|| Volume 3 || Issue 6 || June 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement

Miss. Jayashri Divekar[1], Prof. D. R. Patil[2]
PG Students at Dept. of Computer Engineering ,JSCOE Hadapsar, Pune , Maharashtra, India[1]
Asst. Professor at Dept. of Computer Engineering ,JSCOE Hadapsar, Pune , Maharashtra, India[2]

Abstract— **In distributed computing, accessible encryption plot over outsourced information is a hot research field. Nonetheless, generally existing takes a shot at encoded look over outsourced cloud information take after the model of "one size fits all" and disregard customized seek aim. Additionally, the greater part of them bolster just correct catchphrase look, which significantly influences information convenience and client encounter. So how to outline an accessible encryption conspire that backings customized look and enhances client seek encounter remains an exceptionally difficult errand. In this project, out of the blue, we think about and take care of the issue of customized multi-catchphrase positioned seek over scrambled information (PRSE) while saving protection in distributed computing. With the assistance of semantic philosophy WordNet, we manufacture a client intrigue show for singular client by investigating the client's inquiry history, and receive a scoring component to express client premium keenly. To address the restrictions of the model of "one size fit all" and catchphrase correct inquiry, we propose two PRSE plans for various pursuit goals. Broad examinations on certifiable dataset approve our investigation and demonstrate that our proposed arrangement is extremely proficient and compelling.**

I INTRODUCTION

A prominent approach to look over encrypted information is accessible encryption and numerous helpful plans have been advanced under various applications. Be that as it may, these accessible encryption plans based on keyword never again completely fulfill the new challenges and clients' expanding needs, particularly showed in the accompanying two viewpoints. One is that the vast majority of existing plans take after the model of "one size fits all" and disregard singular clients' involvement because of their distinctive leisure activities, interests or social background. The other one is that a large portion of these plans support just correct keyword search. That implies the returned result is just identified with the client's. We consider and take care of the issue of customized multi-keyword positioned search over encrypted data (PRSE) while protecting security in the distributed computing. In PRSE, with the help of semantic ontology WordNet, user interest model for individual user is built by analyzing the user's search history. And we adopt a scoring mechanism to express user interest smartly by calculating the similarity score between different types of related words and the keyword. We propose a basic design of PRSE, and then give two PRSE schemes based on secure inner product in order to meet different search intentions. A complete system model in cloud computing should involve three different entities: the data owner, the data user and the cloud server.

II LITERATURE REVIEW

Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou, " Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data ", 2014.[1]

The innovation in cloud computing has encouraged the data owners to outsource their data managing system from local sites to profitable public cloud for excessive flexibility and profitable savings. But people can like full benefit of cloud computing, if we are able to report very real secrecy and security concerns that come with loading sensitive personal information. Allowing an encrypted cloud data search facility is of great significance. In view of the huge number of data users, documents in the cloud, it is important for the search facility to agree multi keywords query and arrange for result comparison ranking to meet the actual need of data recovery search and not regularly distinguish the search results. Related mechanisms on searchable encryption emphasis on single keyword search or Boolean keyword search,

Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang, " A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data ", 2016. [2]

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TFIDF model are combined in the index construction and query generation. We construct a special tree-based index

structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results . Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

3. Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou, Xuemin (Sherman) Shen," Enabling FineGrained Multi-Keyword Search Supporting Classified Sub-Dictionaries over Encrypted Cloud Data ", 2016.[3]

Utilizing Cloud Computing, people can store their information on remote servers and permit information access to open clients through the cloud servers. As the outsourced information are liable to contain touchy protection data, they are regularly scrambled before transferred to the cloud. This, on the other hand, altogether restrains the ease of use of outsourced information because of the trouble of seeking over the encoded information.

4. Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, Fengxiao Huang, " Enabling Personalized Search Over Encrypted Outsourced Data With Efficiency Improvement", 2016.[4]

In cloud computing, searchable encryption scheme over outsourced data is a hot research field. However, most existing works on encrypted search over outsourced cloud data follow the model of "one size fits all" and ignore personalized search intention. Moreover, most of them support only exact keyword search, which greatly affects data usability and user experience. So how to design a searchable encryption scheme that supports personalized search and improves user search experience remains a very challenging task. In this paper, for the first time, we study and solve the problem of personalized multi-keyword ranked search over encrypted data (PRSE) while preserving privacy in cloud computing. With the help of semantic ontology WordNet, we build a user interest model for individual user by analyzing the user's

5. Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, Weixin Xie , " An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing ", 2016.[5]

Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. In this paper, an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access Structure.

III SYSTEM ARCHITECTURE

A complete system model in cloud computing involve three different entities: the data owner, the data user and the cloud server. Data User Module includes the user registration login details. Data Owner Module helps the owner to register their details and also include login details. A user interest model stored in the user side. The user interest model is built upon the users long-term search history. It records access frequency of both query keywords and their related keywords with the help of Word-Net.

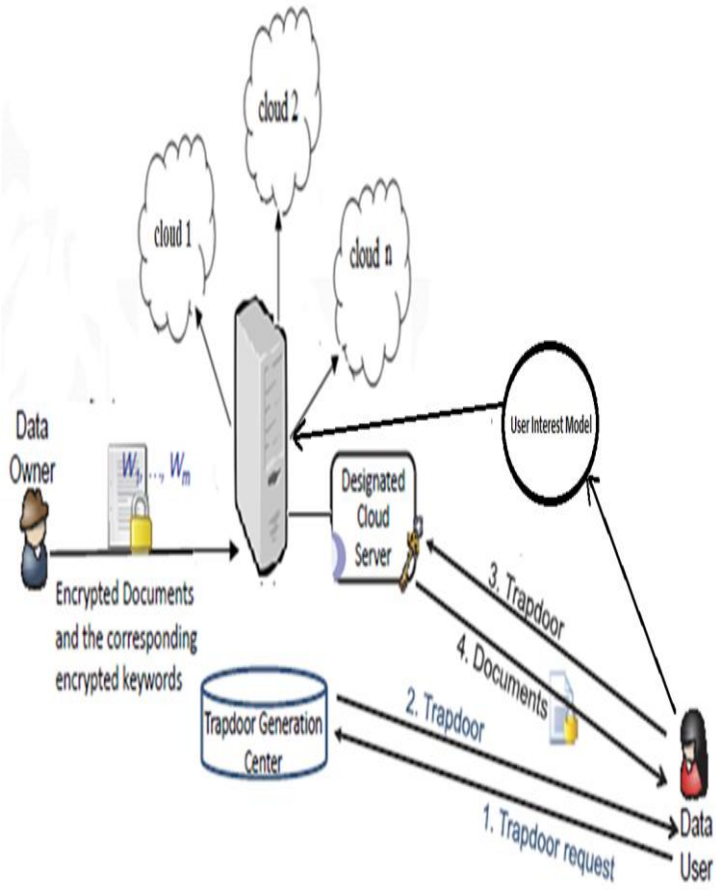

Figure 1 System Architecture

IV MODULES

1. Data User Module:

This module includes the user registration login details. He receives encrypted data from server. He takes secret key from data owner and decrypt the data.

2. Cloud:
Upon receiving the search request from the authorized user, the cloud server will conduct designated search operation over the index and send back relevant encrypted documents, which have been well ranked by the cloud server according to some ranking criteria.

3. Data Owner Module:
This module helps the owner to register them details and also include login details. He encrypts data and uploads it on cloud server.

4. File Upload Module:
This module helps the owner to upload his file with encryption using RSA algorithm. This ensures the files to be protected from unauthorized user.

5. Encryption:
Rank Search Module: This module ensures the user to search the files that are searched frequently using rank search.
File Download Module: This module allows the user to download the file using his secret key to decrypt the downloaded data.

6. Decryption:
View Uploaded and Downloaded File : This module allows the Owner to view the uploaded files and downloaded files

7. User Interest Model :
The user interest model is built upon the user's long-term Data owner Cloud server encrypted data & index search request top-k personalized results search control access control user interest model Data user. Architecture of the search over encrypted cloud data search history. It records access frequency of both query keywords and their related keywords with the help of Word Net. Different access frequency of keywords, as keyword priority, can reflect their different importance in view point of the data user.

