A Proficient Pattern of using Multi Keyword Search In Private Cloud For Multiuser Environment

Aurobind. G, Shivamma. D, Vijiyakumar. K

ABSTRACT-: ***A cloud system with computational services allowing users to access data, process and store features providing on-demand, a group of virtual remote servers, scalability, security, redundancy and elasticity. A model with many server for enabling convenient keys for a on-demand network access with a service provider interaction released with minimal management effort. The computing resources like networks, servers can be rapidly provisioned with a cloud based applications, and services to compute the shared pool of configurable devices, servers, storage. The encrypted data limits all the usage of networks due to the difficulty of searching over the usability of outsourced data to cloud. The privacy information are uploaded to the cloud and outsourced which are typically encrypted before likely to contain sensitive keywords for its consistent. In our paper, we present a scheme which overcomes the above complexity. Here we use two different techniques FMS-I AND FMS-II.***

First comes the simple keyword search using relevance score and preference factors. On other hand it supports the logic gate operations like "AND","OR","NOT" to find the relationship between the keywords and the document. By using these techniques the user can get a improvised search experience in encrypted cloud area. Finally, we tend to improve the single user search to multi user search by using many to many cardinality.

I. INTRODUCTION

The physical storage maintained by third party nowadays is used for storing data on off-site and it is a very popular cloud storage system. The data owner can store their data in cloud in these situations which make their data available for multiple clients is also known as data outsourcing. As cloud possesses scalability with good efficiency as major advantage it provides a constant path for data access.

The data uploaded by the data owner usually contains some private information. Therefore encrypting the data becomes must in such situations. But this encryption process takes the client to difficult phase for searching the data in cloud environment. Searchable encryption technique is a recent approach to search the encrypted data in cloud. Several multi keyword search techniques were addressed in past works, but each suffer from a disadvantage. Even though many measures were taken to solve these kind of issues, still the difficulty for searching encrypted data in cloud cannot be solved.

Some methodologies have been proposed to guarantee security attributes inside a cloud situation to assess cloud computing security and present a "trusted outsider". In this approach it guarantees that the information are not noticeable to outside clients and cloud directors. It anticipates data exposure to cloud server in the standard arrangement which encrypts private information before transferring it onto the cloud system with various servers. Then again, there are severe datas on the server handling process for the encoded information.

For instance, standard of system with plain content based on searching calculations are not appropriate any more. To play out a key based inquiry, the whole informational collection needs to be decrypted regardless of the possibility that the coordinating outcome set is little. It postures unbearable query latency and causes unsatisfactory computational overhead.

To solve this, for multi keyword based searching technique on the encrypted data for present solutions to the cloud. First we decide the keyword for the document and index for the file is uploaded to the cloud and also calculated. Now the information is ready to accessing by the search users. The user searching the required document by secret key and cloud server returns the list of document.

Albeit many pursuit functionalities with efficient searchable encryption that have been created in past writing towards exact and, it is still difficult for the client encounter as that of the plaintext seeks for searchable encryption to accomplish a similar. In additionally is to empower the multi-catchphrase which enhance the client's involvement on seeking, the OR, AND and NO operations an essential and crucial capacity with the thorough rationale operations of catchphrases.

These are rapidly recognize the coveted information and crucial for pursuit clients to prune the looking space in computing paradigm. Cao et al. [6] It proposes a system of searchable encryption conspire with "OR" operation to facilitate coordinating inquiry plot (MRSE) which can be viewed in the system. Zhang et al. [17] It proposes "AND" operation with the returned records coordinating all watchwords which can be respected as a searchable encryption plot and a conjunctive watchword seek plot.

In this paper, we give the conclusion to two problems by incorporating two different FMS approaches for encrypted data.

Firstly, we introduce two schemes for searchable encryption namely relevance scores and preference factors. Relevance score deals with most precise results whereas preference factors number of times the keyword appears.

Revised Manuscript Received on September 2, 2019.

