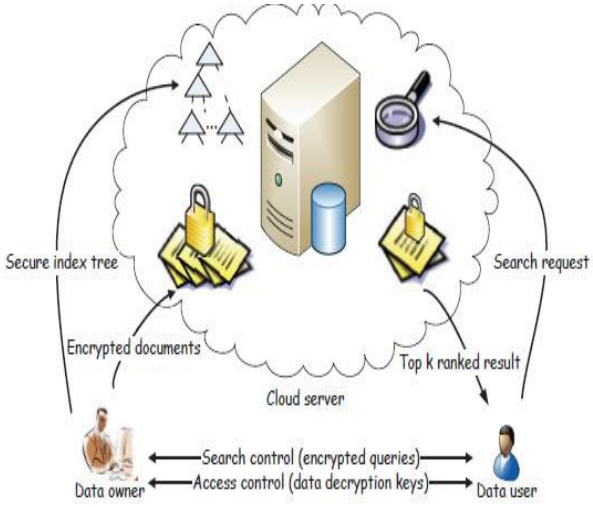


Figure 4.1: Block diagram of retrieval over encrypted cloud data

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

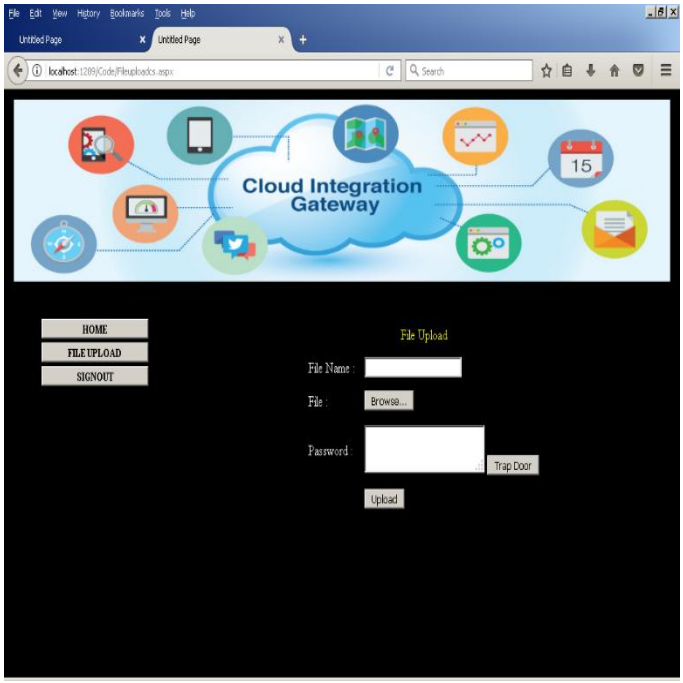
III. RESULT ANALYSIS

In this paper we designed the experiment using simulator tool clouds, the analysis result solves the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud computing. our ranked search mechanism was also investigated, including the efficient support of relevance score the authentication of ranked search results, and the reversibility of our proposed one-to-many order-preserving mapping technique. The file upload module process, when a data owner desires to outsource and share a file with some group of users, the data owner encrypts the file first and then it is to be uploaded under a specified attribute set. Based on the system model provided we attempt to define an One –to-many OPE model to map the search key words and give priority for decrypt files through our access control system.

A. Trapdoor Algorithm

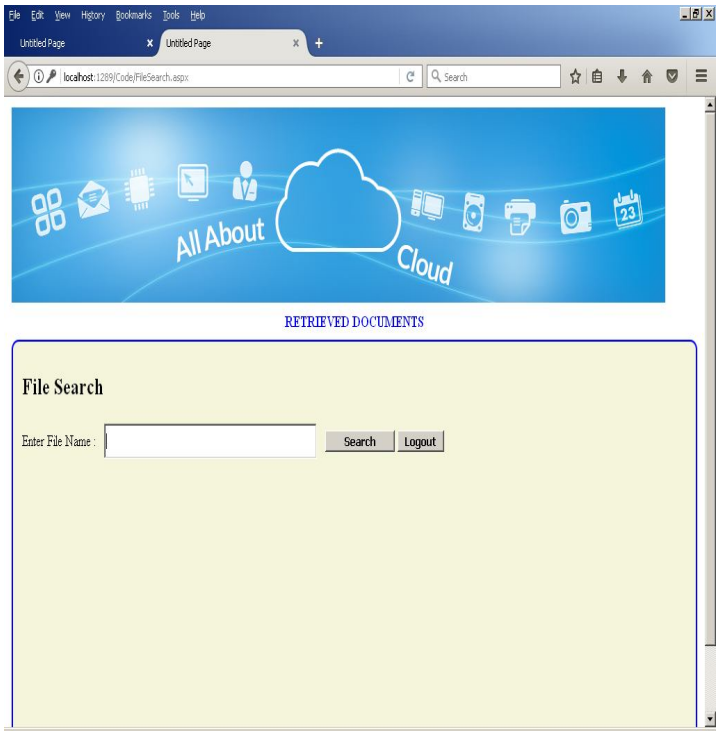
```
begin
    len ⟵ (end−start)+1                    /* The list length */
    if len = 1 then
        σ ⟵ σList[start]
        {μ_k}_{1≤k≤s} ⟵ μList[start][k]
        ê(σ, g) =? ê(∏_{(j,r_j)∈Q} H(ID_F||BN_j||BV_j)^{r_j} · ∏_{k=1}^{s} u_k^{μ_k}, y)
        if NOT verified then
            invalidList.Add(start)
        end
    else
        σ ⟵ ∏_{i=1}^{len} σList[start + i − 1]
        {μ_ik}_{1≤i≤len, 1<k<s} ⟵ μList[start+i − 1][k]
        ê(σ, g) =?
        ê(∏_{(j,r_j)∈Q} H(ID_F||BN_j||BV_j)^{r_j |^{len}, ∏_{k=1}^{s} u_k^{Σ_{i=1}^{len} μ_ik}, y)
        if NOT verified then
            /* work with the left and right halves of
            σ List and μList */
            mid ⟵ ⌊(start+end)/2⌋    /* List middle */
            BS(σ List, μList, start, mid)   /* Left part */
            BS(σ List, μList, mid+1, end)   /* Right */
        end
    end
end
```

