ISSN No. 0976-5697

Volume 5, No. 6, July-August 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient and Secure Searchable Clinical Patient Information on Cloud Infrastructure

Rahul M. Harne
PG Student M.E, Computer Dept,
Smt. Kashibai Navale College of Engineering,
Pune, Maharashtra, India

Prof. S. P. Kosbatwar
Assistant Professor, Computer Dept
Smt. Kashibai Navale College of Engineering,
Pune, Maharashtra, India

*Abstract***:** Cloud computing economically permits the paradigm of information service outsourcing. However, to shield information privacy, sensitive cloud information need to be encrypted before outsourced to clinical cloud, that make efficient information utilization service a really hard task though ancient searchable secret writing techniques enable users to firmly search over encrypted information through keywords, they support solely Boolean search and don't seem to be nonetheless comfortable to satisfy the effective information utilization would like that's inherently demanded by sizable amount of users and large amount of information files in cloud. In paper outline and solve the matter of secure hierarchic keyword search over encrypted information on clinical cloud. For large data searching various techniques are keyword searchable encryption technique allow user to search data through keywords. In searchable encryption having problem searching go through every retrieving file and unnecessary network traffic. Ranked search data searching various techniques are keyword searchable encryption technique allow user to search data through keywords. The relevance score from information retrieval to build a secure searchable index, process one-to-many order-preserving mapping technique to protect those sensitive score information. The design is able to make easy efficient server-side ranking without losing keyword privacy. The Ranked keyword search system enhances system handling by search result and file retrieval correctness. In ranked keyword search system having data owner, data user and cloud server to effective data searching capabilities.

Keywords: Ranked search, information retrieval, searchable encryption, confidential data, cloud computing.

I. INTRODAUCTION

Cloud is the use of computing resources that is hardware and software that are delivered as a service over a network. The cloud makes it possible for people to access people information from anywhere at any time. One requirement is that people need to have an internet connection in order to access the cloud. This means that if people want to look at a specific document people have housed in the cloud, people must first establish an internet connection either through a wireless or wired internet or a mobile broadband connection. The benefit is that people can access that same document from wherever people are with any device that can access the internet. The devices could be a desktop, laptop, tablet or phone. The different types of clouds that are Public cloud, Private cloud, Community cloud, Hybrid cloud. As a home user or small organization owner, people will most likely use public cloud services.

a. ***Public Cloud*** - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space. Public cloud having applications, storage and other resources are available to the general public by a service provider of public cloud. The various services are free and also offered on a pay-per-use model. Generally, public cloud service providers like Amazon, Microsoft and Google own and operate and access only via Internet.

b. ***Private Cloud*** - A private cloud is established for a specific group or organization and limits access to just that group. Private cloud project requires degree of commitment virtualized the business environment and it will require the organization to check decisions about existing resources. Private cloud is infrastructure operate on single organization and manage or hosted internally or externally.

c. ***Community Cloud*** - A community cloud is shared among two or more organizations that have similar cloud requirements, they managed internally or hosted internally or externally.

d. ***Hybrid Cloud*** - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community. Hybrid clouds lack the security and certainty of in house applications.

The cloud storage service providers are nothing new, but given the complexity of current backup, replication and disaster recovery needs. Storage is rented from the provider using a cost-per-gigabyte stored or cost-per-data transferred model. End user does not have to pay for infrastructure. Cloud storage providers balance server loads and move data among various datacenters, ensuring that information is stored close and thereby available quickly. Storing data on the cloud is advantageous because it allows people to protect people data in case there is a disaster. People may have backup files of people critical information, but if there is fire or a hurricane wipes out people organization in this case having the backups stored locally does not help.

In cloud infrastructure data owner share their outsourced data with a large number of users, who might want to only retrieve certain specific data files they are interested in during a given session. The one ways is through keyword-based search and keyword search technique allows users to selectively retrieve files of interest and has useful in plaintext search scenarios but in encryption traditional search method fails due to retrieving every file in decryption. Therefore, we used searchable encryption system with secure ranked search in paper. We explore ranked search over encrypted data in Cloud Computing it enhances system usability by returning the matching files in a ranked order regarding to certain relevance score.

