Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology - CCIT 2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-23

Encryption on Data in Cloud Environment

[Muhammad Sajid Khan, Prof Chengliang Wang]

Abstract— **In this research paper, an encryption technique has been developed which consists of indexing and searching. The scheme does not need to inculcate the decryption steps, the users no longer need to decrypt the data during search operation. The proposed method makes the search operation more efficient and fast. Besides, it guarantees the protection and security of data.**

Keywords*—datastorage, indexing, searchable encryption, *cloud computing

I. Introduction

Recently development aroused in cloud computing made the information companies to rapidly provide convenient services to users like Google who provide services like Gmail, Documents and Google Calendar [1] .With the advancement of cloud computing, hundreds of thousands of network users or enterprises like to register their personal or private information for the use of some services. While adapting cloud services, security issue is the biggest problem as all the secret information and sensitive data are fully controlled by cloud providers. To overcome the security issues CSA, ENISA and NIST provide Counseling and suggestion for cloud storage in order to keep privacy of confidential data. [2]. However, some data outsourcing services may be malicious, illegally monitoring or retrieving user stored private information. The file search service is often used in cloud storage. Therefore, providing a searchable encryption method for enterprises in outsourcing cloud storage is an important issue and up to an extent this problem has been focused in this letter.

II. Related Work

The clouds have different architecture based on the services they provide. Ateniese et al. were the first to design a provable data possession model. It is used for ensuring the presence of data on the server. Ming Li et al. [3] identified the challenges and problems against the flexible, efficient and privacy assured outsourced cloud services.

Muhammad Sajid Khan
College of Software Engineering, Chongqing University
China

Prof Chenglian Wang
College of Software Engineering Chongqing University
China

Ranked keyword search and search over structured data has been focused by the authors. On the basis of these existing techniques, a framework for privacy assured search in cloud has been given.

Swaminathan et al. [4] introduced a framework for confidentiality of ranked ordered large set of documents. The framework provides protection of searched keyword, whole set of documents and data center security. Treesa Maria Vincent Mrs. J.Sakunthala discussed various concepts for searchable encryption in cloud environment [5].

In the service provider's datacenter, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. For the cloud provider, the best means for securing data is cryptographic encryption and shipping self-encrypting.Self-encrypting provides automated encryption with performance or minimal cost impact.

III. Security of Sentence Search

The searching of sentence includes two security has been briefly describes in "searching encrypted data on cloud"[6]. The searched sentence keywords are first converted to trapdoors and then to codewords. These two levels of security fulfill the required need of security for cloud environments and data passed through these two security levels cannot be hacked or predicted by cloud. The searched sentence keywords are directed towards data owner where they are converted to codewords and sent to cloud server for fetch matching documents in ranked order i.e. the most relevant document on top.

IV. Indexing time of Encryption Technique

The time required to index a document is called indexing time and it is calculated by indexing the document. A set of 130 documents are taken for experimental evaluation but few documents are listed in the table below to make the concise and understandable graph as 150 files index time if plotted on graph makes it hard to understand. The time required to index number of distinct words in each document has been shown in Table 1.1.

Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology - CCIT 2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-23

Document name	No. Of index word	Indexing Time (Sec)
How to search eu gin goh.txt	180	10
Cloud_computing_security_risk.txt	421	22
Optimizing security of cloud computing within the dod.txt	698	32
Deploying public key infrastructure as a cloud service.txt	1169	63
Service-oriented modeling and architecture.txt	1877	96
A wrapping approach and tool for migrating legacy components.txt	2105	111
Risk management in global software development process planning.txt	2375	120
Project management a case study.txt	2556	131
Data protection-aware design for cloud services.txt	2873	148

Table 1.1 No of indexing words and Index Time

The statistical results obtained in Table 1.1 have been graphically depicted in Figure 1

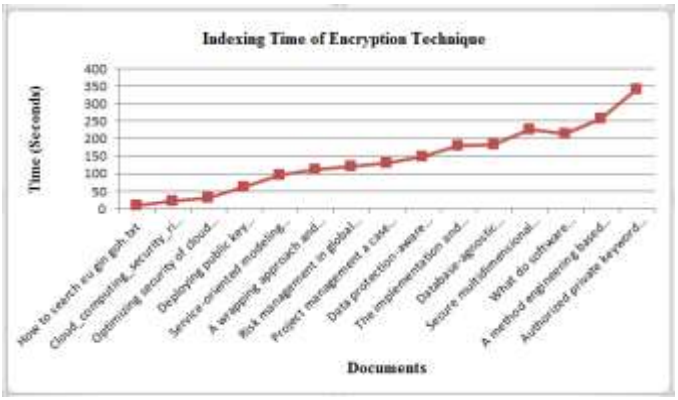

Fig.1 Representation of Index Time

Figure.1 shows that with the number of indexed words shown horizontally increase in the documents, the indexing time shown vertically also increases. Hence it can be said that:

Indexing a document α No. of index words

A. *Index time for one keyword*

From the results in Table 1.1, the indexing time for one keyword is calculated as:

Total keywords = 42354

Total time consumed = 2136

One keyword index time = Total time / Total words = 2136/42354 = .0504 seconds

B. *Words indexed in one second*

The total number of keywords indexed per second can be calculated as follows:

Total keywords= 42354

Total time consumed = 2136

Keywords indexed in one sec = Total keywords / Total time consumed = 42354/2136 = 19.82 words

These results can be used for time estimation of time for indexing of specific number of keywords. The increase in the number of index words increase the indexing time. The reason proposed technique takes more time to index documents is that each individual word has to be indexed with its position in the document instead in ranked search where only distinct words are indexed with their ranks. The similar words only increment the rank.

v. Search Time of Encryption Technique

When a sentence is searched, its keyword's codewords are matched in the document indexes. After the matching of keyword's codewords, the collection of data is arranged and the combinations of the sentence are found.

