RESEARCH ARTICLE OPEN ACCESS

Secure Syntactic key Ranked Search over Encrypted Cloud in Data

Kasula Rama Gopi [1]Vemula Rajiv Jetson [2]B. Satyanarayana Reddy[3] Dr. B. Tarakeswara Rao [4]

[1] PG Student,Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P.
[2]Assoc.Professor, Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P
[3]Assoc.Professor,HOD, Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P
[4]Professor, Dept of CSE,Kallam Haranadhareddy Inst of Technology,NH-5 Guntur(dt),A.P

ABSTRACT

In Today's world cloud computing is one of the most effective data storage centre. The data owners usually want to share or outsource their data. They find cloud is the alternative storage data centre to outsource their data from local sites to cloud server. Outsourcing data will have great flexibility and economically effective. Usually outsourcing data is sensitive data. So we need to provide some security to that data.

As data is sensitive we use access control mechanisms to stop accessing unauthorized users in clouds. The data must be encrypted before it is going to outsource. Which obsoletes traditional data utilization based on plaintext keyword search Thus, enabling an encrypted cloud data search service is of paramount importance. Cloud usually maintains multiple users and also stores huge amount of data in it. In the proposed system we use a multiple search keyword for searching most relevant data stored in clouds. In early system, the scheme is entirely focused on single key search or a Boolean keyword search.

In implementing system we overcome the all the problems in the existing system like single key search technique, unauthorized users access on data stored in clouds. We used Access Control method to to avoid unauthorized access from data stored in clouds. For multi keyword search we proposed "coordinate matching" that is " as many matches as possible" for the given query.

Key Words: Cloud Computing, Privacy preserving, Keyword Search, Searchable encryption, Access Control.

I. INTRODUCTION

In clouds, Access control is the one of the most important concept which gains more attention from user of the clouds. This is why because of only the authorized individuals can access valid services. Usually a bulk or huge amount of data or information stores in clouds. All most all the data stored in the clouds is sensitive data only. As it is sensitive data, we need to provide valid access to access the information stored in the clouds. Mostly the information stored in clouds is totally related to the health domain that can be a important documents or the personal information in the social networking. So in this paper we mainly concentrated on Access control and Privacy Preserving.. Access controls are of 3 types. User Based Access Control, Role Based Access Control and Attribute based Access control.

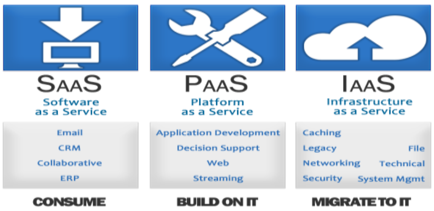


Fig 1. Cloud services

Let us see few examples to put an end to your confusion. Google Drive is the best example for pure cloud computing service. You can work with cloud apps like Google Docs, Google Sheets, and Google Slides; because of all most all the storage is found online. Drive is available on more than just desktop computers. You can also find separate apps for Google Sheets and Google Slides as well. All the Google services like Gmail, Google calendar and Google Maps cloud are considered as Cloud Computing. Apple's cloud service is the primary resources that can be used for online storage, contacts, calendar, backup and synchronization of your mails. ICloud is the place where iphone users go to utilize the find my Iphone features that's all important when the phone goes missing.

Usually users of the cloud outsource their data to remote servers. Privacy and Security is the two things to be taken into consideration. We can also make sure that cloud does not tamper with the data that is outsourced. User privacy is also important in clouds, so the validity of the users who stores the data is also verified. Searching concept is most important concept in this system. For the given query, the cloud must return the matched records. The correct matched records are returned by the clouds. "Coordinate matching" to capture the relevance of files to the query. They use "inner product similarity" to measure the score of each file. This solution supports exact multi-keyword ranked search. It is practical, and the search is flexible. Sun et al., proposed a MDB-tree based scheme which supports ranked multi-keyword search. This scheme is very efficient, but the higher efficiency will lead to lower precision of the search results in this scheme.

