International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

The Keywords of the Depth of the First Encoding Data on Greedy Algorithm Nube

[1]SANDELA KIRAN KUMAR [2]P NAGESWARA RAO

[1] PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

[2]Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206

ABSTRACT:

Due to the growing popularity of cloud computing, more and more data owners are willing to outsource their data Cloud great service for the convenience and cost reduction in the field of data management. However, you should encrypt sensitive data before Outsourcing to meet specific needs, which obsoletes the use of data, such as document retrieval by keyword. In this paper, we present Multi-word search safer place cloud encrypted data, which supports the plan revaluations dynamics same time Such as inserting and deleting documents. Specifically, the combination of vector space model is used in a large scale TF? model FIL Building index and generate query. We build the index structure based on your tree and propose "greed depth I. Search "algorithm is effective to provide a search for multiple words in the place. KNN algorithm is used to encrypt Index safe and consultation Tankers, and at the same time guarantee the accuracy of the result calculated link between the vectors index query and encrypted. In order to resist He added statistical ghost where vectors attacks against the index result is blindness. This is because the use of our private tree based index structure, the proposed system can achieve sub-time search of sin and deal with the insertion and removal of documents flexibly. And I conducted extensive tests to demonstrate the effectiveness of the proposed plan.

1 INTRODUCTION

Cloud computing as new was considered Model of the infrastructure of the institutions of information technology, which can be Organize vast resources of the computing and storage applications, And enable users to enjoy ubiquitous, convenient

And on-demand network access to a common set of Configurable computing resources with great efficiency And a minimum of economic overhead [1]. Attracted by this Attractive features, both individuals and companies and Motivated to outsource their data to the cloud, rather than The purchase of hardware and software for data management themselves. In spite of the various advantages of cloud services, Outsourcing sensitive information sources (such as e-mail messages, and personal Health records, financial company data, government Documentation, etc.) to serve remote areas brings privacy concerns. Cloud service providers (CSPs) that keeps Data users have access to sensitive information of users Without a license. General approach to protect Confidentiality of data is to encrypt the data before Outsourcing [2]. However, this leads to a huge cost in Terms of usability data. For example, current technologies On the basis of word retrieval of information, whichUsed widely on the encrypted data can not be directly Applied to the encrypted data. Download all And decoding data from the cloud locally Obviously it is not practical. In order to address the above problem, researchers Some solutions have been designed for general purpose with Fully homomorphic encryption [3] or RAMs oblivious [4]. However, these methods are not due to process High computational overhead for each of the Cloud Cut and the user. On the contrary special purpose, more realistic Solutions, such as encryption research (SE) Made specific in terms of contribution schemes Efficiency and functionality and security. Encryption Search Enables the client plans to store encrypted data To the cloud and execute the search for keywords on the ciphertext Domain. So far, the proposal has been abundant work Under different threat to discuss various models Functions, such as a single search words, similarity Search and multi-word search logical, and search the place, Multi-word search in the place, and so forth, including, multi keyword Search achieves ranked more and more attention Practical application. Recently, some of the dynamic It plans to support the introduction and has proposed Delete operations on the collection of documents. here they are Important work and it is very possible that the data Owners need to update their data on the cloud server. But a small number of dynamic support multi keyword efficiency schemes Search ranked. This paper proposes the research plan based on a safe tree Data encrypted cloud, which supports multi keyword Search

ranked and dynamic process Collection of documents. Specifically, the model space vectors Used on a large scale, "the term frequency (TF) × inverse document. And summed up our contributions

As follows:

1) We design encryption system can be searched It supports both multi-word minutes Grade Find a flexible and dynamic process to a close Collection.

2) Due to the special structure of the index based on our tree, The complexity of the search of the proposed scheme I kept basically logarithmic. In practice, The proposed plan can achieve higher search Efficiency through our implementation of the "greed depth I. Search "algorithm. Moreover, it can be parallel search Implementation flexibility to further reduce the cost of time Of the research process.

