OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

PERSONALIZED AND EFFICIENT SEARCH OVER ENCRYPTED DATA ON CLOUD: A SURVEY

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 paper, 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.**

Keywords: *Cloud security, outsourcing security, personalized search, user interest model.*

I INTRODUCTION

As of late, distributed computing has accomplished extraordinary advancement both in scholastic and industry groups as it gives financial and advantageous administration. Also, now an ever increasing number of organizations and clients want to transfer their information onto public cloud.

Be that as it may, information put away in the cloud may experience the malicious use by cloud specialist co-ops since information proprietors have never again direct control over information. Considering information protection and security, it is a prescribed practice for information proprietors to encrypt information before transferring onto the cloud. In spite of the fact that it shields information security from unlawful utilize both from untrusted cloud specialist co-ops and outside clients, it makes information usage more troublesome since numerous procedures in light of plaintext are not any more. Along these lines, investigating a productive look system for encrypted information is extremely urgent.

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 fulfil 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 input.

Accordingly, how to outline an accessible encryption scheme with help of both customized positioning and inquiry extension, is the issue that we attempt to handle in this paper. In this paper, for the first time, 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.

II RELATED WORK

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, and often sort the search outcomes.[1]

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 TF×IDF 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.[2]

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. In this paper, we address this issue by building up the fine-grained multi-watchword hunt plans over scrambled cloud information. Our unique commitments are three-fold. To begin with, we present the significance scores and inclination elements upon watchwords which empower the exact catchphrase seek and customized client experience. Second, we build up a handy and exceptionally effective multicatchphrase inquiry plan. The proposed plan can backing entangled rationale seek the blended "AND", "OR" and "NO" operations of catchphrases. Third, we further utilize the ordered sub-lexicons procedure to accomplish better proficiency on list building, trapdoor producing and question. Finally, we examine the security of the proposed plans as far as secrecy of reports, security assurance of file and trapdoor, and unlinkability of trapdoor. Through broad investigations utilizing this present reality dataset, we approve the execution of the proposed plans. Both the security examination and test results show that the proposed plans can accomplish the same security level contrasting with the current ones and better execution as far as usefulness, question multifaceted nature and effectiveness.[3]

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 search history, and adopt a scoring mechanism to express user interest smartly. To address the limitations of the model of "one size fit all" and keyword exact search, we propose two PRSE schemes for different search intentions .Extensive experiments on real-world dataset validate our analysis and show that our proposed solution is very efficient and effective.[4]

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. The cipher text components related to attributes could be shared by the files. Therefore,

both cipher text storage and time cost of encryption is saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.[5]

Sr. No.	Paper/Publication	Author	Methods
1	"A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, February 2016	Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang	Scheme supports dynamic update operations like deletion of documents and insertion of documents. Tree-based index structure and "Greedy Depth First Search" algorithms are use to provide efficient multi-keyword ranked search.
2	"Enabling Fine-Grained Multi-Keyword Search Supporting Classified Sub-Dictionaries over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, May/June 2016	Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou	Relevance scores and preference factors of keywords use to enable precise keyword search and personalized user experience. Support complicated logic search by using the mixed "AND", "OR" and "NO" operations of keywords. Classified sub-dictionaries technique is used to achieve better efficiency on index building, trapdoor generating and query.
3	Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, September 2016	Zhangjie Fu, KuiRen, JiangangShu, Xingming Sun, Fengxiao Huang	By using the user search history, a user interest model is build for individual user with the help of semantic ontology WordNet. The user interest model is use to realize automatic evaluation of the keyword priority and it solved the limitation of the artificial method of measuring
4	An Efficient File Hierarchy Attribute Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, June 2016	Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen	Uses Ciphertext-policy attribute-based encryption (CP-ABE) encryption technology to solve the challenging problem of secure data sharing in cloud computing. Efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing.
5	"Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Information Forensics and Security, January 2014	Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen	Propose two MRSE schemes based on the similarity measure of "coordinate matching" to provide as many matches as possible to effectively capture the relevance of outsourced documents to the query keywords while meeting different privacy requirements. "Inner product similarity" is used to quantitatively evaluate similarity measure.

