IJRRECS/October 2013/Volume-1/Issue-6/1453-1458 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

FACILITATING OF PROFICIENT KEYWORD SEARCH IN CLOUD COMPUTING

K.Shashidhar[1], B.Madhavi Devi[2], Ch.Srinivasulu[3]

[1]Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

[2]Assistant Professor, Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

[3]Associate Professor, Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

ABSTRACT:

Cloud computing construct on established trends for motivating the cost out of the delivery of services while growing the speed and agility with which services are deployed. The advantages of cloud computing include on-demand self-service, ubiquitous network admission, location autonomous resource pooling, fast resource elasticity, usage-based charge, transmission of risk. Along with the extensive enthusiasm on cloud computing, though, concerns on data security with cloud storage are arising due to unpredictability of the service and malicious attacks from hackers. Protecting private and significant information from malicious insiders is of crucial consequence. Recently more and more proceedings on cloud service outage or server fraud with major cloud infrastructure providers are reported. Well-organized methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. The user is allowed to search over the encrypted information securely by means of conventional methods of encryption devoid of initially decrypting it, these techniques only supports the search of Boolean keyword devoid of capturing the significance of the files in the result of the search. To facilitate a searchable encryption system by means of secure ranked search was proposed. The process used by the ranked search improves the system greatly by means of recovering the files which are matching in the order of ranked in order to assure

significance criteria hence makes the realistic deployment of the data services of secure preserving in the perspective of cloud computing.

Keywords: Cloud computing, Boolean keyword, Data integrity, Ranked search, Encryption system.

1. INTRODUCTION:

A cloud provider put forward numerous services that can possibly profit its customers, such as quick access to their data, scalability, pay-for-use, data storage, data recovery and defend against various hackers, on-demand protection controls, and usage of the network and infrastructure conveniences [4]. Cloud service providers should make sure the protection of their customers' data and should be accountable if any security risk affects their customers' service infrastructure. Along with the extensive eagerness on cloud computing, on the other hand, anxiety on data security with cloud storage are arising due to unpredictability of the service and malicious attacks from hackers [9]. Reliability and ease of use are other proceeds of the public cloud, in adding up to low outlay. By taking a variety of kinds of data in the data safety, the difficulty of checking correctness of data is still became a challenging one [11]. The advantages of cloud computing include on-demand self-service, ubiquitous network admission, location autonomous resource pooling, fast resource elasticity, usage-based charge, transmission of risk. Cloud computing users want to keep away from an entrusted cloud provider as data will be managed with a third party [1] [14]. Protecting private data from malicious insiders is of critical consequence. Well-organized methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. The owners of the data might possibly share their information with huge numbers of the users by means of the well known technique of keyword search in which the users can possibly recover particular data files for which they are interested in and thus method is widely used in plain text search technique [3] [6]. The user is allowed to search over the encrypted information securely by means of conventional methods of encryption devoid of initially decrypting it, these techniques

only supports the search of Boolean keyword devoid of capturing the significance of the files in the result of the search [10]. To facilitate a searchable encryption system by means of secure ranked search was proposed. The process used by the ranked search improves the system greatly by means of recovering the files which are matching in the order of ranked in order to assure significance criteria hence makes the realistic deployment of the data services of secure preserving in the perspective of cloud computing [2] [5].