Searched Sentences	Search Time (Sec)
Cloud Computing sees a technical and cultural shift of computing service	2.792
The problems and risks of poor architectural practices are well known	2.005
Cloud computing is fraught with security risks, according to analyst firm Gartner	2.468
The Terminal Emulator manages the communications	1.505
Business Information Integration from XML and Relational Databases Sources	2.059
Deploying Public Key Infrastructure as a Cloud Service	2.023
2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science	2.617
IDENTIFIED SECURITY ATTRIBUTES IN CLOUD COMPUTING	1.593

Table1.2 No of Search Sentence and Search Time

The statistical results obtained in Table 1.2 have been graphically shown in Figure 2. It depicts that the vertical axis show the time required for searching specific keywords and on horizontal axis searched keywords have been shown. It has been observed that the search time remains in the range of 1.5 seconds to 3.5 seconds.

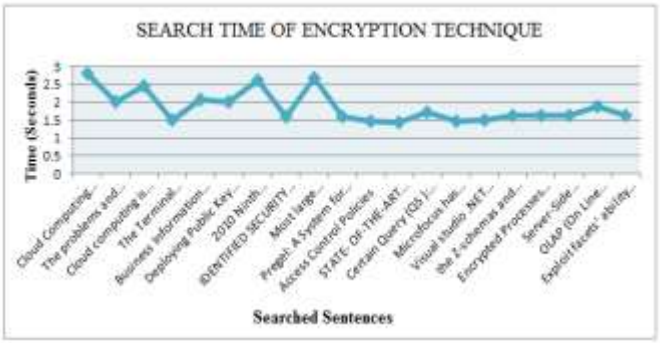

Fig.2 Representation of Search Time

Proc. of the Intl. Conf. on Advances In Computing, Communication and Information Technology - CCIT 2014.

ISBN: 978-1-63248-010-1 doi: 10.15224/ 978-1-63248-010-1-23

VI. Conclusion and Futher Discussion

This paper focuses on time calculation of indexing and searching in order to improve the efficiency of searchable encryption. The experimental results show that the proposed encryption technique is provably fast and efficient. It further provides security and privacy of data search. It can also be extended by using case insensitivity and encrypted data bases.
The encryption technique is proposed for cloud environment where a large amount of unstructured data is stored in encrypted form. This can be used on individual server within an organization for data security. This technique is an easily deployed working technique which can be customized according to the users need. It can be implemented in banking systems, defense systems and other areas where security achievement with efficient and accurate search on encrypted unstructured data is major concern.

Acknowledgment

Author is grateful to Prof Chenliang wang whose guidance and assistance made it possible for me to accomplish this task. He has been a source of encouragement and inspiration to me throughout this task completion. His guidance, assistance and unsurpassed knowledge provided me necessary support for carrying out this research.
.

References

[1] Anu Rathi, Yogesh Kumar Anish Talwar, "Aspects of Security in cloud computing." International Journal Of Engineering And Computer Science, Volume 2 Issue 4 April, 2013 Page No. 1361-1363 .

[2] D. Shivalingaiah "Applications of Cloud computing for resource sharing in academic libraries". Proceedings of 20121ntemational Conference on Cloud Computing, Technologies, Applications & Management

[3] A. Tripathi and A. Mishra, "Cloud Computing Security Considerations." 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 14-16 Sept., Xi'an-Chaina, pp 1-5.

[4] Swaminathan, Ashwin, Yinian Mao, Guan-Ming Su, Hongmei Gou, Avinash L. Varna, Shan He, Min Wu, and Douglas W. Oard, "Confidentiality-preserving rank-ordered search." In Proceedings of the 2007 ACM workshop on Storage security and survivability, pp. 7-12. ACM, 2007.

[5] Vincent, Treesa Maria, and Mrs J. Sakunthala, "Encrypted Data Storage in Cloud Environment." Internationl Journal of Advanced Research in Computer Science and Software Engineering Vol. 3, Issue 3, March(2013), pp 498-506.

[6] M.sajid.khan "searching encrypted data on cloud" published iInternational journal of computer science issue.

Muhammad Sajid Khan was born in Pakistan. He was awarded bachelor degree in Computer Engineering by Comsats Institute of Information Technology Pakistan in 2011.He worked in I-intellect International (Pvt.) Ltd Pakistan as web designer He worked on Wireless on/off controlling of 30 HP Tube well as a final year project in bachelous. Mr. Khan participated in EMCOT Science Exhibition by presenting his project in it and also awarded Chinese Govt Scholarship. Later on he go to Chongqing university for higher education in software engineering in 2012. His semester project accepted for presentation in 5th world Engineering Congress 2013 Islamabad Pakistan. He publish "Searching Encrypted data on cloud " in International Journal of Computer Science Issues.