2. RELATED BUSINESS

Encryption software enables to search for clients to store Encrypted data to the cloud and the implementation of the floor Search through the ciphertext scale. Because of different encryption Primitives, it can be encryption schemes Search Constructed using public key cryptography based on [5], [6] Or symmetric key encryption based on [7] [8] [9] [10]. Song et al. [7] proposed a symmetric first search Encryption (SSE) scheme, and the time in search of their

Line chart to the size of the data collection process. Goh [8] proposed a formal security definitions of small businesses and Design a plan based on the Bloom filter. Search Time of the faces of the scheme is O (n), where n is the origin of From the collection of documents. Curtmola and others. [10] Suggested planners (SSE-1 and SSE-2) investigating While search engine optimization. Scheme SSE-1 is safe Against the selection of keywords attacks (CKA1) and SSE-2 Insurance against attacks on selected word adjustment (CKA2). This early work is one logical search keywords

Drawings, which are very simple in terms of functionality. After that, it was proposed and plentiful work under Different threat to the investigation and search functions of various models, Such as searching for a word, and the search for similarities

[11], [12], [13], [14] and multi-word search logical [15], [16], [17], [18] [19] [20], [21], [22], and research in place [23], [24] [25], and multi-word search in rank [26], [27],

[28], [29], etc. Find logical multi keywords allows users to Enter multiple query to request appropriate documentation keywords. Among these works, searching for keywords connected Schemes [15], [16],

[17] only returns documents Containing all the main query words. Call contrapuntal Research programs [18] [19] the return of all documents That contains a subset of the query words. Predicate Research programs [20], [21], [22] proposes to support Both associated stratiform and research. All these multikeyword Find retrieve search on the basis of the results of programs On the existence of keywords, which can not provide As a result acceptable positions respectively. Ranked research can enable the quick search more Relevant data. Only send top as the most relevant Documents can effectively reduce network traffic. Some Early works [23], [24], [25] it has realized ranked Search using techniques to maintain order, but it's Designed only to search for a single word. Cao et al. I realized [26] The first-floor maintaining multiple Privacy Grade planned research, in the documents and inquiries Its a carrier the size of a dictionary. With the "Matching Format", are arranged according to the documents For a number of keyword query matching. However, Cao and others in the scheme is not considered The importance of different words, and therefore not Accurate enough. In addition, the efficiency of the search Line chart with the origin of the documents set. Sun and others. Provided [27] and secure multi-word The research plan that supports the order based on the similarity. The book constructed index based tree to look The space vector model and measure approved cosine pocket Along with the team × Israeli army to present the results of arrangement. Sun et al. Allah. To search algorithm achieves better than linear search But the efficiency and results in a loss of accuracy. ô rencik and others. [28] Proposed multi-word search safe way Using sensitive hash (LSH) local jobs to the cluster And similar documents. Suitable algorithm LSH To search a similar but could not provide the exact ranking. At [29], Zhang and others. It proposed a plan to deal with safer Multi-word search rank in a multi-owner model. At This scheme, owners of the various data using different Secret Documents and keywords encryption keys while in Authorized users can query data without knowing the keys Of the owners of these different data. Proposed book And "added the order to maintain the function" to recover Most relevant search results. However, these actions do not Support vital processes.

3. DESIGN GOALS

Multikeyword to enable safe, efficient, accurate and dynamic Ranked search on

encrypted cloud outsourcing and constructed based on the vector space model The tree KBB. Based on UDMRS planned, two safe Is constructed research programs (BDMRS and EDMRS schemes) The threat against the two models, respectively.