Aurobind. G, NIMHANS Digital Academy, National Institute of Mental Health And Neurosciences (NIMHANS), (An INI), Bangalore, Karnataka, India
(email: aurofindsyou@gmail.com)
Shivamma. D, NIMHANS Digital Academy, National Institute of Mental Health And Neurosciences (NIMHANS), (An INI), Bangalore, Karnataka, India
Vijiyakumar. K, Department of Information Technology, Manakula Vinayagar Institute of Technology, Pondicherry, Tamilnadu, India.

It improves the searching experience and clients satisfaction.

Secondly, the comprehensive logic operations "AND", "OR" and "NO" are employed to achieve searchable encryption in multi keyword search. Finally, the efficiency of above two approaches was added advantage by the classified sub – dictionaries technique [fig.1].

In real world, apart from some important keyword, other keyword in the dictionary are very technical terms, and dictionary size will becomes larger and more complex to accessing the data. The data owner dictionary are used to resize all the files on the other hand.

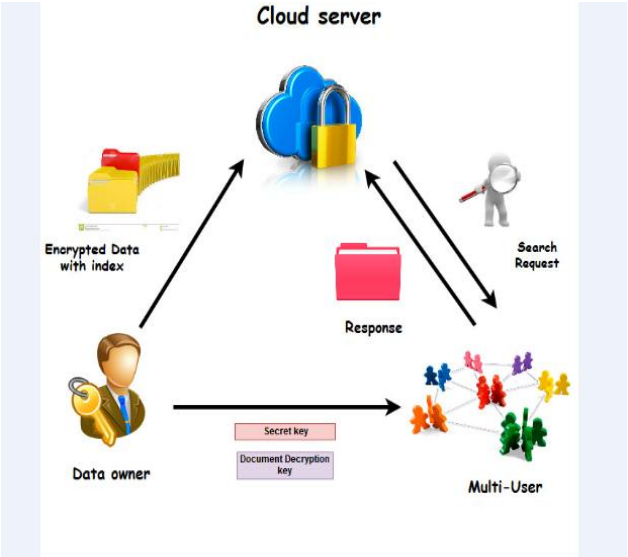

Fig.1 System model

II. PROPOSED WORK

The projected theme will support difficult logic search the mixed operations of keywords like "AND", "OR" and "NO" with a sensible and really economical multi-keyword search theme is developed. The delivered documents matching all keywords which may be considered a searchable encryption concept with "AND" operation and a conjunctive keyword search theme.

To coordinate a searchable secret encryption concept with "OR" operation which may be considered matching search theme (MRSE). We are going to make the data access by multi user at same time. We are using algorithm for producing key and encryption and decryption called Identity Based algorithm.

The searchable encryption also has the preference with factors of keywords which has relevance scores and for searchable encryption makes multi keyword search easier [fig.2].

The search users correspondingly permits customized search for specific user to enable the preference keywords and relevance score, and also the importance of keywords within the search keyword has lot of preference factors with keywords which represents set such as it will alter additional precise results. In searchable encryption it improves the multi user experience and search functionalities and the NO, AND ,OR operations within the multi-keyword search. The incorporated concept can lower the query complexity and improves the comprehensive functionality.

To boost the potency on the top of two approaches and tend to use the classified sub-dictionaries technique.

III. IDENTITY BASED ENCRYPTION

An Identity Base Encryption (IBE) scheme which generates a public key with many set of encrypted keys from a known identity value such as an ASCII string values is a valid public key with any string public-key cryptosystem which has any numbers that allows any party to access al keys systems.

The Private Key Generator (PKG) with a multiple set of trusted third party or data owner generates more number of corresponding private keys in particular with email addresses and dates can be public keys.