In next section II, the related work over the various methods security at data sharing systems. In section III, the proposed approach and its mathematical description and result of the system which is discuss. Finally conclusion and future work is predicted in section IV and references in section V.

II. RELATED WORK

A. Survey:

In the literature survey we are going to discuss Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data: Below in literature we are discussing some of them.

The initial attempt, to motivate and solve the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in cloud computing. The first give a basic scheme and show that by following the same existing searchable encryption framework, it is very inefficient to achieve ranked search. Then appropriately weaken the security guarantee, resort to the newly developed crypto primitive OPSE, and derive an efficient one-to-many order-preserving mapping function, which allows the effective RSSE to be designed [1]. Through security analysis, they show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of our solution.

The long dreamed vision of computing as a utility is finally emerging. The elasticity of a utility matches the need of businesses providing services directly to customers over the Internet, as workloads can grow (and shrink) far faster than 20 years ago. It used to take years to grow a business to several million customers now it can happen in months. From the cloud providers view, the construction of very large datacenters at low cost sites using commodity computing, storage, and networking uncovered the possibility of selling those resources on a pay-as-you-go model below the costs of many medium-sized datacenters, while making a profit by statistically multiplexing among a large group of customers. From the cloud user's view, it would be as startling for a new software startup to build its own datacenter as it would for a hardware startup to build its own fabrication line. In addition to startups, many other established organizations take advantage of the elasticity of Cloud Computing regularly, including newspapers like the Washington Post, movie companies like Pixar, and universities like ours. Our lab has benefited substantially from the ability to complete research by conference deadlines and adjust resources over the semester to accommodate course deadlines. As Cloud Computing users, we were relieved of dealing with the twin dangers of over provisioning and under-provisioning our internal datacenters as in [3].

Cloud Security Alliance, they should now understand the importance of what you are considering moving to the cloud, your risk tolerance (at least at a high level), and which combinations of deployment and service models are acceptable and also have a rough idea of potential Exposure points for sensitive information and operations as in [4].

The provide provable secrecy for encryption, in the sense that the un trusted server cannot learn anything about the plaintext when only given the cipher text; they provide query isolation for searches, meaning that the un trusted server cannot learn anything more about the plaintext than the search result and provide controlled searching, so that the un trusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the un trusted server to search for a secret word without revealing the word to the server [6]. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Formally define a secure index and formulate a security model for indexes known as semantic security against adaptive chosen keyword attack (ind-cka) and develop an efficient ind-cka secure index construction called z-idx using pseudo-random functions and Bloom filters, and show how to use z-idx to implement searches on encrypted data. This search scheme is the most efficient encrypted data search scheme currently known; it provides O (1) search time per document, and handles compressed data, variable length words, and Boolean and certain regular expression queries. The techniques developed in this paper can also be used to build encrypted searchable audit logs, private database query schemes, accumulated hashing schemes, and secure set membership tests as in [7].

Searchable encryption traditional searchable encryption has been generally calculated as a cryptographic primitive, with a focus on security explanation formalizations and efficiency improvements. They proposed a scheme in the symmetric key setting and all word in the file is encrypted separately under a special two-layered encryption construction as in [8].

Secure top-k retrieval from Database Community from database community is the most related work to our proposed system [1]. The idea of uniformly distributing posting elements using an order-preserving cryptographic function but still, the order preserving mapping function proposed does not support score dynamics and any insertion and updates of the scores in the index will result in the posting list completely rebuild. Top-K retrieval, in this method user search query & keyword is same as already they searched query & keyword means the already selected content click will displayed in the top link and then all other ranking based links are display as in [9].