V ALGORITHM

Algorithm for updating of original User Index Model
Require:
U:the original user interest model;
w:the new query word;
θ: an impact factor, fixed as 1;
Ensure:
U' :the updated user interest model
1: if w in U then
2: update the score of w, score = 1 + score × θ;
3: else
4: create a new node with score 1 labeling w;
5: end if
6: synonym set=GetSynonymSet();
7: for every synonym w' in synonym set do
8: if w' in U then
9: update the score of w' , score = α + score × θ;
10: else
11: create a new node with score α labeling w' ; add a edge w – w' and label synonym relation;
12: end if
13: end for
14: hypernym hyponym set= GetHypernym hyponymSet();
15: for every hypernym/hyponym w' in hypernym hyponym set do
16: if w' in U then
17: update the score of w' , score = β + score × θ;
18: else
19: create a new node with score β labeling w' ; add a edge w – w' and label hypernym/hyponym relation;
20: end if
21: end for
22: meronym holonym set= GetMeronym HolonymSet();
23: for every meronym/holonym w' in meronym holonym set do
24: if w' in U then 25: update the score of w' , score = γ + score × θ;
26: else
27: create a new node with score γ labeling w' ; add a edge w−w' and label meronym/holonym relation;
28: end if
29: end for
30: return U' ;

VI RESULTS

Figure. 2 User Home Page

Figure. 3 User Login

Figure. 4 Adrive File Details

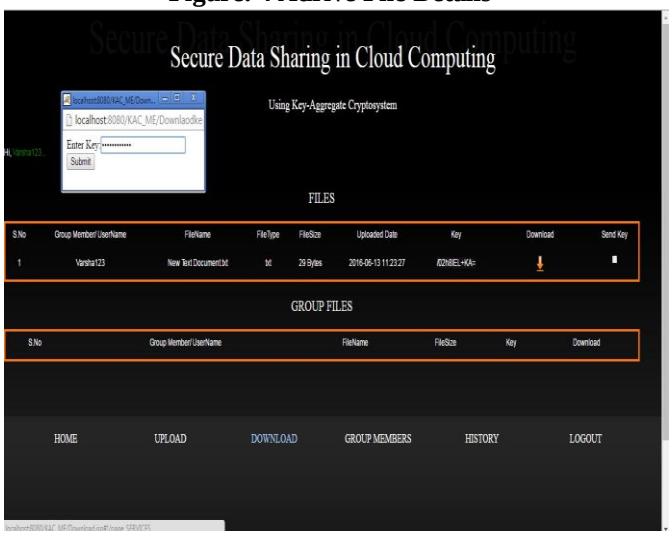

Figure. 5 Trapdoor Page

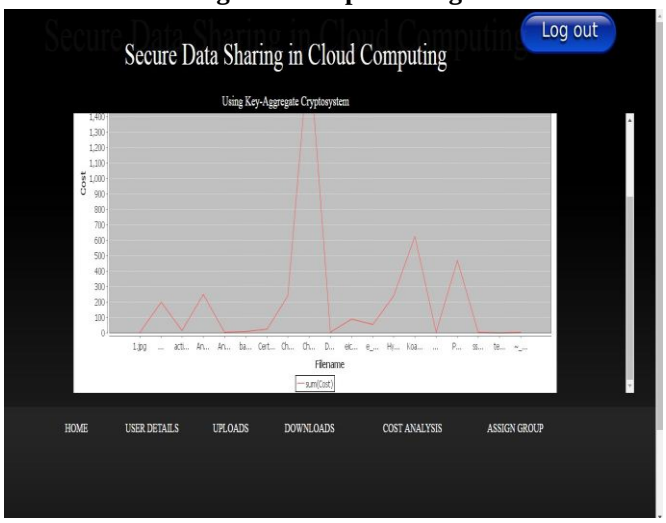

Figure. 6 System time Analysis

The below analysis graph shows that to encrypt and partition of our file data not vary to much with file size. To complete this analysis we perform execution on different files of different size. In this first size is of very small size till it taking same time as the file of size 1500 byte is taking. This time taken is for the operations such as key generation, file encryption, file partition and file upload on cloud. So analysis result shows that there is no much time variance even if file size increased.