4. EDMRS SCHEME

The security analysis above shows that the BDMRS scheme can protect the Index Confidentiality and Query Confidentiality in the known ciphertext model. However, the cloud server is able to link the same search requests by tracking path of visited nodes. In addition, in the known background model, it is possible for the cloud server to identify a keyword as the normalized TF distribution of the keyword can be exactly obtained from the final calculated relevance scores. The primary cause is that the relevance score calculated from Iu and TD is exactly equal to that from Du and Q. A heuristic method to further improve the security is to break such exact equality. Thus, we can introduce some tunable randomness to disturb the relevance score calculation. In addition, to suit different users' preferences for higher accurate ranked results or better protected keyword privacy, the randomness are set adjustable. The enhanced EDMRS scheme is almost the same as BDMRS scheme except that:

• SK ← Setup() In this algorithm, we set the secret vector S as a m-bit vector, and set M1 and M2 are (m + m′) × (m + m′) invertible matrices, where m′ is the number of phantom terms. • I ← GenIndex(F; SK) Before encrypting the index vector Du, we extend the vector Du to be a (m+m′)-dimensional vector. Each extended element Du[m+ j], j = 1; :::;m′, is set as a random number "j . • TD ← GenTrapdoor(Wq; SK) The query vector Q is extended to be a (m + m′)-dimensional vector. Among the extended elements, a number of m″ elements are randomly chosen to set as 1, and the rest are set as 0.

• RelevanceScore ← SRScore(Iu;TD) After the execution of relevance evaluation by cloud server, the final relevance score for index vector Iu equals to Du · Q + Σ "v, where v ∈ {j|Q[m + j] = 1}.

Security analysis. The security of EDMRS scheme is also analyzed according to the three predefined privacy requirements in the design goals:

1) Index Confidentiality and Query Confidentiality: Inherited from BDMRS scheme, the EDMRS scheme can protect index confidentiality and query confidentiality in the known background model. Due to the utilization of phantom

terms, the confidentiality is further enhanced as the transformation matrices are harder to figure out [38].

2) Query Unlinkability: By introducing the random value ", the same search requests will generate different query vectors and receive different relevance score distributions. Thus, the query unlinkability is protected better. However, since the proposed scheme is not designed to protect access pattern for efficiency issues, the motivated cloud server can analyze the similarity of search results to judge whether the retrieved results come from the same requests. In the proposed EDMRS scheme, the data user can control the level of unlinkability by adjusting the value of Σ "v. This is a trade-off between accuracy and privacy, which is determined by the user.

3) Keyword Privacy: the BDMRS scheme cannot resist TF statistical attack in the known background model, as the cloud server is able to deduce/identify keywords through analyzing the TF distribution histogram.

5. DYNAMIC UPDATE OPERATION OF DMRS

After insertion or deletion of a document, we need to update synchronously the index. Since the index of DMRS scheme is designed as a balanced binary tree, the dynamic operation is carried out by updating nodes in the index tree. Note that the update on index is merely based on document identifies, and no access to the content of documents is required.

6. CONCLUSION AND FUTURE WORK

In this paper, a safe, effective and dynamic search It is proposed that the scheme, which supports not only accurate Multi-word search rank but also dynamic Deletion and insertion of documents. Build Especially keywords balanced binary tree as the index, The proposal "Greedy depth first search" algorithm for Get the best of linear search efficiency. In addition to, You can search process parallel to conduct more Reduce the cost of time. Security scheme Two models protected against the threat of using safe KNN algorithm. The experimental results show The efficiency of our proposed plan.

There are still many problems in the challenge symmetric SE schemes. In the proposed plan, the owner of the data It is responsible for generating complete information and Sent to the cloud server. Thus, the owner of the data It needs to store non-encrypted index information tree That are necessary to recalculate the IDF values.

This active data owner may not be very suitable for Cloud computing model. It can be meaningful But the future is difficult to work on the design of dynamic search Encryption system, which can be a process of modernization The completion of the only cloud server, and at the same retention time The ability to support multi-word search rank. At In addition, as most of the work on encryption research, The scheme basically our challenge Cloud server. In fact, there are many safe challenges In a multi-user system. First, all users are usually Maintaining the same secure key generation trapdoor in SE symmetric scheme. In this case, the abolition of the The user is the big challenge. If there was a need to cancel the user in This scheme, we need to re-create the index and distribution New keys safe for all authorized users. Second, Usually symmetric schemes SE assume that all data Trustworthy users. It is not practical and dishonest And users of the data leads to many problems safe. For example, The user can search the data dishonest in the documentation and Distribution of documents decoder for unauthorized Of which. More than that, you may distribute the user dishonest data

7.**REFERENCES**

[1] K. Ren, C.Wang, Q.Wang *et al.*, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136–149.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," *Journal of the ACM (JACM)*, vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology-Eurocrypt 2004*. Springer, 2004, pp. 506–522.