B. Motivation:

The rapid development of the computer technology and network technology brings growing computing demands and storage demands. Many companies, organizations and individuals choose to outsource their computing demands and storage demands. Cloud computing and cloud storage are proposed to satisfy these requirements. Cloud storage is a dynamic service provided by Server. Since cloud service providers (CSP) are separate industries entities, data integrity and privacy are the most critical issues that need to be addressed in cloud computing. Clients can pay a fee to obtain an appropriate storage space to store their own data. Even though the cloud service providers have standard regulations and powerful infrastructure to ensure customers data privacy and provide a better availability.

As Cloud Computing becomes common and more sensitive information are being central into the cloud, such as patient data, personal health records and government documents, etc. The fact of data owner and cloud server are no longer in the same trust domain may put the outsourced unencrypted data at risk: the cloud server may disclose data information to unauthorized entities. It follows that sensitive data has to be encrypted prior to outsourcing for data privacy and combating unsolicited accesses. If server fails there is no backup available or load balancing technique available for handle this work this is main problem in this system.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Problem Definaation:

Secure and Efficient search Over Encrypted Data on Clinical Cloud consist enable searchable encryption system with support of secure ranked search and also exploring ranked search over encrypted data in cloud computing and then Returning match files in ranked.

B. Proposed system and Design:

The proposed system, we will make use of multi cloud storage to upload clinical data on the cloud. If one of the server gets corrupted then file can be retrieve from other servers, the backup server is used for the retrieval of the file. As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as emails, personal health records, company finance data, and government documents, etc. 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 that sensitive data has to be encrypted prior to outsourcing for data privacy and combating unsolicited accesses. If server fails there is no backup available or load balancing technique available for handle this work this is main problem in this system.

For the first time, we define the problem of secure ranked keyword search over encrypted cloud data, and provide such an effective protocol, which fulfills the secure ranked search functionality with little relevance score information leakage against keyword privacy. Thorough security analysis shows that our ranked searchable symmetric encryption scheme indeed enjoys as-strong-as-possible security guarantee compared to previous SSE schemes. We investigate the practical considerations and enhancements of our ranked search mechanism, including the efficient support of relevance score dynamics, the authentication of ranked search results, and the reversibility of our proposed one-to much order-preserving mapping technique. Extensive experimental results demonstrate the effectiveness and efficiency of the proposed solution.

Figure 1 shows the proposed system of Search over Encrypted Cloud Data model. There are three main actors as first User, Data Owner and cloud server. Data owner has a collection of n data files C = (F1, F2, . .. , Fn) that he wants to outsource on the cloud server in encrypted form while still keeping the capability to search through them for effective data utilization reasons. To do so, before outsourcing, data owner will first build a secure searchable index I from a set of m distinct keywords W= (w1, w2, wm) extracted2 from the file collection C and store both the index I and the encrypted file collection C on the cloud server.

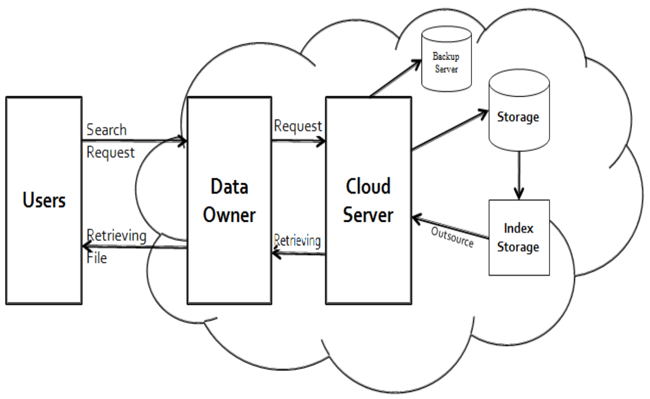

Figure.1: Proposed system architecture of Search over Encrypted Cloud Data

We assume the authorization between the data owner and users is appropriately done. To search the file collection for a given keyword w, an authorized user generates and submits a search request in a secret forma trapdoor Tw of the keyword w to the cloud server. Upon receiving the search request Tw, the cloud server is responsible to search the index I and return the corresponding set of files to the user. We consider the secure ranked keyword search problem as follows: the search result should be returned according to certain ranked relevance criteria to improve file retrieval accuracy for users without prior knowledge on the file collection C. However, cloud server should learn nothing or little about the relevance criteria as they exhibit significant sensitive information against keyword privacy. To reduce bandwidth, the user may send an optional value k along with the trapdoor Tw and cloud server only sends back the top-k most relevant files to the users interested as in [1].

