Combined Keyword Search over Encrypted Cloud Data Providing Security and Confidentiality

[1]Y.Srikanth
M.Tech (II CSE)
MITS, Madanapalle, A.P,India

[2]M.Veeresh Babu
Assistant professor (CSE Dept.)
MITS, Madanapalle, A.P, India

[3]P.Narasimhulu
Associate professor (CSE Dept.)
MITS, Madanapalle, A.P, India

ABSTRACT
In this paper proposes multi-user searchable encryption with the help of order preserve encryption for providing efficient encrypted data. when proposed these constructions it formally defines the multiuser settings for ranked keyword search by using searchable symmetric encryption and order preserve symmetric encryption. Consider a dataowner is the administrator who can uploads the files before encrypted into the outsourced cloud server. These files are encrypted in the cloud server which can be shown as an index file for users. The users can login and download the files what ever the document need from the cloud server at the same time so many users can download the files with efiicient and security manner.

Keywords
Searchable symmetric encryption, multiuser, ranked keyword, order preserving encryption

1. INTRODUCTION

Cloud Computing means a remote server that access through the internet which helps in business applications and functionality along with the usage of computer software. A few of the cloud services and appliance in the internet modem is available from the computer. Cloud helps for logging in to the computer applications as a desire with Cloud Computing, one can helpful for use of web services, sales force or office automation programs, spam filtering, data storage services one simply logs into our computer applications. This technology prevents wastages in finance, because it saves money that customer spend on other cable services for which customer need to pay monthly annual subscriptions[3]. The business people are assisted with better way activities and stop any advanced technological disasters such as the failure of data, system break down.

There are three service models are present in cloud. They are

A. Software as a service (SaaS)

Software as a service (SaaS)—cloud based applications are available from various user devices through a slim client interface such as web browser (eg; email).

B. Platform as a service (PaaS)

Platform as a service provides a cloud-based background with everything required to support the applications are created by using programming languages like servers, programming languages, or database etc;

C. Infrastructure as a service (IaaS)

Infrastructure as a service provides companies with computing resources including servers, networking, deployed applications, and data center space on a pay-per-use basis.

2. BACKGROUND AND RELATED WORK

Now a days in internet, digital information becomes more and more valuable information is stored in cloud to protect this data from virus, hacking. More computers are linked together when the data is downloaded from cloud these files can be exposed to dangerous of being destroyed. Cloud Computing is the remotely store their data into the cloud the on-demand high-quality applications and services from a shared pool of configurable computing resources. The benefits of the new computing model include but are not limited to: relief of the trouble for storage administration, universal data access with independent geological locations, and avoidance of high expenditure on hardware mechanism, software, etc.

Ranked search greatly improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus a practical deployment of privacy-preserving data hosting services in the framework of cloud computing. An achieved design goals on both system protection and usability, propose bring mutually the advance of both crypto and IR society to design the ranked searchable symmetric encryption scheme, to strengthen "as-strong as-possible" security guarantee. As directly outsourcing relevance scores will drips a lot of sensitive information against the keyword privacy, To integrate a recent crypto primary order preserving symmetric encryption (OPSE) and properly modify it to develop one-to-many order-preserving mapping technique for our purpose to protect those sensitive weight information, whereas providing efficient ranked search functionalities.

The security of our ranked searchable encryption [1,2] is the same as previous SSE schemes, i.e., the user gets the ranked results with outletting cloud server gives additional information more than the access pattern and search pattern. This is achieved with the tradeoff of efficiency: namely, there should be a user wait for two round-trip time for each search request, or it may even lose the capability to perform top-k retrieval, resulting the unnecessary communication overhead. The analysis of these demerits will lead to our main result. It tightly pertained to recent work, though our focus is on secure

result ranking. It can be consider a searchable symmetric encryption that assures the non-adaptive security [1].