Existing System

Most of the data is outsourcing to remote servers. Maintaining all these in clouds is crucial issue. If larger the number of cloud users and documents search results and inefficient with existing system.. So search with multi keyword is very crucial in-addition to retrieve ranked data. In the existing it mainly focused on single key or Boolean key searches only, so it does not differentiate the search results. To improve the accuracy of the search results and also to extend user searching experience ranking system with multiple keyword search is necessary.

Disadvantages of Existing System:

- Single Keyword search Without Ranking
- Boolean Keyword search Without Ranking.
- Single Keyword search with Ranking.

Proposed System

In implemented system, we overcome all the problems identified in the existing system, i.e., single keyword is replaced multiple keywords, Provides privacy and security to the data stores in clouds, generates ranking results. We can find various algorithms for multi-keyword search. Among these semantic we choose an efficient principle of "coordinate matching". Specifically, we use 'inner product similarity", that is the number of query keywords appearing in a document, to quantitatively evaluate such a similarity measure of that document to the search query. During the index construction, each document is associated with a binary vector as a sub index where each bit represents whether corresponding keyword is contained in the documents.

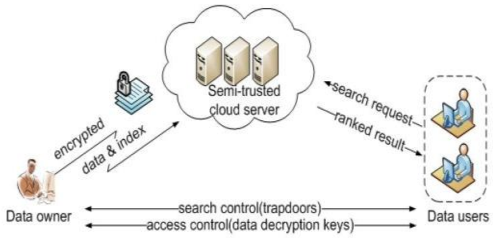

Semi-trusted cloud server
encrypted data & index
search request
ranked result
Data owner
search control(trapdoors)
access control(data decryption keys)
Data users

Fig 2: Proposed System Model.

We implemented a new design that supports both dynamic operation on documents and multi keyword ranked search. The proposed system model is as follows. In information retrieval latent semantic analysis is a solution. It adopts singular value decomposition.

In the Architecture of the newly implemented system, the owner of the file will outsource their data to remote server. The outsourced file must be encrypted before it stored in clouds and also attaches index to each file to be outsourcing.

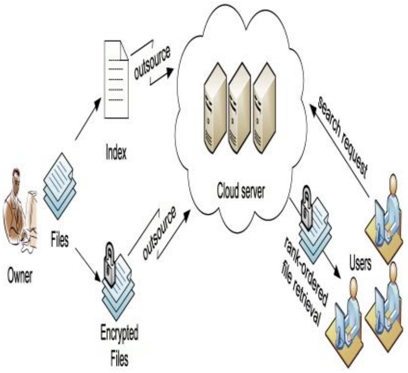


Fig 3: Architecture of Ranked Search over Encrypted Cloud Data

The user, who wants to access the data stored in clouds must provide a valid keyword to get matched results. Once search key is given to the cloud server, the server will resulted out the matched information and also it decrypts the files before outsourcing which is encrypted while storing in clouds. The results also in ranking order file retrievals.

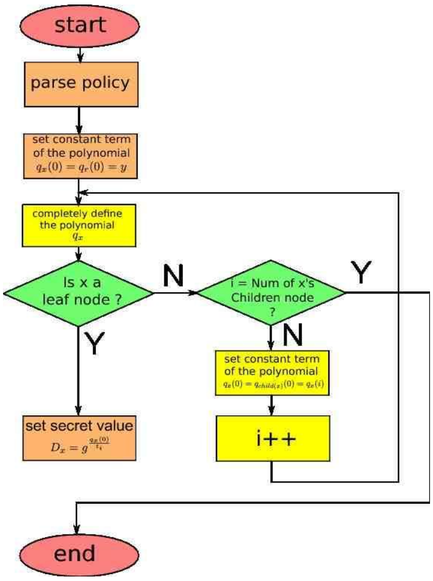

start
parse policy
set constant term of the polynomial $q_x(0) = q_r(0) = y$
completely define the polynomial q_x
Is x a leaf node ?
N
i = Num of x's Children node ?
Y
Y
N
set constant term of the polynomial $q_x(0) = q_{child(x)}(0) = q_x(i)$
set secret value $D_x = g^{\frac{q_x(0)}{t_i}}$
i++
end

Fig 4:Algorithm For ciphertext-policy attribute-based encryption.