Primarily consider an honest-but-curious server in model, which is consistent with most of the previous searchable encryption schemes. Assume the cloud server acts in an honest fashion and correctly follows the designated protocol specification, but is curious to infer and analyze the message ow received during the protocol so as to learn additional information. In other words, the cloud server has no intention to actively modify the message ow or disrupt any other kind of services. However, in some unexpected events, the cloud server may behave beyond the honest but curious model keyword w.

C. Notations and Proposed Mathematic:

The data set provide in searching of encrypted data on cloud. Calculation of ranked order of data in the form of index Tag at the data user send request to data owner then outsource data to the cloud server. Index that data in cloud server storage index and outsourced index data to cloud server. One-to-many order preversing applied from cloud server to data owner Response send from data owner to data user cloud Server has to provide response for the request and if data has not retrieved then alert generate and otherwise success. The relevant score calculating with the Term Frequency mortifying with Inverse Document Frequency. The term frequency is simply number of times a given keyword appears within file and inverse document frequency obtain by divide number of files in whole collection by number of file contain keyword.

a. Notations:

C = Set of collection of Files
CSP = Total number of cloud service provider
DO = Total number of data owner
W = Total number of distinct keyword extract from C
F = File having search name and score to find unique location of actual file
S = Score Calculation depends on patient visits
V = Visits of patient registered in clinic
R = Ranked depend on highest score

b. Proposal Mathematical:

Input
C= $\{C_i\}$
CSP = $\{Csp_i\}$
DO = $\{DO_i\}$
W = $\{W_i\}$
Intermediate Result
F = {W, S}
S = $\{V_i\}$
V = {1... , n}
R = $\{S_i\}$
Output
M = System
I = Inputs
M = $\{W_i, |R_i|, S_i\}$

If relevant score for requested file not match then send request again otherwise Success message.

The score calculation depends upon term frequency and inverse document frequency of document search. The term frequency is depends upon how terms in single fragment and directory frequency is depend upon how many documents does term work and inverse document frequency (IDF) is obtained by dividing the number of files in the whole collection by the number of files containing the term (to measure the overall importance of the term within the whole collection).

$$\mathrm{Score(W,F)} = \sum_{t\in W} \left(1 + \mathrm{I}n\, F_{d,t}\right) .\mathrm{I}n(1+\frac{N}{f}) \qquad (1)$$

W denoted the search keywords $F_{d,t}$ denotes the term frequency of term t in file F, f denotes the number of files that contain term t and N denotes total number of files in the collection C. The visits of patient calculated from patient registered in system; according to visits calculation of score is done. The size of file calculated for derive score calculation.

D. Basic RSE Scheme:

In ranked searchable encryption (RSE) scheme consists of four important encryption parameter are KeyGen, BuildIndex, TrapdoorGen, SearchIndex. This ranked searchable encryption system in two phases, Setup and Retrieval

In Setup phase, the data owner initializes the public and secret parameters of the system by executing KeyGen on patient new registration and collects all the data into single string to encrypt that data. The data file collection C by using BuildIndex to generate the searchable index from the unique words extracted from C. The search request publishes the index including the keyword frequency-based relevance scores in some encrypted form, with the encrypted collection C to the Cloud. As part of Setup phase, the data owner also needs to distribute the necessary secret parameters to patient registration.

In Retrieval phase, the user send searching request to cloud server and uses TrapdoorGen to generate a secure trapdoor corresponding to his interested keyword and submits it to the cloud server. Upon receiving the trapdoor T, π_x(w) used to cloud server will derive a list of matched file with their suggested keyword and F_y(w) to decrypt the entities and Receive that trapdoor cloud server derive list of match file. Their corresponding relevance scores by searching the index via SearchIndex. The matched files should be sent back in a ranked sequence based on the relevance scores.