B. File Upload

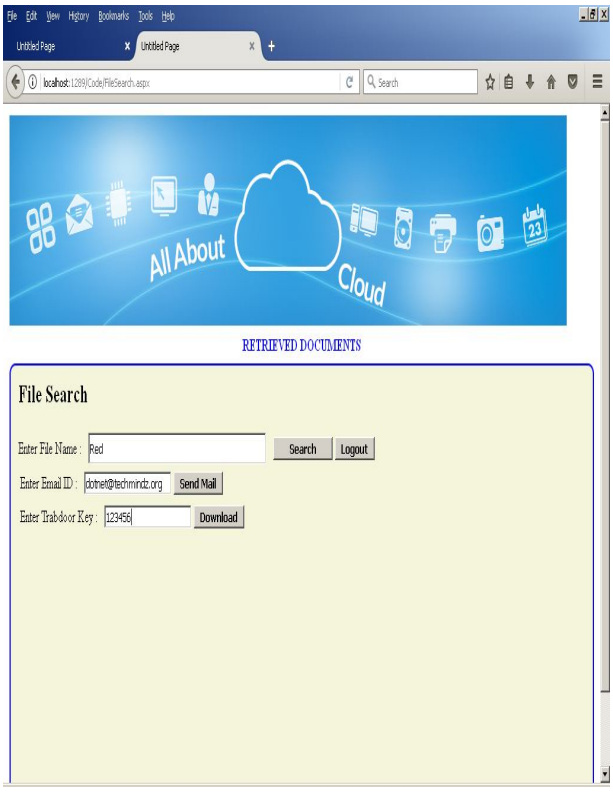


ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

C. Search Your Encrypted File

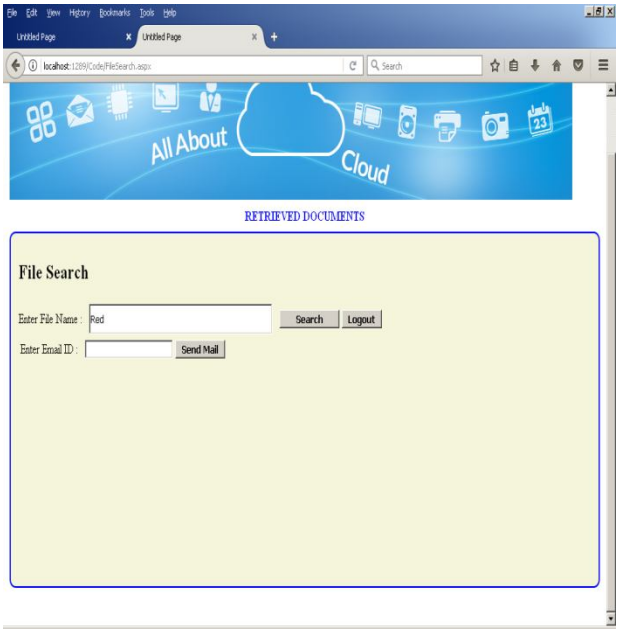


D. File Download



E. Enter Valid Email Id

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com



IV. CONCLUSION

In this paper we investigate efficient data retrieval from the cloud database. The demand for cloud computing increases day by day, consumers can store their data and can retrieve it since it is valuable and soothing process. The result shows that data can be retrieved faster by efficient multi keyword search from remotely stored encrypted data. Future work, elaborates these ideas to design secure methods of probabilistic OPE and schemes for search in encrypted data.

A. Encrypted Documents

REFERENCES

[1] Elias Awasthi," System Analysis and Design", Sixth Edition, Tata McGraw Hill Publication,2003
[2] Ramachandran, "Computer Aided Design", Third Edition, Air Walk Publication, 2003
[3] Richard Fairley, "Software Engineering Concepts", Second Edition, Tata McGraw Hill Publication,1997