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in *Advances in Cryptology-CRYPTO 2007*. Springer, 2007, pp. 50–67.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P*

2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–
55.

[8] E.-J. Goh *et al.*, "Secure indexes." *IACR Cryptology ePrint Archive*,
vol. 2003, p. 216, 2003.

[9] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword
searches on remote encrypted data," in *Proceedings of the Third international conference on Applied Cryptography and Network Security*.
Springer-Verlag, 2005, pp. 442–455.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable
symmetric encryption: improved definitions and efficient constructions,"
in *Proceedings of the 13th ACM conference on Computer
and communications security*. ACM, 2006, pp. 79–88.

[11] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy
keyword search over encrypted data in cloud computing," in
INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–5.

[12] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity
search over encrypted data," in *Data Engineering (ICDE), 2012
IEEE 28th International Conference on*. IEEE, 2012, pp. 1156–1167.

[13] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and
privacy-assured similarity search over outsourced cloud data," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 451–459.

[14] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword
fuzzy search over encrypted data in the cloud," in *IEEE
INFOCOM*, 2014.

[15] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword
search over encrypted data," in *Applied Cryptography and Network
Security*. Springer, 2004, pp. 31–45.

[16] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive
keyword search and its extension to a multi-user system,"
in *Proceedings of the First international conference on Pairing-Based
Cryptography*. Springer-Verlag, 2007, pp. 2–22.

[17] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive
keyword searches over encrypted data," in *Proceedings of*

the 7th international conference on Information and Communications Security. Springer-Verlag, 2005, pp. 414–426.

[18] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proceedings of the 4th conference on Theory of cryptography*. Springer-Verlag, 2007, pp. 535–554.

[19] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 262–267, 2011.

[20] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology–EUROCRYPT 2008*. Springer, 2008, pp. 146–162.

[21] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*. Springer-Verlag, 2009, pp. 457–473.

[22] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques*. Springer-Verlag, 2010, pp. 62–91.

[23] 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," in *Proceedings of the 2007 ACM workshop on Storage security and survivability*. ACM, 2007, pp. 7–12.

[24] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Topk retrieval from a confidential index," in *Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology*. ACM, 2009, pp. 439–449.

[25] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 8, pp. 1467–1479, 2012.

[26] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *IEEE INFOCOM*, April 2011, pp. 829–837.

[27] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM, 2013, pp. 71–82.

[28] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*. IEEE, 2013, pp. 390–397.

[29] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*. IEEE, 2014, pp. 276–286.

[30] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 965–976.

[31] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 258–274.

[32] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ros¸u, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in *Advances in Cryptology–CRYPTO 2013*. Springer, 2013, pp. 353–373.

[33] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: Data structures and implementation," in *Proc. of NDSS*, vol. 14, 2014.

[34] C. D. Manning, P. Raghavan, and H. Sch ¨ utze, *Introduction to information retrieval*. Cambridge university press Cambridge, 2008, vol. 1.

[35] B. Gu and V. S. Sheng, "Feasibility and finite convergence analysis

for accurate on-line -support vector learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 24, no. 8, pp. 1304–1315, 2013.

[36] X. Wen, L. Shao, W. Fang, and Y. Xue, "Efficient feature selection and classification for vehicle detection."

[37] H. Delfs and H. Knebl, *Introduction to cryptography: principles and applications*. Springer, 2007.

[38] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*. ACM, 2009, pp. 139–152.

[39] "Request for comments," http://www.rfc-editor.org/index.html.

AUTHOR'S PROFILE:

SANDELA KIRAN KUMAR

PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

P NAGESWARARAO,

Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206