The KeyGen (.) used security parameter k, l, p suppose. The advance encryption standard algorithm used to encrypt the string which is collection of all the other fields stored in the patient registration P: $\{0,1\}^l * \{0,1\}^r \rightarrow \{0,1\}^r$ and π used for hash function which is used to map data of arbitrary size to data of fixed size and takes input and returns fixed size string.

a. Initialize:

Input Request file with distinct keyword w from collection of file C to data owner

b. Build Encrypt key

Data owner Call $KeyGen(1^k, 1^l, 1^p)$,and generate random keys x,$y \xleftarrow{R} \{0,1\}^r, z \xleftarrow{R} \{0,1\}^r$ and Output K $=$ {x, y, z$, 1^k, 1^l, 1^p$}
Data owner build secure Index call BuildIndex (K, C)

c. Search request file

Select Interested Keyword w
Generate Trapdoor T= (π_x(w), f_y(w)) by TrapdoorGen(w) and submit to cloud server
Receiving T_w, call SearchIndex (I, T_w)
Locate matching index π_x(w) and use f_y(w) to decrypt the entities
Ranked search result gets by relevance score via key z

d. Output

If there is mismatch, generate alerts Otherwise SUCCESS
BuildIndex (K, C)

a. Initialize

Scan file collection C and extract distinct words of W $=$ $\{\mathrm{w1, w2, \ldots\ldots, wm}\}$from C

b. Encryption

i) for each w_i where $1\leq i \leq m$
Calculated encrypted string of given keyword which encrypted at the time of registration and process it.

c. Build Score

i) for each $w_i \in W$
Calculate score for file according to "(1)", denote s
Compute score and find the list of file

d. Match file

Computing score and calculate match file gives w_i to π_x(w)

E. Evaluation of result:

The score calculation depends upon term frequency and inverse document frequency of document search. The term frequency is depends upon how terms in single fragment and directory frequency is depend upon how many documents does term work and inverse document frequency (IDF) is obtained by dividing the number of files in the whole collection by the number of files containing the term (to measure the overall importance of the term within the whole collection). The calculating score with patient visits to clinic, how many times patient visits for the case like fever, cough, etc and calculating that visits and according to that visits calculating ranked for the search patient which are requested. The figure 1 shows the distribution of relevance score for the number of visits. The score calculation depends upon visits and the files that containing requested keywords. The distribution of ranked depend upon the how many visits of patient in clinic maximum visits gets maximum ranked. For ranked search purpose, the job of determining which files are most relevant is typically done by assigning a numerical score, which can be precomputed and with help of "(1)".

Table 1: An example of relevance score of requested keyword of related files.

Word	w_i				
File ID	F1	F2	F3	F4	…….
Relevance Score	0.47	0.35	0.53	0.28	…….

The relevance score distribution for keywords requested from data user to cloud data through data owner. The distribution of score depends on match keyword files which are requested from user and calculating the relevance score of the match files.

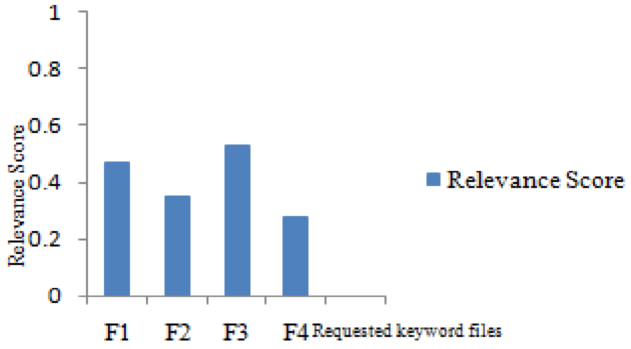

Figure 2: Relevance score distribution of match keyword files

The distribution of ranked depend upon the how many visits of patient in clinic maximum visits gets maximum ranked. The evolution of time required to search files which are requested from the data user to data owner in cloud server. The search keyword from search page goes to search that keyword match files and extracted. The encryption carried out on the string, which contains all the fields of registration of the patient. At the time of searching the decrypt those entities and gives the visits of match files and view all patient details. The other system required more time to retrieve all patient data one by one. The efficiency of our project is better than other system algorithm.