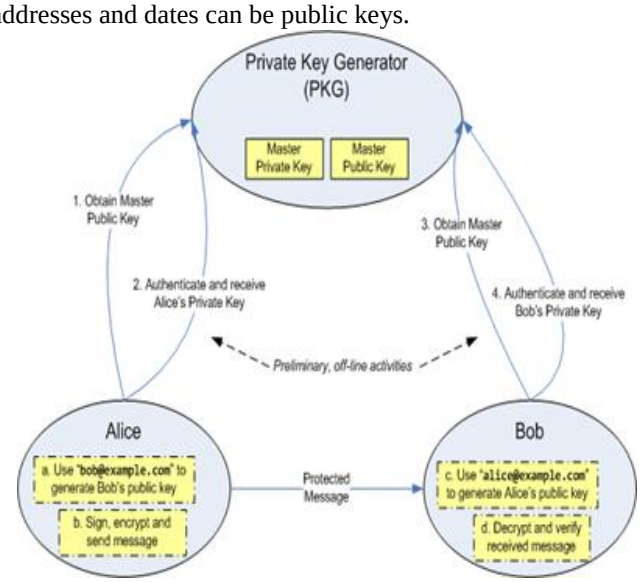

Fig .2 Identity Based Encryption

IV. SYSTEM DESIGN

As per the requirements the system design is classified into three modules,

- Data owner
- Cloud server
- Multi user search

4. 1. Data owner

The cloud server for production which access data to the clients are conducive and stable and the owner of data uploads entire set of data server to cloud systems. To the data owner of cloud who encrypts the key to pioneer data with Identity based encryption are to protect sensitive data that has a key mechancism [fig.3].

For every uploaded document there are some keywords which provokes the data owner of cloud system to enhance the search potency. The secret key and keywords are created with index which are consistent.

After that, ample client environment which transfers the encrypted documents indexes to the cloud server system with various key sets, and delivers the symmetric and secret key with all encrypted key values to the cloud system [fig.4].

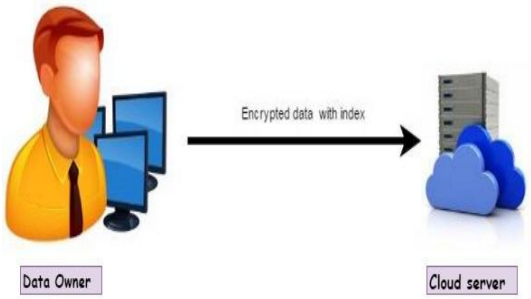

Fig.3 Data owner uploads the data to Cloud server

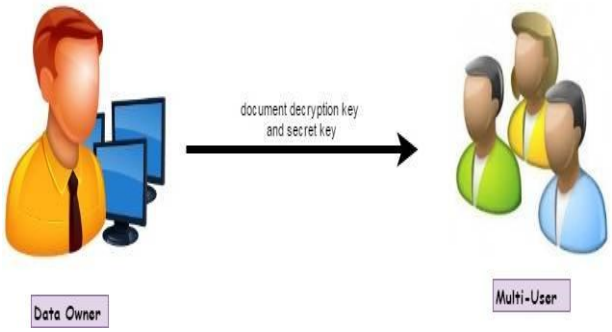

Fig.4 Data owner provides the key to Multi - user

4. 2. Cloud Server

The intermediate entity with lot of documents encrypted and the indexes which acts as the data owner of cloud group created by keys and the system of cloud servers are were outsourced to search technique. The data were provided to the user requests were accessed for encryption and data are being processed. It provides more data access to the users for computing.

4.3. Multi User Search

The multiple users enquire the outsourced documents from the cloud server. At first, the user collects the unique secret key and symmetric key from the data owner. Then, with the help of the keywords, the user adopts the secret key to provoke a trapdoor and forward it to the cloud server[fig.5].

Finally, the user receives the equivalent documents from the document collection. Atlast decrypts it using the symmetric key decrypts it using the equivalent documents from where the user receives from the document collection.

