International Journal of Multidisciplinary Research and Development

Volume :2, Issue :4, 427-430
April 2015
www.allsubjectjournal.com
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

Prashant Salunkhe
Computer Engineering,
P.R.E.C Loni Ahmednagar,
Maharashtra, India

Pratik Walkhade
Computer Engineering,
P.R.E.C Loni Ahmednagar,
Maharashtra, India

Gaurav Sawant
Computer Engineering,
P.R.E.C Loni Ahmednagar,
Maharashtra, India

Correspondence:
Prashant Salunkhe
Computer Engineering,
P.R.E.C Loni Ahmednagar,
Maharashtra, India

Fault tolerance management for document searching on cloud

Prashant Salunkhe, Pratik Walkhade, Gaurav Sawant

Abstract
Cloud Computing is receiving a great deal of attention, both in publications & among users, from individuals at home to the government. Data can be outsourced from local sites to public cloud by data owners. Although cloud computing having benefits, there are privacy & security concerns too. For this, sensitive data have to be encrypted before outsourcing, which will be beneficial to the data owners & data. Users can securely search over encrypted data through keywords, but these techniques support only Boolean search and even there is no such guarantee that we can get relevant data. Taking into account that a large number of data users, data owners in cloud it is necessary that search system will allow multi-keyword search and provide the result similarity ranking to get the effective data that we need. In this paper, we propose the problem of fault tolerance management for document searching cloud. In document search, it will return the result by matching files in ranked order regarding to certain relevance criteria, and in Fault tolerance we will provide high security to data. We first propose a document searching and then we will improve it, to meet different privacy concerns. Also, we propose our system will have fault tolerance management that will improve the security of the system. Fault tolerance will manage the things related to security concerns.

Keywords: Secure Cloud computing, encryption, search, falut tolerance

1. Introduction
Cloud computing is the method of availing computing resources from a provider, on demand, by a user using a computer connected to internet [1]. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, web mail, and online business applications.

Cloud computing reduces the cost as there is no need to purchase infrastructure thus low maintenance and the billing model is pay as per usage. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

As cloud computing service is popular, more and more sensitive information are being centralized into the cloud servers, such as private photos and videos, emails, financial reports of individual or company, government documents, etc.

To protect data and its privacy, confidential data has to be encrypted before outsourcing, so as to prove high data confidentiality in the cloud.

Data encryption makes effective data utilization. But it is very challenging task when there is a large amount of outsourced data files. Besides, in cloud computing, large number of users can access the data outsourced by data owners. Users might want to only retrieve certain specific data files they are interested in during a given session. For this purpose, we can use keyword-based search. Such keyword-based technique allows users to selectively retrieve files of interests and has been widely applied in plain text search scenarios. Unfortunately, these traditional plaintext search methods fails for encrypted cloud data as it restricts user ability to perform keyword search and further demands the protection of keyword privacy. The Fault tolerance in this system will give more security to the data owners. In fault tolerance we are going to give the notification to user through email and SMS when there will be unauthorized access to their files made.

2. Related Work
Now days there are so many organizations, companies are using the clouds to protect the data. This new technology helps in many ways, but it also has limits of protecting data

against attack. For better result the Ranked result is introduced. It can show search result in a Ranked manner by using some relevance. This technique is very sensitive, and we can also implement in an encrypted data searching.

The directly outsourcing of data will leak a lots of sensitive frequency information against the keyword privacy.

We propose an encryption with ranking result of queried data which will only give the expected data. The purpose of our system is to protect the sensitive data information.

A. Existing system

Existing searchable encryption schemes allow a user to securely search over encrypted data through keywords without first decrypting it, these techniques support only conventional Boolean keyword search, without capturing any relevance of the files in the search result. It can have the following drawbacks when these techniques are applied to large data outsourcing cloud environment.

Disadvantages of existing system:

1. Boolean-keyword search without ranking.
2. Single-keyword search without ranking.
3. Single-keyword search with ranking.
4. No guarantee of getting the relevant data.
5. No Fault Tolerance Management.

3. Problem Formulation

A. Proposed System

Now a days there are so many organization, company are used the clouds to protect the data. This new technology help in many ways but it also has limits of protecting data against attack. For better result the Ranked result is introduced. It can show search result in Ranked manner by using some relevance (e.g. keyword frequency). This technique is very sensitive. And we can also implement in encrypted data searching. The main aim of our project is to provide security. So we are also adding the facility of fault tolerance system.

