International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Privacy preserving search scheme over encrypted data in cloud

S. Himachand
MCA, Sri Padmavathi College of Computer Sciences and Technology , Tiruchanoor, Andhra Pradesh, India

ABSTRACT

Due to the increasing quality of cloud computing, more and more information owners are actuated to source their information to cloud servers for nice convenience and reduced price in information management. However, sensitive information ought to be encrypted before outsourcing for privacy necessities, that obsoletes information utilization like keyword-based document retrieval. during this paper, we present a secure multi-keyword stratified search theme over encrypted cloud information, that at the same time supports dynamic update operations like deletion and insertion of documents. Specifically, the vector area model and therefore the widely-used TFIDF model are combined in the index construction and question generation. we construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithmic rule to produce economical multi-keyword stratified search. The secure kNN algorithmic rule is employed to cipher the index and question vectors, and in the meantime guarantee correct connection score calculation between encrypted index and question vectors. so as to resist statistical attacks, phantom terms are additional to the index vector for bright search results . owing to the utilization of our special tree-based index structure, the planned theme can do sub-linear search time and upset the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the potency of the planned theme.

Keywords: Searchable encryption, multi-keyword ranked search, dynamic update, cloud computing

I. INTRODUCTION

Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications, and alter users to relish present, convenient and on-demand network access to a shared pool of configurable computing resources with nice potency and least economic overhead. Attracted by these appealing options, each people and enterprises are motivated to source their knowledge to the cloud, instead of purchasing package and hardware to manage the information themselves.

Despite of the varied benefits of cloud services, outsourcing sensitive data (such as e-mails, personal health records, company finance knowledge, government documents, etc.) to remote servers brings privacy considerations. The cloud service suppliers (CSPs) that keep the data for users could access users' sensitive data without authorization. A general approach to guard the data confidentiality is to encrypt the data before outsourcing. However, this can cause an enormous value interms of knowledge usability. for instance, the prevailing techniqueson keyword-based data retrieval, which are wide used on the plaintext data, can not be directlyapplied on the encrypted knowledge. Downloading all thedata from the cloud and decipher domestically is clearlyimpractical.

In order to handle the on top of downside, research have designed some all-purpose solutions withfully-homomorphic encoding or oblivious RAMs.

However, these strategies don't seem to be sensible as a result of their high procedure overhead for each the cloud sever and user. On the contrary, additional sensible special purpose solutions, like searchable encoding (SE) schemes have created specific contributions in terms of efficiency, practicality and security. Searchable encoding schemes alter the shopper to store the encrypted knowledge to the cloud and execute keyword search over cipher text domain. So far, copious works are projected under completely different threat models to realize numerous search functionality, like single keyword search, similarity search, multi-keyword boolean search, graded search, multi-keyword graded search, etc. Among them, multikeyword ranked search achieves additional and additional attention for its sensible pertinence. Recently, some dynamic schemes are projected to support inserting and deleting operations on document assortment. These are significant works because it is extremely attainable that the information owners got to update their knowledge on the cloud server. But few of the dynamic schemes support economical multikeyword ranked search.

In existing system we propose a secure framework for outsourced privacy-preserving storage and retrieval in large shared image repositories. Our proposal is based on IES-CBIR, a novel Image Encryption Scheme that exhibits Content-Based Image Retrieval properties. The framework enables both encrypted storage and searching using Content-Based Image Retrieval queries while preserving privacy against honest-but-curious cloud administrators. We have built a prototype of the proposed framework, formally analyzed and proven its security properties, and experimentally evaluated its performance and retrieval precision. But there is no security for the data which we are sending. This paper proposes a secure tree-based search theme over the encrypted cloud knowledge, that supports multikeyword ranked search and dynamic operation on the document assortment. Specifically, the vector area model and the widely-used “term frequency (TF) × inverse document frequency (IDF)” model area unit combined within the index construction and question generation to produce multikeyword ranked search. so as to get high search efficiency, we have a tendency to construct a tree-based index structure and propose a “Greedy Depth-first Search” rule primarily based on this index tree. attributable to the special structure of our tree-based index, the projected search theme will flexibly achieve sub-linear search time and influence the deletion and insertion of documents. The secure kNN algorithm is used to code the index and question vectors, and in the meantime guarantee correct connectedness score calculation between encrypted index and question vectors. To resist completely different attacks in numerous threat models, we construct 2 secure search schemes: the fundamental dynamic multi-keyword hierarchal search (BDMRS) theme within the known ciphertext model, and therefore the increased dynamic multi-keyword hierarchal search (EDMRS) theme within the known background model. Our contributions area unit summarized as follows:

1) we have a tendency to style a searchable encoding theme that supports each the correct multi-keyword hierarchal

search and versatile dynamic operation on document collection.

2) attributable to the special structure of our tree-based index, the search quality of the projected theme is fundamentally unbroken to index. And in observe, the projected theme can do higher search efficiency by capital punishment our “Greedy Depth-first Search” rule. Moreover, parallel search is flexibly performed to more scale back the time price of search method.

II. ALGORITHM

Greedy Depth first Search (GDFS)

The search process of the UDMRS scheme is a recursive procedure upon the tree, named as “Greedy

Depthfirst Search (GDFS)” algorithm. We construct a result list denoted as RList, whose element is defined as (RScore; FID). Here, the RScore is the relevance score of the document fFID to the query. The RList stores the k accessed documents with the largest relevance scores to the query. The elements of the list are ranked in descending order according to the RScore, and will be updated timely during the search process.

RScore(Du;Q)– The function to calculate the relevance score for query vector Q and index vector Du stored in node u.
kthscore– The smallest relevance score in current RList, which is initialized as 0.
hchild– The child node of a tree node with higher relevance score.
lchild– The child node of a tree node with lower relevance score. Since the possible largest relevance score of documents rooted by the node u can be predicted, only a part of the nodes in the tree are accessed during the search process.

```
if the node u is not a leaf node then
    if RScore(Du;Q) > kthscore then
        GDFS(u:hchild);
        GDFS(u:lchild);
    else
        return
    end if
else
    if RScore(Du;Q) > kthscore then
        Delete the element with the smallest relevance score from RList;
        Insert a new element ⟨RScore(Du;Q); u:FID⟩ and sort all the elements of RList;
    end if
    return
end if
```

III. CONCLUSION

In this paper, a secure, economical and dynamic search scheme is planned, that supports not solely the correct multi-keyword graded search however additionally the dynamic deletion and insertion of documents. we have a tendency to construct a special keyword balanced binary tree because the index, and propose a “Greedy Depth-first Search” algorithmic rule to obtain higher potency than linear search. additionally, the parallel search method is administered to additional reduce the time price. the safety of the theme is protected against 2 threat models by mistreatment the secure kNN algorithmic rule.

IV. 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.

ABOUT AUTHOR:

S.HIMACHAND is currently pursuing his MCA in MCA Department, Sri Padmavathi College of Computer Science & Technology, Tirupathi, AP. He Received Bachelor of Science From SVU