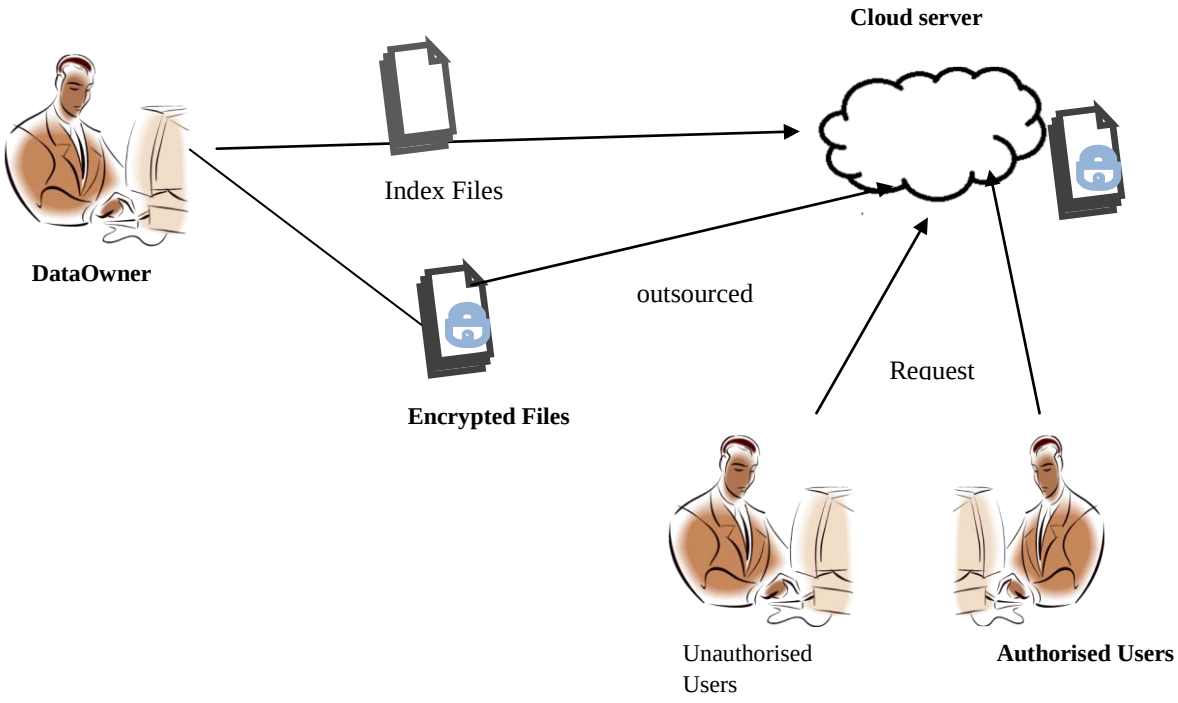

Fig.1 Architecture for Ranked Search Encrypted Cloud Data

- It provides outsourcing relevance score data leakages against keyword privacy.
- Systematic security analysis can be made "as-strong-as-possible" security guarantee compared to previous SSE schemes.
- It provides multi-user searchable encryption ranked keywords.

The Order-Preserving Symmetric Encryption can be used for giving highest priority to the keywords with each of them. Searchable symmetric encryption provides adaptive security settings for multi-user settings with the help of order preserving symmetric encryption against from data inefficiency and data leakages.

3. PROBLEM FORMULATION

Consider an encrypted cloud data service involving three different entities, as shown in Fig. 1: Data owner collects *n* data files *C*=(*F1*,*F2*,...,*Fn*) that he wants to outsource on the cloud server in encrypted for effective data utilization reasons. Before outsourcing, data owner will build a secure searchable index *I* from a set of *m* distinct keywords W=(*w1*,*w2*, ..., *wm*) extracted from the file collection *C*, and store both the index *I* and the encrypted file collection *C* on the cloud server. The previous work of SSE comes under non-adaptive settings can causes security weakening and looses its privacy also.

A. **Inverted index**: In information retrieval, inverted index (also referred to as postings file) is a widely used file structure that stores a list of mappings from keywords to the equivalent set of files that contain this keyword, allows full text search[1].