III SYSTEM ARCHITECTURE

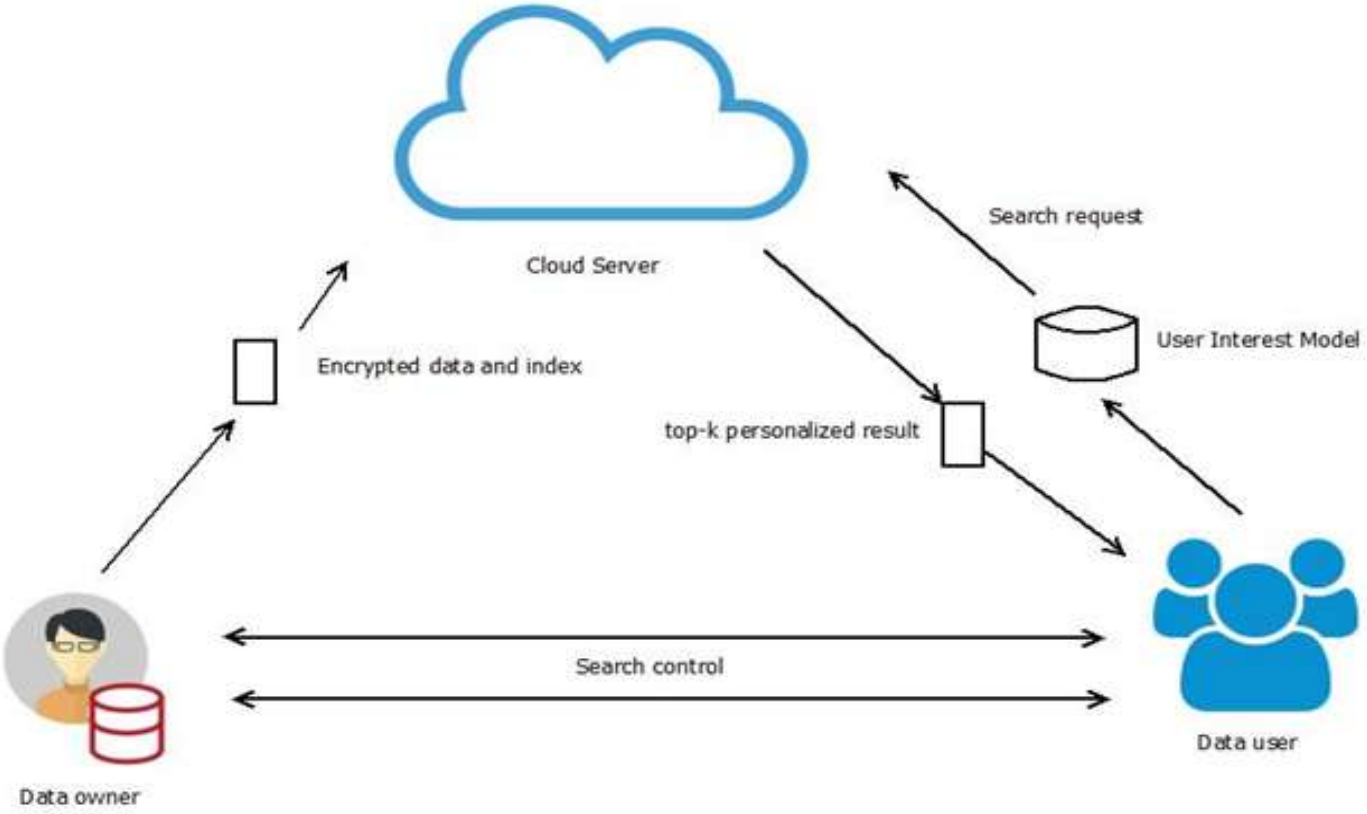

Figure 1 System Architecture

IV METHODOLOGY

Modules:

- **Data User Module:** This module includes the user registration login details.
- **Data Owner Module:**This module helps the owner to register them details and also include login details.
- **File Upload Module:**This module help the owner to upload his file with encryption using RSA algorithm. This ensures the files to be protected from unauthorized user.
- **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.
- **Decryption**
  - View Uploaded and Downloaded File: This module allows the Owner to view the uploaded files and downloaded files

V APPLICATIONS

- Cloud computing

VI CONCLUSION AND FUTURE WORK

In this paper, we address 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 WordNet. 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, KuiRen, 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, XinhuiWang, 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, KuiRen, JiangangShu, 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, WeixinXie, "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, http://eprint.iacr.org/ .

[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, 2012, pp. 451-459.

[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, 2011, pp. 829-837.

[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, pp. 269-273.

[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, pp. 253-262.