IMPROVED SEARCH AND ACCESS CONTROL MECHANISM FOR OUTSOURCED ENCRYPTED CLOUD DATA

[1]M.Kowsalya, [2]Ms.G.SriVidhya
[1]Student, M.E,Computer Science and Engineering,
Sona College of Technology,Salem,Tamil Nadu,India
[2]Assistant Professor, M.Tech, M.S,Computer Science and Engineering,
Sona College of Technology,Salem,Tamil Nadu,India

Abstract:

Cloud computing enables data owner to store their data remotely in cloud and to enjoy the on-demand access with high quality application and share the services from a pool with configurable computing resources. In this paper, as a first attempt, we solve the problem for searching data from cloud and implement the framework for supporting efficient ranked keyword search for utilize the data in encrypted cloud resources. We first give similarity computation for encrypted data. Efficient Multi-keyword Ranked Search(EMRS) framework is proposed using Cipher Text policy encryption algorithm and K-Nearest Neighbour classification technique. Using Cipher Text policy-Attribute Based Encryption(CP-ABE) algorithm to encrypt the cloud data and calculate the similarity computation to construct the index table and ranked based term frequency. Finally implement KNN classification technique to retrieve the data from cloud in reduced response time in secure manner. Finally, the user accesses the documents through the access control mechanism. So implement attribute based access control mechanism to provide restricted permission to authorized users and overcome the user revocation problem. The experimental results can be implementing in mobile cloud computing environment.

Keywords: Multi Keyword search, Ranking, Indexing, Classification, Access control

Introduction: With the development of cloud computing, more and more users to provide new computing framework for access the data conveniently in shared pool of resources. This computing provides ubiquitous and flexible access and on-demand resource configuration and various computing resources with very low price. In spite of these conveniences, data owner may loses their data and handle various risks because of direct access and control over their information. Privacy settings becomes the important barrier that hiders is embracing cloud storage by corporations. To protect privacy of data and anonymous accesses in the cloud and beyond, sensitive data, e.g., emails, personal health records, photo albums, tax related documents, files including financial transactions, etc., may have to be encrypted by data owners before outsourcing to the commercial public cloud, this may be traditional data utilization service depend on plaintext keyword search. The trivial solution of retrieving all data by downloading and decrypting them for accessing locally is clearly impractical, due to the increasing amount of bandwidth cost in cloud systems. Thus, exploiting privacy preservation and effective searching in encrypted cloud data is main role in cloud storage. And considering the large number of data users in on-demand and huge amount of outsourced data storage in the cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements includes performance analysis, scalability limits and usability needs. On the one hand, to meet the effective data retrieval need, the massively huge amount of corpora demand the cloud server to produce result relevance ranking, instead of returning undifferentiated outcomes. Such searching and ranking system enable users in cloud to gather the most relevant information quickly, rather than burdensomely classifying data through every match in the collected contents

Ranked search can also elegantly eliminate unnecessary traffics in network by sending back only the data that are relevant to the topic, which is greatly popular in the "pay-as-you use" cloud paradigm. For protecting data in privacy, need for ranking operation arise, however, should not leak any information regarding keywords. On the other hand, to improve the growth of search result accuracy and also to enhance the user searching experience, thus enhancing such ranking system in order to support multiple keywords search, as single keyword search often yields far too coarse results.

Related work:

[1] study cloud resource allocation in a multi-domain mobile cloud system that has the following properties: 1) Both the starting point and its ending point of mobile cloud services follow Poisson distribution; 2) the available resource of the cloud is time dependent; and 3) current resource allocating decision may have a big impact on the future decision. In a multi-domain systems of cloud, problem raises in the overall performance degradation in systems, if the mobile cloud system does not consider the relationship that occur between current and future needs in terms of the decision making in allocating resources and its outcomes.

[2] define a hotspot occurrence that cause an noticeable inconsistency in the network traffic prototype due to a great volume of packets originating from a tiny area. Hotspots can be shaped for diverse reasons, e.g., when pandas have bulk of data or spend some time in one region due to the accessibility of food, shadow, shelter, water, etc. Second, we extend a practical adversary model assuming that the adversary has a part view to the network traffic by issue a group of watching devices at different observation points.

[3] propose a resource allocation scheme to achieve the minimized service delay and the reduced communication costs. We first derive a sufficient condition in resource allocation to ensure the stability of cloud servers. Considering this situation, we need to design the resource allocation scheme: each server only redirects the requests to others who have minimum queues in their lengths; and increasing number of redirected requests must be proportioned to the difference of their queue lengths and reciprocal to the service delay between them. We also prove that the proposed resource allocation scheme satisfies the derived sufficient condition in the balanced state.

[4] technology can assist mobile users beat the limitations of cloud computing owed to wide area network latency and low bandwidth. However, there are several considerations that require to be addressed before idea preserve be applied extensively in practical system. First, web interface is not specially designed for mobile devices. Therefore, web interface may contain more overhead. Also, compatibility between devices for web interface can be an issue. In this case, the typical protocol, signaling, and interface for interacting between mobile users and cloud would be required to guarantee seamless services.