Fault tolerance management:

If in any case any malicious activities are happened during the sharing of data then, it is very important issue to detect the attack or malicious activity. For this purpose we are introducing Fault tolerance system. In which attack is detected and the acknowledgement of such attack is inform to authorized person.

Detecting and informing about attack:

If any unauthorized person is trying is steal or accessing data which is store in cloud. Then our design software will send a message of attack by e-mail and text Message to authorized account. Also it will send message when any change is done by unauthorized user.

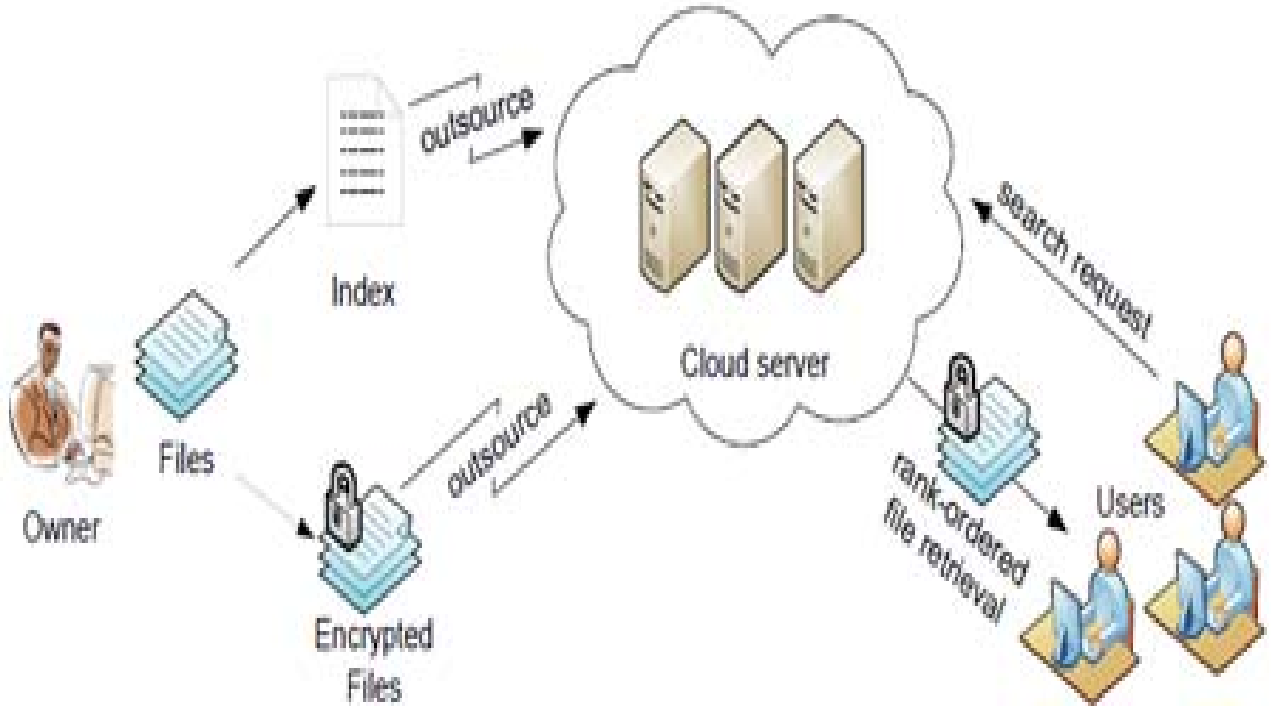

Fig 1: Architecture of fault tolerance managaement for document searching cloud

B. Design Modules

1. Encryption Module

This module used to help the server the documents. The encryption is done using RSA algorithm. The encrypted document is converted into the Zip file with the activation code and then activation code send to user for download.

2. Multi-Keyword Module

This module is used to generate the accurate results based on the multiple keywords. The user can give multiple keywords in the query, and then server splits that query into a single word after search that word file in database. Finally, it displays the matched word from list of database and the user gets the file from that list.

3. File upload Module

This module can be used to upload the files securely to the server. Admin uses the log key while login.

The file can be uploaded after the conversion of Zip file format. Admin can see the log file for more details about each & every file.

4. Fault Tolerance Module

This model will be helpful for increasing the security of the system. This module will help when any unauthorized person

make any changes in your file. It will send the notifications through SMS and email when it seems like someone have changed the file.