B. **Ranking function**: In information retrieval, a ranking function is used to analyze relevance scores of matching files to a given search request. The most widely used numerical measurement for estimate relevance score in the information retrieval community uses the TFxIDF rule, where term frequency (TF) is simply the no of times a given term or keyword (is uses them changes internally hereafter) appears within a organizer (to measure the importance of the term within the particular file), and inverse document frequency (IDF).

C. **DESIGN GOALS:** To enable ranked search for effective deployment of outsourced cloud data under the a fore mentioned model, our system design should concurrently achieve security and performance guarantees as follows[9]. Multi-user Ranked Search keyword: To design search method which allows multi-keyword query and provide result similarity ranking for efficient data can be retrieved, instead of returning undifferentiated results. Privacy-Preserving: To prevent cloud server additional information from dataset and index, to meet privacy requirements. Efficiency: These goals on functionalities and privacy should be achieved with low communication and computation overhead.

4. DEFINITIONS AND FRAME WORK FOR MULTIUSER SYSTEM:

Adversaries make their search queries without taking into account the trapdoors and search results of previous searches. Adversaries choose their queries as a functional previously obtained trapdoors and search outcomes. The previous work of SSE comes under non-adaptive setting. These definitions [8] only gives security guarantee for users that performs all their searches at once.