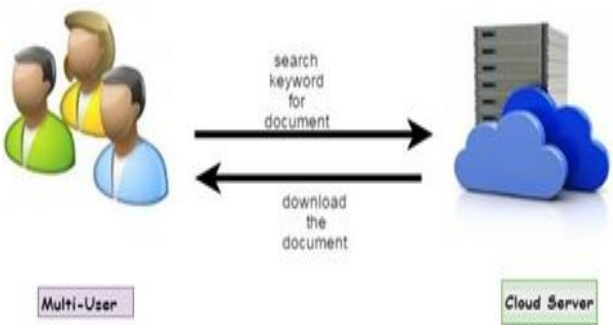

Fig .5 Multi user Requests and retrieves data from cloud

V. HAZARD MODEL AND REQUIREMENTS

In the hazard model, the group of cloud servers are deduced to be honest but curious to the system as most relevant works which is in the search form on secure cloud. The message flows throughout the protocol cloud server with repository collection which are received must have a curious to induce and figure out data (including index) [fig.6, 7 & 8]. It also includes the two different models:

5.1 Known Cipher Text Model

The Known Cipher Text Model which has cloud server of system is known to the data owner to outsource the encrypt the entire documents and the index which is a cipher model.

5.2. Known Background Model

The data from a best-known comparable dataset. The alternative data with related census of cloud server within the best-known encrypted model like the relationship of trapdoors and therefore it will acquire wider proficiency than what will be accessed.

The security requirements on the behave of the above hazard model, is defined as:

- Documents with more Confidentiality
- Trapdoor of keys and Privacy protection of index
- Ability of trapdoor to Unlink

The targeting dataset bears with the similar nature that the cloud server bears the similar nature will possess the census.