C. Cloud Service

For this system we are using Salesforce cloud service provider. Salesforce cloud provides high security. The performance of this cloud is better than other cloud service providers.

Fig 2: Salesforce Cloud Applications

Salesforce is easy to use and it provides various services of cloud. As Salesfoce platform is very secure, it will be beneficial for our system that why we used the Salesforce.

4. Algorithms

A.RSA Algorithm

The RSA algorithm,named after Ron Rivest, Adi Shamir, and Leonard Adleman is based on a property of positive integers. This algorithm consists of: key generation, encryption and decryption.

Key generation

The RSA algorithm involves the use of two keys: **public key** and **private key.** A public key, which may be known by anybody, and can be used to encrypt messages. A private key, known only by the recipient, and used to decrypt messages. The keys for RSA algorithm can be generated the following way:

1. Choose 2 distinct random prime numbers : p;q
2. Compute n = p:q
3. Compute f(n) = (p□1)(q□1) (Euler's totient function)
4. Choose an integer e, such that
1 < e < f(n) and gcd(e;f(n)) = 1
5. Compute d _ e□1 mod [f(n)]
6. Publish the public encryption key : (e;n)
7. Keep secret private decryption key : (d;n)

Encryption

To encrypt a message the sender has to:

1. Obtain public key of recipient (e;n)
2. Represent the message as an integer m in [0;n-1]
3. Compute: $c = m^e \bmod n$

Decryption

To decrypt the ciphertext c the recipient:

1. Uses his private key (d;n)
2. Computes: $m = c^d \bmod n$

B. K-Nearest Neighbour Algorithm

K-nearest neighbour search identifies the top k nearest neighbours to the query.

Nearest Neighbour Search (q, k) // optimal algorithm

1. Initialize ranking = index.increm-ranking (F(q), df)
2. Initialize result = new sorted-list (key, object)
3. Initialize dmax = w
4. While o = ranking.getnext and d,(o, q) I d,,, do
5. If do@, s> s dmax then result.insert (d,(o, q) , o)
6. If result.length 2 k then dmax = result[k].key

3. Conclusion

In this paper, we proposed the problem fault tolerance management for document searching cloud. We first give a basic system with document searching. We then proposed a system with the fault tolerance management which will improve the security of our system. When any changes made in data that will be informed to the data owner by notifications via email and SMS.

References

1. Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, National Institute of Science & Technology USA, Special Publication 800-145, September 2011(Accessible on the World Wide Web).
2. Ning Caoy, Cong Wangz, Ming Liy, Kui Renz, and Wenjing Louy Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data
3. Cong Wang†, Ning Cao‡, Jin Li†, Kui Ren†, and Wenjing Lou‡ †Department of ECE, Illinois Institute of Technology, Chicago, IL 60616 ‡Department of ECE, Worcester Polytechnic Institute, Worcester, MA 01609 Secure Ranked Keyword Search over Encrypted Cloud Data .
4. S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010*, January 2010.
5. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of IEEE Symposium on Security and Privacy'00*, 2000.
6. Weifeng Su, Jiying Wang, and Frederick H. Lochovsky, Member, IEEE Computer Society Record Matching over Query Results from Multiple Web Databases.
7. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. of EUROCRYP'04, volume 3027 of LNCS*. Springer, 2004.
8. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, ―Searchable symmetric encryption: improved definitions and efficient constructions,‖ in Proc. of ACM CCS'06, 2006.
9. A. Singhal, Modern information retrieval: A brief overview, IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 3543, 2001.
10. 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 *Proc. of the Workshop on Storage Security and Survivability*, 2007.
11. Y. H. Hwang and P. J. Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System," in *Proc. Of Pairing'07*, 2007, pp. 31–45.
12. Y.Srikanth,M.Veeresh Babu, P.Narasimhulu Combined Keyword Search over Encrypted Cloud Data Providing Security and Confidentiality.
13. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. of IEEE INFOCOM'10 Mini-Conference*, San Diego, CA, USA, March 2010.
14. L. Kozma, k Nearest Neighbours Algorithm. Helsinki University of Technology, Available: http://www.lkozma.net/knn2.pdf, 2008.
15. H. Witten, A. Moffat, and T. C. Bell, Managing gigabytes: Compressing and indexing documents and images, Morgan Kaufmann Publishing, San Francisco, May 1999.