[6] address the challenges of constructing practically efficient and flexible encrypted search functionalities that support result ranking and multi-keyword queries. In particular, to support multi-keyword queries and search result ranking functionalities, we plan to construct the search index found on the vector space model, i.e., cosine measure, and incorporate the TF × IDF weight to achieve elevated search result accuracy. To develop the search efficiency, we suggest a tree-based index structure, where each value in a node is a vector of term frequency related information.

Existing methodology:

In existing approach, provide privacy and secure ranked multi-keyword search on remotely stored encrypted database model where the database users are protected against privacy violations. We first define the security requirements for the given problem. We then employ a secure usage of the method given for practical application scenarios where total number of keywords that can be searched is relatively limited and there are only few search terms in a query by using a trapdoor based system where the trapdoor can only be generated by the data owner. We appropriately increase the efficiency of the scheme by using symmetric-key encryption method rather than public-key encryption for document encryption. We also propose to use the blinded encryption technique in accessing the contents of the retrieved documents without revealing them to other parties. We prove that this method satisfies the security requirements. This ranking method proves to be efficient to return highly relevant documents corresponding to submitted search terms based KNN approach as in fig 1.

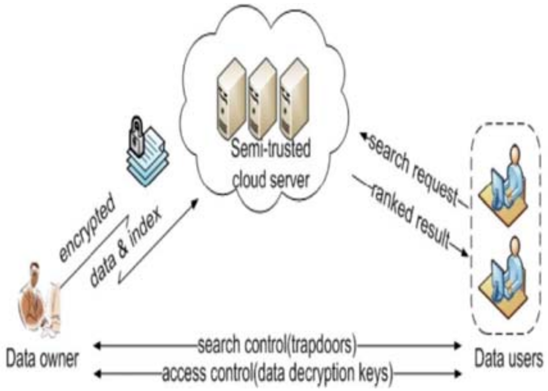
Semi-trusted cloud server
encrypted data & index
search request
ranked result
Data owner
Data users
search control(trapdoors)
access control(data decryption keys)

Fig 1.Existing framework

Proposed methodology:

Security and privacy are very significant issues in cloud computing. Access control in traditional system is centralized manner and the scheme uses asymmetric key approach and does support authentication. Asymmetric key algorithm uses pair of keys for both encryption and decryption. The provider takes a centralized approach where owner dispatches the secret keys and attributes to all users. In this paper, we can implement new approach that is multi data users approach to supports anonymous authentication. The user is authenticated using attributes that are issued by data owner. The proposed scheme is flexible to replay attacks and using cipher text attribute based encryption (CP-ABE) for authentication purpose; ABE is the one of several cryptographic algorithms, and often used to verify file based on attributes. And also implement attribute based access control whereby access privileges are granted to users during the use of policies which merge attributes together. The policies can use any type of attributes (user attributes, resource attributes, environment attribute etc.). Accordingly, a policy based access control known as Attribute Based Access Control (ABAC) came into existence. In ABAC, access is granted on attributes that the user could prove to have such as date of birth or national number. We can implement this process in real time cloud environments and improve accuracy of the system and illustrated in fig 2.

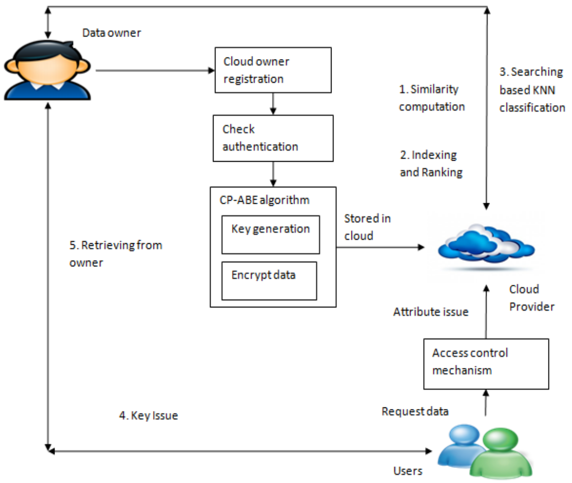

Fig 2. Proposed Architecture diagram

Experimental Results:

This type of ranked keyword search enhances the efficient usage of outsourced files by providing Inter cloud communication constantly between data owners and users. So that the cloud server learn nothing from the data uploaded by data owners. The search time is not affected while fetching the posting list in the index, decrypting, and rank ordering each entry. The experimental results provide parameters such as storage overhead, communication cost and computational efficiency and the storage overhead is one of the most significant issues of the access control scheme in cloud storage systems. In our scheme, besides the storage of attributes, each provider also needs to store a public key and a secret key for each user in the system. Thus, the storage overhead on provider in our scheme is also linear to the number of in the system. The communication cost of the normal access control is almost the same. The communication cost of attribute revocation is linear to the number of cipher texts which contain the revoked attribute. We compare the computation efficiency of both encryption and decryption in two criteria: the number of authorities and the number of attributes per authority is shown in diagrammatic representation of storage overhead, computation efficiency and communication cost.