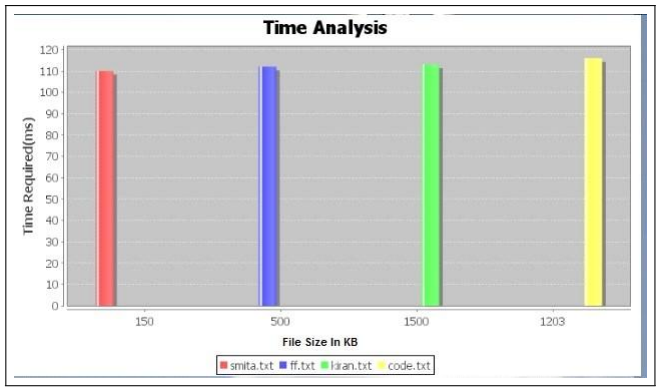

Figure. 7 Efficiency of Proposed System

VII CONCLUSION AND FUTURE WORK

We have addressed the issue of customized multi-keyword positioned look over encrypted cloud information. Considering the client search history, we built a client intrigue show for singular client with the assistance of semantic philosophy Word-Net. Through the model, we have acknowledged automatic assessment of the keyword need and settled the confinement of the simulated strategy for measuring. In addition, we propose two PRSE plans to explain two constraints (the model of ”one size fit all” and watchword correct hunt) in most existing accessible encryption plans. What’s more, intensive protection examination and execution investigation exhibits that our plan is practicable.

REFERENCES

1. Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou, `` Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data '', IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, January 2014.
2. Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang, `` A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data '', IEEE Transactions on Parallel and Distributed Systems, Vol. 27, No. 2, February 2016.
3. Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou, Xuemin (Sherman) Shen, `` Enabling FineGrained Multi-Keyword Search Supporting Classified Sub-Dictionaries over Encrypted Cloud Data '', IEEE Transactions on Dependable and Secure Computing, Vol. 13, No. 3, May/June 2016.
4. Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, Fengxiao Huang, `` Enabling Personalized Search Over Encrypted Outsourced Data With Efficiency Improvement '', IEEE Transactions on Parallel and Distributed Systems, Vol. 27, No. 9, September 2016.
5. Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, Weixin Xie, `` An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing '', IEEE Transactions on Information Forensics and Security, Vol. 11, No. 6, June 2016.
6. Z. Shen, J. Shu, and W. Xue, `` Preferred keyword search over encrypted data in cloud computing '', In Proc. of 21st International Symposium on Quality of Service (IWQoS'13), 2013.
7. C. Liu, L. Zhu, M. Wang, and Y. Tan, `` Search Pattern Leakage in Searchable Encryption : Attacks and New Constructions '', Cryptology ePrint Archive, Report 2013/163, 2013.
8. M. Islam, M. Kuzu, and M. Kantarcioglu, `` Access pattern disclosure on searchable encryption : Ramification, attack and mitigation '', In Proc.of NDSS'12, 2012.
9. C. Wang, K. Ren, S. C. Yu, and K. M. R. Urs, `` Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data '', in Proc. of IEEE INFOCOM 2012.
10. N. Cao, C. Wang, M. Li, K. Ren. W. J. Lou, `` Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data '', in Proc. of IEEE INFOCOM 2011.
11. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. j. Lou, `` Fuzzy keyword search over encrypted data in cloud computing '', in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March 2010.
12. C. Liu, L. H. Zhu, L. Li, and Y. Tan, `` Fuzzy Keyword Search on Encrypted Cloud Storage Data with Small Index '', in Proc. of IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), 2011.
13. C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, `` Secure Ranked Keyword Search over Encrypted Cloud Data '', in Proc. of IEEE 30th International Conference on Distributed Computing Systems (ICDCS), 2010.