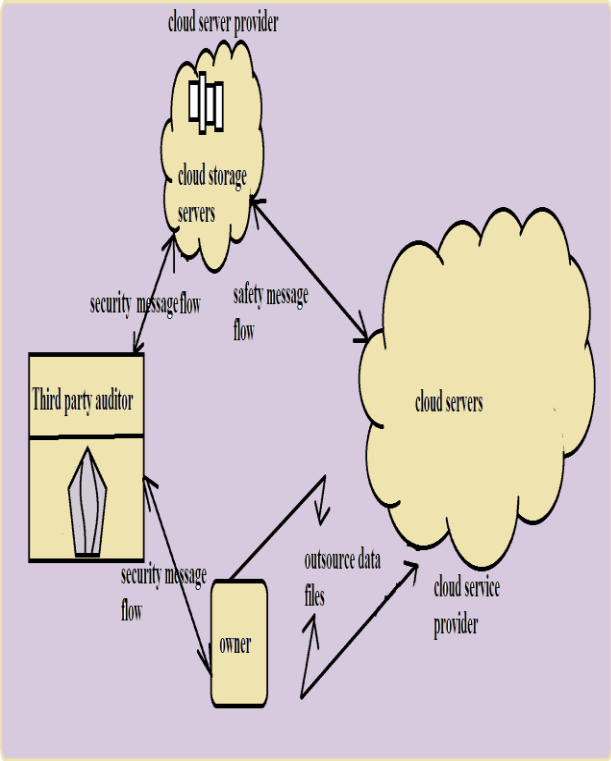

Fig1: An overview of encrypted cloud data

2. METHODOLOGY:

The system of encrypted cloud service shown in fig1 comprises the data owner, user and the cloud server. The owner of the data has an assemblage of the data files that are to be outsourced on the cloud server in the form of encrypted on the other hand maintains the capacity to search by means of them for the reasons of effectual exploitation of the data [13]. The data owner initially constructs a protected searchable index from the set of various keywords which are taken out from the collection of the files before the outsourcing and the index and the collection of encrypted files are stored on the cloud server [8] [15]. In order to search for a given keyword in the file collection, the search request was generated and submitted by the confirmed user in a secret form to the cloud server and the cloud server searches the index and returns the particular set of files to the user upon receiving the request of search. The scheme of ranked searchable encryption consists of setup and retrieval phases [12]. The owner of the data initializes the system constraints of public and secret by means of running KeyGen, and by using Build Index pre processes the file of data collection and produce the searchable index from the exclusive words taken out from the

data collection. Subsequently the owner of the data encrypts the file of the data collection and publishes the index together with the significance of the keyword frequency based scores along with the collection of encrypted data to the cloud. The TrapdoorGen was used by the user to produce a confidential trapdoor that corresponds to the concerned keyword and provides to the cloud server and it will possibly develop file IDs which are matching and the scores of their corresponding significance [7]. The files of the matching IDs are sent back based on the sequence of ranked on the significance scores.

3. RESULTS:

While comparing the techniques of Searchable Symmetric Encryption to the ranked Keyword Search sets in the scores of the encrypted relevance in the searchable index as well as to the ID of the file. As a consequence the only added data are the encrypted scores which are made used by the adversary against to the assurance of security is the keyword and the security and the confidentiality of the file. Hence mainly due to the strength of the security, in the method of file encryption the content of the file is well protected.

4. CONCLUSION:

The advantages of cloud computing include on-demand self-service, ubiquitous network admission, location autonomous resource pooling, fast resource elasticity, usage-based charge, transmission of risk. Along with the extensive enthusiasm on cloud computing, though, concerns on data security with cloud storage are arising due to unpredictability of the service and malicious attacks from hackers. Recently more and more proceedings on cloud service outage or server fraud with major cloud infrastructure providers are reported. Well-organized methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. By means of conventional methods of encryption, the user is allowed to search over the encrypted information securely devoid of initially decrypting it, these techniques only supports the search of Boolean keyword devoid of capturing the significance of the files in the result of the search. To facilitate a searchable encryption system by means of

secure ranked search was proposed and it improves the system greatly by means of recovering the files which are matching in the order of ranked in order to assure significance criteria hence makes the realistic deployment of the data services of secure preserving in the perspective of cloud computing. The scheme of ranked searchable encryption consists of setup and retrieval phases. Although comparing the techniques of Searchable Symmetric Encryption to the ranked Keyword Search sets in the scores of the encrypted relevance in the searchable index as well as to the ID of the file. Hence the only added data are the encrypted scores which are made used by the adversary against to the assurance of security are the keyword and the security and the confidentiality of the file.

REFERENCES:

[1] 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.

[2] 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.

[3] 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, 2010.

[4] E. Shi, J. Bethencourt, H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in Proc. of IEEE Symposium on Security and Privacy'07, 2007.

[5] 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.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Service Computing (TSC), to appear.

[7] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on Jan. 23rd, 2010 Online at http://csrc. nist.gov/groups/SNS/cloud-computing/index.html, 2010.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems

[9] I. H. Witten, A. Moffat, and T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images," Morgan Kaufmann Publishing, San Francisco, May 1999.

[10] 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.

[11] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCBEECS- 2009-28, Feb 2009.

[12] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proc. of Crypto'07, volume 4622 of LNCS. Springer, 2007.

[13] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org.

[14] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+r: Top-k retrieval from a confidential index," in Proc. of EDBT'09, 2009.
(TPDS), vol. 22, no. 5, pp. 847–859, May 2011.

[15] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Of ICICS'05, 2005.