EXPERIMENTAL RESULTS

Fig.6 Home page

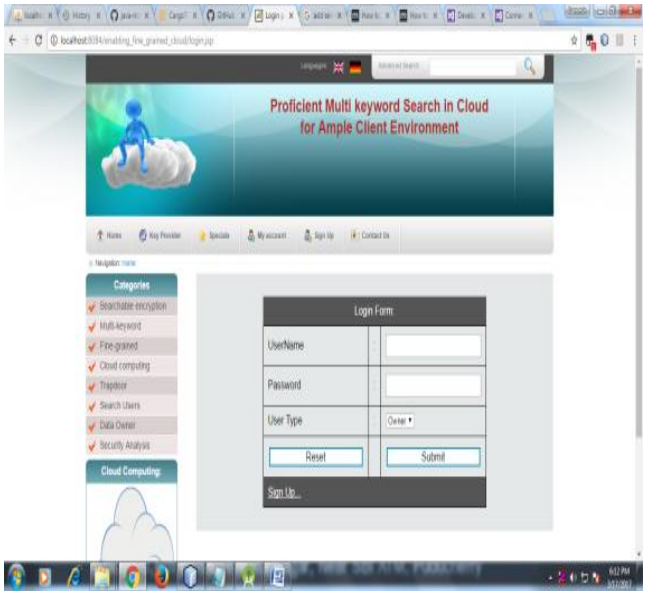

Fig. 7 Login Form

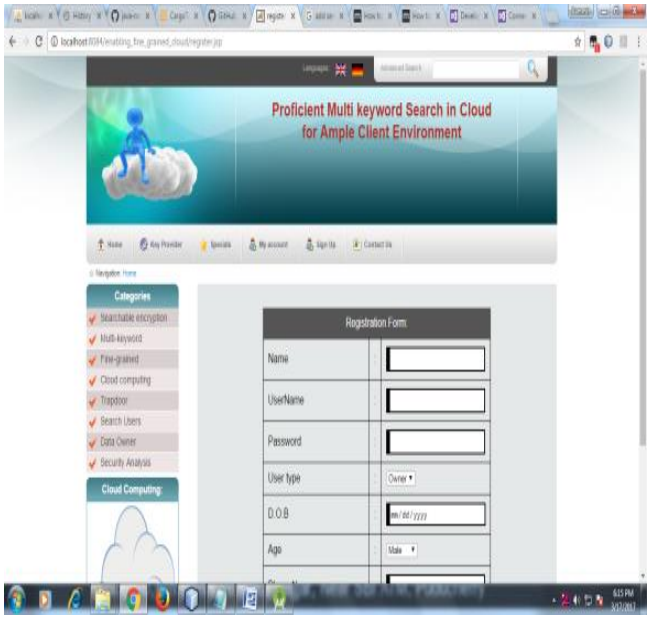

Fig. 8 Registration Form

VI. CONCLUSION

In this, two FMS schemes were suggested, the encrypted cloud data is investigated this issue over the multi-keyword search with fine grained (FMS). In FMS-I, the preference factors of with many number of keywords to relevance scores which reinforce additional precise search and extend users expertise. In FMS-II , The operations of keywords are formulated with logical search AND, OR and NO. In multi-user cloud environment, we majorly classifies sub-dictionaries of cloud keys (FMSCS) to enhance potency with the improved approaches supporting the cloud platform.

VII. FUTURE SCOPE

For the future work, the cloud environment is to develop the highly with various keyword factors which leads to faster searchable encryption that alter proficient search and tend improvise the extensibility of the file set

REFERENCES

1. Ting Xu , Wei Xiang , Qing Guo , Lifeng Mo, Mining Cloud 3D Video Data for Interactive Video Services, Mobile Networks and Applications, v.20 n.3, p.320-327,June 2015 [doi: 10.1007/s11036-015-0596-1]
2. K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, Y. Zhou, Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions, IEEE Commun. Surv. Tut., 17 (2015) 2377-2396.
3. X. Xiong, L. Hou, K. Zheng, W. Xiang, M. Hossain, S. Rahman, SMDP-based radio resource allocation scheme in software-defined internet of things networks, IEEE Sens J, 16 (2016) 7304-7314.
4. P. Zhao, L. Feng, P. Yu, W. Li, X. Qiu, A social-aware resource allocation for 5g device-to-device multicast communication, IEEE Access, 5 (2017) 15717-15730.
5. S. Misra, P. V. Krishna, and V. Saritha, "LACAV: An energy-efficient channel assignment mechanism for vehicular ad hoc networks," J. Supercomput., vol. Volume 62, no. Issue 3, pp. 1241-1262, 2012.
6. A. Singhal, "Modern Information Retrieval: A Brief Overview," IEEE Data Eng. Bull., vol. 24, no. 4, pp. 35-43, Mar. 2001. 6. I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.
7. R. Li, Z. Xu, W. Kang, K. C. Yow, and C.-Z. Xu, "Efficient multi-keyword ranked query over encrypted data in cloud computing,"Future Generation Comput. Syst., vol. 30, pp. 179-190, 2014.
8. H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, "Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage," IEEE Trans. Emerging Topics Comput., 2014, DOI:10.1109/TETC.2014.2371239
9. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2010, pp. 253-262.
10. A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in Advances in Cryptology-EUROCRYPT, Springer, 2009, pp. 224-241.
11. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li,"Verifiable privacy-preserving multi-keyword text search in thecloud supporting similarity-based ranking," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 11, pp. 3025-3035, Nov. 2014.
12. J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multikeywordtop-k retrieval over encrypted cloud data," IEEE Trans.Dependable Secure Comput., vol. 10, no. 4, pp. 239-250, Jun. 2013.
13. A. Arvanitis and G. Koutrika, "Towards preference-aware relationaldatabases," in Proc. IEEE Int. Conf. Data Eng., 2012, pp. 426-437.
14. G. Koutrika, E. Pitoura, and K. Stefanidis, "Preference-basedquery personalization," in Advanced Query Processing. Springer,2013, pp. 57-81.
15. B. Zhang and F. Zhang, "An efficient public key encryption withconjunctive-subset keywords search," J. Netw. Comput. Appl.,vol. 34, no. 1, pp. 262-267, 2011.