Advantages of Proposed System

- Multi-Keyword Ranked search over encrypted cloud data.
- Coordinate Matching" by inner product similarity.
- Multi Keyword Ranking for Secure the cloud data.

II. RESULT AND ANALYSIS

Algorithm(1):For index table generation:

```
Srep1. Read the document F
Step2. Segment the document term wise and encrypt with key
Step3. Calculate term frequency (TF) and inverse document frequency(IDF) and publishing time(PT)
Step4. Generate index table(Itable) and files upload to server.
```

Algorithm(2): Ranked Search

```
For all documents Ri do
    Compare(level1 index of Ri , query index)
    j = 1
    while match do
        increment j
        Compare (levelj indices of Ri, query index)
    end while
    rank of Ri = highest level that match with query index
en
```

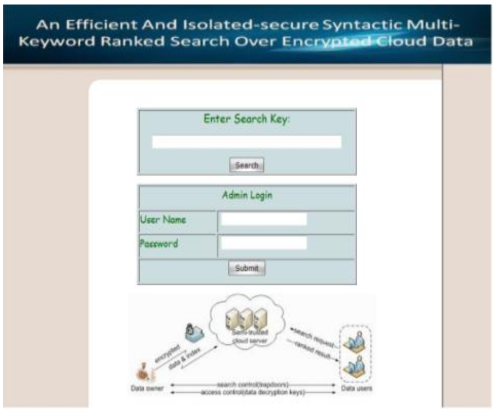
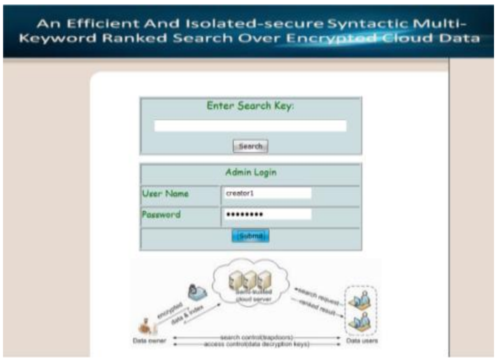

An Efficient And Isolated-secure Syntactic Multi-Keyword Ranked Search Over Encrypted Cloud Data

Fig: Main Page

.


An Efficient And Isolated-secure Syntactic Multi-Keyword Ranked Search Over Encrypted Cloud Data

User Name: creator1
Password: ••••••••

Fig: Login page.

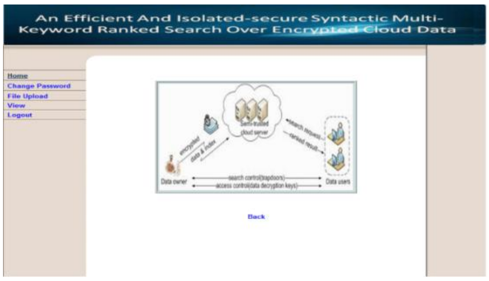
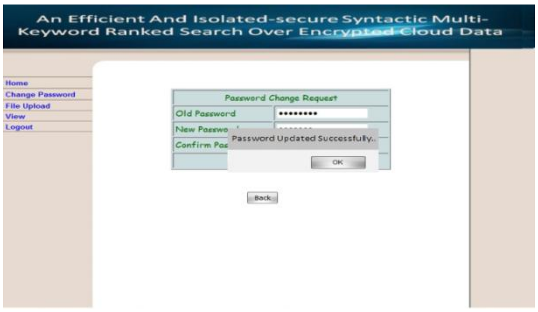

An Efficient And Isolated-secure Syntactic Multi-Keyword Ranked Search Over Encrypted Cloud Data

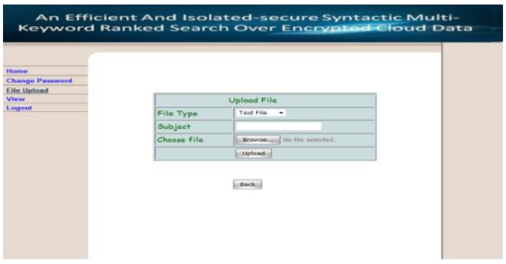
Fig: After login.