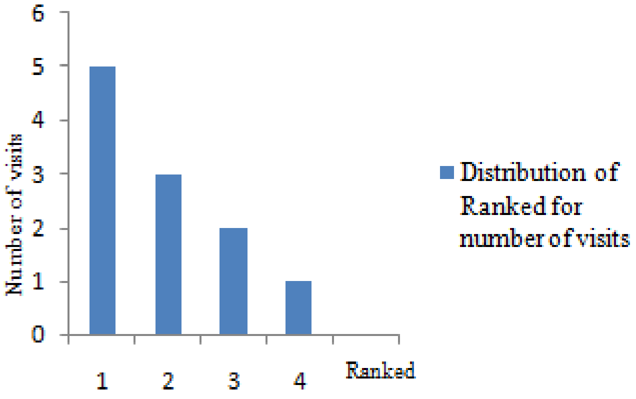

Figure 3: An example of distribution of ranked to requested file.

Searchable encryption scheme, in which novel technologies in cryptography community and IR community are employed, including homomorphic encryption and the vector space model. In Secure top-k retrieval, the data owner encrypts the searchable index with homomorphic encryption. When the cloud server receives a query consisting of multikeywords, it computes the scores from the encrypted index stored on cloud and then returns the encrypted scores of files to the data user. Next, the data user decrypts the scores and picks out the top-k highest scoring files' identifiers to request to the cloud server.

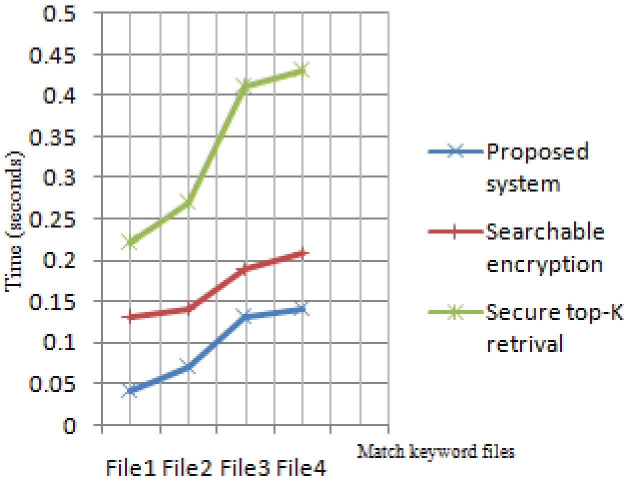

Figure 4: The time required for match keyword files for different system.

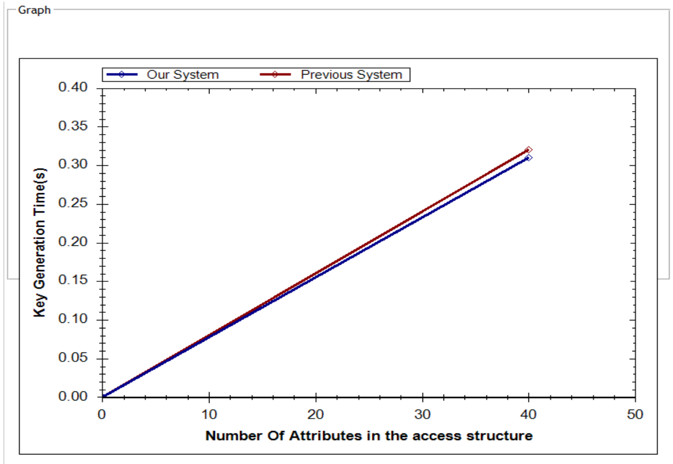

Figure 5: Encryption Key generation time for our system and previous system.