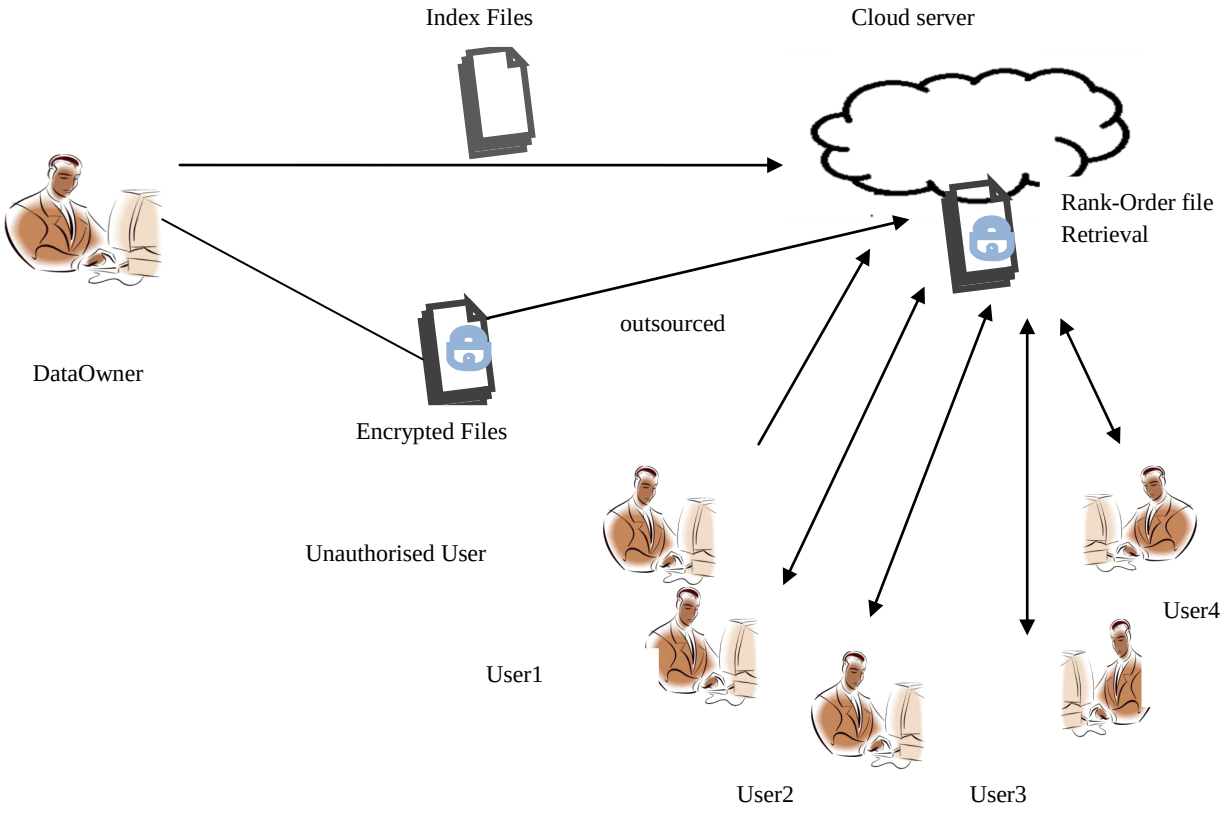

Fig.2 Multi-User Searchable Encryption by using Sse and OPSE

SSE construction requires the server to perform an amount of work that is linear in total number of documents in the collection.SSE construction secures against an adaptive adversary with efficient and provable secure in SSE schemes. Order preserving symmetric encryption supports multiuser system with efficient ranking search functions. We cannot target for strongest security level, we need to define the best possible security under the order preserving symmetric encryption as shown in the fig:2.

There are four different algorithms are used to provide efficient ranked keyword search. They are
KeyGen: which can generates the key for executable files.
BuildIndex: It generates the searchable index from unique keywords.

Trapdoor: It generates a secure trapdoor(which diverts from destination) corresponding its interested keyword.

SearchIndex:It shows which file we are searching.

KeyGen and BuildIndex comes under Setup phase and Trapdoor and SearchIndex[10] comes under Retrieval phase.

Setup phase: The data owner collect the data files and encrypt the files using OPS encryption and generate a secret key Then data owner generates the searchable key terms from the unique words which was extracted from file collection.

Retrieval phase: The data owner where the data can be stored in encrypted file format. In this phase data files can be searched where it is present.

$k_0 \leftarrow Gen(1^k)$:is a probabilistic key generation algorithm that is run by owner to set up the scheme. It takes as input a security parameter *k*, and output an owner secret key k_0.

$t \leftarrow Trpdr(K_u, w)$:is a deterministic algorithm run by user to generate a trapdoor for a keyword. It takes as input a user U's secret key K_u and a keyword *w*, and outputs a trapdoor t or the failure symbol $t \leftarrow Trpdr_{ku}(w)$.

$x \leftarrow search(sts, I, t)$:is a deterministic algorithm run by the server S to perform a search. It takes as input a server state st_s,an index I and trapdoor t, and outputs a set $x \in 2^{[1,n]} \cup \{\perp\}$, where $\perp$ denotes the failure symbol.

$k_u \leftarrow Add(k_0, st_0, U)$: is a probabilistic algorithm run by the owner to add a user. It takes as input the owner's secret key k_0 and state st_0 and a unique user id U and outputs U's secret key k_u.

Consider a multi-user searchable encryption scheme and some of the desirable security properties are followed by an efficient ranked keyword search which combines in the essence of a single-user SSE scheme with a broadcast

Cloud services	user1	user2	user3
Gmail	50	45	30
Facebook	45	60	30
Orkut	50	30	35
Twitter	45	30	29

encryption scheme. The secure index reveals no information about its content without valid trapdoors and it can only generates with a secret key. Data structure with a confidentiality guarantees can be used to safely index the contents of semantically secure cipher a keyword without decrypt entire document.

SSE achieved its full generality and optimal security on oblivious RAMS. This techniques of search query can be achieved without leaking any information to server, not even to access the document contains keywords. a strong privacy guarantee on a number of interactions for each read and write. Searchable encryption tries to achieve more efficient solution by weakening the privacy guarantees [5].

Order Preserve Encryption determines symmetric key encryption that preserves the order of plaintext. Cipher text leaks the order of information into plaintext. Search queries can be processed efficiently converted with DBMS techniques[7].