An Efficient And Isolated-secure Syntactic Multi-Keyword Ranked Search Over Encrypted Cloud Data

Password Change Request
Old Password: •••••••••
New Passwo
Confirm Pas

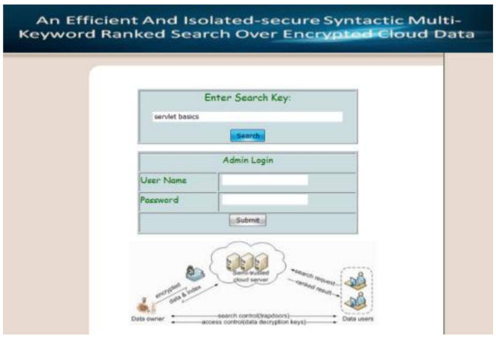
Password Updated Successfully..

Fig: Password Updated Successfully.


An Efficient And Isolated-secure Syntactic Multi-Keyword Ranked Search Over Encrypted Cloud Data

Upload File
File Type: Text File
Subject:
Choose file: No file selected.

Fig: File Upload.


An Efficient And Isolated-secure Syntactic Multi-Keyword Ranked Search Over Encrypted Cloud Data

Enter Search Key: servlet basics

Fig: Searching File With Key.

III. CONCLUSION

We discover solutions to the problems identified in existing system. We defined and solved the multi keyword search over encrypted data in clouds. We choose an efficient principle of "coordinate matching" as many matches as possible. In addition, it further reduces the time cost.

FUTURE SCOPE

Following the current research, we propose several possible directions for future work on ranked keyword search over encrypted data. The most promising one is the support for multiple keywords. In this case, for the security requirement of searchable encryption, constructions for conjunctive keyword search in the existing literature might be good candidates for our proposed ranked search. However, as the IDF factor now has to be included for score calculation, new approaches still need to be designed to completely preserve the order when summing up scores for all the provided keywords. Another interesting direction is to integrate advanced crypto techniques, such as attribute-based encryption to enable finegrained access control in our multi-user settings.

ACKNOWLEDGEMENT

Mr.Kasula Rama Gopi would like to thank Sri. Vemula Rajiv Jetson, Assoc.Professor and B. Satyanarayana Reddy Assoc. Professor, HOD, Dept of CSE, who had been guiding throughout the project and supporting me. Also in giving technical ideas about the paper and motivating me to complete the work efficiently and successfully.

REFERENCES

[1] K. Ren C. Wang, Q. Wang et al., “Security challenges for the public clouds” 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] D. Boneh, “ Public key encryption with keyword search”, Advances in ryptology-Encryption 2004, Springer,(2004).

[4] R. Curtmola, “ Searchable symmetric encryption: improved definitions and efficient constructions”, Proceedings of the 13the ACM conference on Computer and Communications security, ACM, (2006).

[5] C. wang, “Secure ranked keyword search over encrypted cloud data”, Distributed Computing Systems and Privacy”, 2000. S&P 2000, Proceedings 2000 IEEE Symposium, IEEE, (2000).

[6] D. S. 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.

[7] E.J. Goh et al., “ Secure indexes.” IACR Cryptology ePrint Archive, vol.2003, p.216, 2003.

[8] 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 Newtork Security. Springer-Verlag, 2005, pp.442-455.

[9] J.Li, Q. Wang, C.Wang, N. Cao, K. Ren and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing” in INFOCOM, 2000 Proceedings IEEE, IEEE 2010, pp.1-5

[10] I. H. Witten, A. Moffat, and T. C. Bell, “Managing gigabytes: Compressing and indexing documents and images”, Morgan Kaufmann Publishing, Sam Francisco, May 1999.

[11] M Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Pailer, and H. Shi, “ Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions” J. Cryptol., vol. 21, no. 3, pp.350-391, 2008

[12] L. Ballard, S. Kamara and F. Monrose, “Achieving efficient conjunctive keyword searches over encrypted data” in Proc.of ICICS, 2005.

[13] R. Brinkman, “ Searching in encrypted data” in University of Twente, PhD thesis, 2007.

[14] J. Katz, A. Sahai, and B/ Waters “Predicate encryption supporting disjunctions, polynomial equations, and inner products” in Proc.of EUROCRYPT, 2008.