The Encryption key generates using string encryption calculation , thus previous system encrypt all the entities one by one , to recover that problem we encrypt all data in string and generates key for that. The time required is less than the other system, thus it is more efficient.

IV. CONCLUSION AND FUTURE WORK

In Secure and Efficient search Over Encrypted Data on Clinical Cloud, as an initial attempt, motivate and solve the problem of supporting efficient ranked keyword search for achieving executive utilization of remotely stored encrypted data in Cloud Computing. The existing searchable encryption framework, it is very inefficient to achieve ranked search and appropriately weaken the security guarantee. The proposed system uses ranked keyword search technique for searching data on cloud server and also uses load balancing technique for security. The proposed system is more efficient searchable technique and backup service and security.

Improvements on this model to achieve some common Load Balancing functions in the Clinical Cloud and Authenticated Ranked Search Result to improve the security of retrieving of file from cloud server, thus enabling a search result authentication mechanism that can detect such unexpected behaviors of cloud server is also of practical interest and worth further investigation. To authenticate a ranked search result, one need to ensure the retrieved results are the most relevant ones and the relevance sequence among the results are not disrupted. Cloud follows that sensitive data has to be encrypted prior to outsourcing for data privacy and combating unsolicited accesses. If server fails there is no backup available or load balancing technique available for handle this work this is main problem in this system. The load balancing is achieved using backup server for the data file on the cloud that preventing the server failure within any condition.

This Ranked Search model can be enhanced to work on the hybrid clouds formed by combinations of private and public clouds.

V. REFERENCES

[1] CongWang, Student Member, IEEE, Ning Cao, Student Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Enabling Secure and Efficient Ranked Keyword Search over Out- sourced Cloud Data" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 8, AUGUST 2012.

[2] Ming Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Stu- dent Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" IEEE 2012 Transactions on Parallel and Distributed Systems, Volume: 11, Issue: 2

[3] 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", Technical Report UCB- EECS-2011-28, Univ. of California, Berkeley, Feb. 2011.

[4] Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing, http://www.cloudsecurity alliance.org, 2011.

[5] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, KuiRen, Member, IEEE, Wenjing Lou, Senior Member, IEEE and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel and Distributed System, VOL. 22, NO. 5, MAY 2011.

[6] D. Song, D. Wagner, and A. Perrig, Practical Techniques for Searches on Encrypted Data, Proc. IEEE Symp. Security and Privacy, 2010.Farah Habib Chanchary, Samiul Islam Data Migration: Connecting Databases in the Cloud.

[7] E.-J. Goh, Secure Indexes, Technical Report 2003/216, Cryptology ePrint Archive, http://eprint.iacr.org/, 2010.

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

[9] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A.L. Varna, S. He, M.Wu, and D.W. Oard, "Confidentiality-Preserving Rank-Ordered Search," Proc. Workshop Storage Security and Survivability, 2007.

[10] Rahul M. Harne, Prof. S.P. Kosbatwar "Secure And Efficient Search Over Outsourced Data On cloud in INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY, VOL.3- Issue 1 (January - 2014).

Short Bio Data for the Authors

Rahul M. Harne received B.E Degree in Computer Technology from K. D. K College of Engg.& Tech. Nagpur, MH, India. Pursuing M.E in Computer Engineering (Computer Networks) at Smt. Kashibai Navale College of Engineering, Pune, India. His research interests include networking and cloud computing. Author published paper in IJERT, VOL3- Issue 1(January - 2014) and CPGCON 2014 Conference.

Prof S. P. Kosbatwar received B.E degree in Computer Science & Engineering from MGM COE from Marathwada University Aurangabad, ME from Govt. College of Engineering Aurangabad, Marathwada University Aurangabad. Ph.D. pursuing from JNU. He is currently working as an assistant professor at SKNCOE, Pune. His research interest includes pattern recognition and image processing and networking.