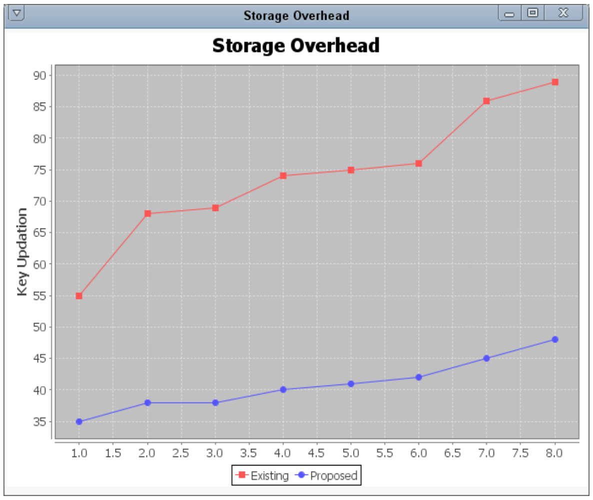

Fig 4. Storage overhead

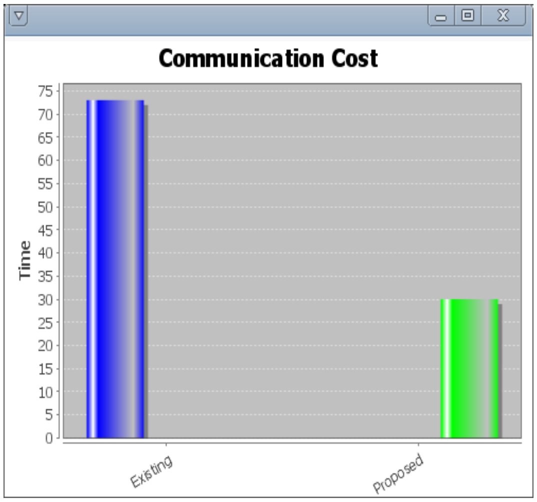

Fig 5.Communication cost

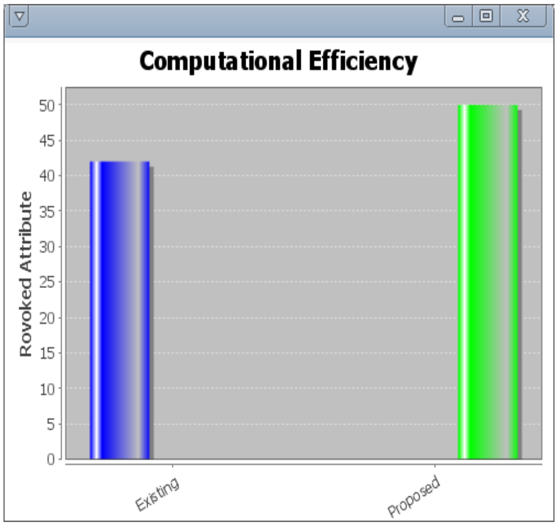

Fig 6. Computational efficiency

Conclusion:

In this paper, we propose an efficient search approach to supports multi-keyword ranked search and employs CP-ABE algorithm to encrypt the data and create index table and efficient search patterns for multi-keyword ranked search and then implement similarity computation approach for retrieving data quickly in blind cloud storage system. And implemented access control mechanism for secure the data from unauthorized system to simplify the file access control to the privilege control, by which rights of all operations on the cloud data can be handled in a fine-grained manner. The experiment results reveals that our scheme can permit the encrypted multi-keyword ranked search service for anonymous access with high efficiency in cloud computing.

References:

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, ``An SMDP-based service model for inter domain resource allocation in mobile cloud networks," IEEE Trans. Veh. Technol., vol. 61, no. 5, pp. 2222-2232, Jun. 2012.

[2] M. M. E. A. Mahmoud and X. Shen, “A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 10, pp. 1805-1818, Oct. 2012.

[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo, ``Exploiting geo-distributed clouds for a e-health monitoring system with minimum service delay and privacy preservation," IEEE J. Biomed. Health Inform. vol. 18 no. 2, pp. 430-439, Mar. 2014.

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, ``A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587-1611, Dec. 2013.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, ``Identity-based authentication for cloud computing," in Cloud Computing. Berlin, Germany: Springer-Verlag, 2009, pp. 157-166.

[6] W. Sun, et al., ``Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur., 2013, pp. 71-82.

[7] B.Wang, S.Yu,W. Lou, andY. T. Hou, ``Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2112 - 2120.

[8] E. Stefanov, C. Papamanthou, and E. Shi, ``Practical dynamic searchable encryption with small leakage," in Proc. NDSS, Feb. 2014.
[9] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, ``Secure dynamic searchable symmetric encryption with constant document update cost," in Proc. GLOBECOM, Anaheim, CA, USA, 2014.
[10] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rou, and M. Steiner ``Highly-scalable searchable symmetric encryption with support for Boolean queries," in Proc. CRYPTO, 2013, pp. 353-373.