5. AUTHENTICATING MULTIUSER SYSTEM AND RESULTS:

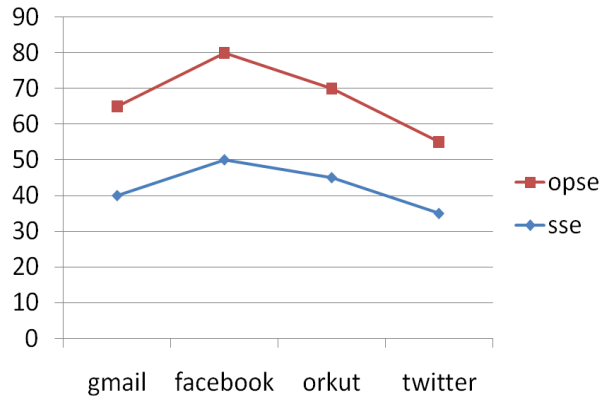

Fig.3 Comparision Between Opse and Sse

For multi-user system settings purpose we shown the efficiency between the SSE and OPSE in the form of graph. OPSE gives high performance when compare with SSE.

Below the table shows that how many users are using the cloud services and how much efficiency the cloud service works with the multi-user system. It is an example which explains about the efficiency of the cloud services by using adaptive security and order preserving symmetric encryption. The number of users in gmail, facebook, orkut, and twitter. These are the examples which are maintaining cloud server.

By using Searchable symmetric encryption we are providing multiuser settings which can be used to perform so many tasks at a time and by using order preserving symmetric encryption which is used to avoid data leakages and increases data efficiency with the encrypted files in the outsourced cloud server. Consider a dataowner is uploaded encrypted files which are highly confidential so many authorized data users access internet for downloading these files at a time from different web

TABLE: 1

Services and from different places also. It can be accessed very easily with high efficiency.

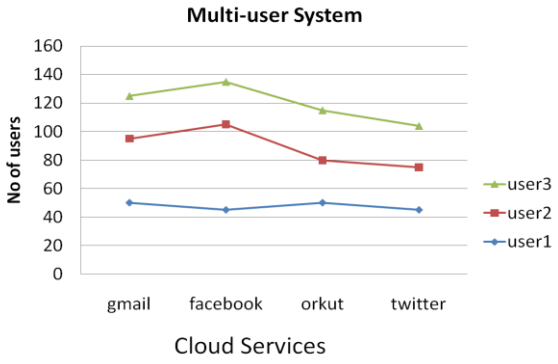

Fig.4 Efficiency of Multiuser System by using Opse and Adaptive Security in Graph

6. CONCLUSION

In this paper proposes multi-user searchable encryption with the help of order preserve encryption for providing efficient encrypted data. when proposes these constructions it formally defines the multiuser settings for ranked keyword search by using searchable symmetric encryption and order preserve symmetric encryption. As shown in the above results explains the efficiency in between the SSE and OPSE. This paper shown the Multi User searchable encryption which can be downloads by the users performing multi tasks through the internet at a time.

7. REFERENCES

[1] Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data Cong Wang,Student Member, IEEE, Ning Cao, Student Member, IEEE, Kui Ren,Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 8, AUGUST 2012.

[2] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud

Data,"Proc. IEEE 30th Int'lConf. Distributed Computing Systems (ICDCS '10),2010.

[3] P.MellandT.Grance,"Draft Nist Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud computing/index.html, Jan. 2010.

[4] 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 Comput-ing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[5] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.

[6] Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.

[7] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-Preserving Symmetric Encryption,"Proc. Int'l Conf. Advances in Cryptology (Eurocrypt '09),2009.

[8] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption:Improved Definitions and Efficient Con-structions," Proc. ACM Conf. Computer and Comm. Security (CCS'06), 2006.

[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data,"Proc. IEEE INFOCOM '11, 2011.

[10] E.-J. Goh, "Secure Indexes," Technical Report 2003/216,CryptologyePrintArchive,http://eprint.iacr.org/, 2003