IJRRECS/August 2015/Volume-3/Issue-8/4510-4514 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A SCALABLE APPROACH FOR ELIMINATION OF DATA LEAKAGE IN CLOUD SYSTEM

CH.Nagesh[1], Dr.Vaka Murali Mohan[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

[2]Professor & HOD, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

ABSTRACT:

Cloud computing is an important prototype for superior data service, that has turn out to be an essential possibility for data users to outsource information. Searchable methods of symmetric encryption permit recovery of encrypted data above cloud. In our work we focus on tackling of issues regarding of data privacy by means of searchable symmetric encryption. Novel searchable encryption system was introduced where novel technologies within cryptography community and information retrieval community are utilized, including homomorphic encryption as well as vector space model. We name system as a two round searchable encryption, since ranking is made at user side whereas scoring calculation is made at server side. The vector space representation make accessible enough search accuracy, and homomorphic encryption make easy user to involve in ranking process while mainstream of computing work is completed on server side by means of operations just on cipher-text hence information leak can be removed and data security is guaranteed.

Keywords: Cloud computing, Homomorphic encryption, Vector space, Searchable encryption, Cryptography, Cipher-text.

1. INTRODUCTION:

In cloud computing, owners of data share their outsourced data with several users, who want to recover only interested data files and one of accepted ways to perform so is all the way through keyword-based retrieval. For improving of feasibility and

save on expenditure in cloud paradigm, it is preferred to obtain retrieval result by most applicable files that match user concentration rather than all files [1]. It indicates that files have to be ranked in order of importance by means of users' interest and the files with uppermost relevance are forward back to users. Series of searchable methods of symmetric encryption were projected to facilitate search on cipher-text. Traditional searchable methods of symmetric encryption facilitate users to strongly get back cipher-text, but these methods support whether a keyword exists within a file or not, devoid of considering variation of relevance with queried keyword of these files within result. In our work we make a focus on tackling of issues regarding of data privacy by means of searchable symmetric encryption. We recommend a novel searchable encryption system, where novel technologies within cryptography community and information retrieval community are utilized, including homomorphic encryption as well as vector space model [2][3]. In proposed scheme, the data owner encrypts searchable index by homomorphic encryption. When cloud server receive query consisting of multi-keyword, it work out scores from encrypted index hat is stored on cloud, and returns encrypted scores of files towards data user. The data user decrypts scores and pick out top-k highest-scoring file identifiers to appeal to cloud server. The recovery takes a two-round communication among cloud server as well as data user. We hence name the system as a two round searchable encryption, where ranking is made at user side whereas scoring calculation is made at server side.

2. METHODOLOGY:

Concerns of sensitive information on cloud may potentially cause privacy problems. Encryption of data defends data security to some scope, however at the cost of compromised effectiveness. Searchable methods of symmetric encryption were projected to facilitate search on cipher-text and these allows recovery of encrypted data above cloud. When users outsource their confidential data onto cloud, providers of cloud service control and check data as well as communication among users and cloud at will. Prevention of cloud from linking in ranking as well as entrusting work to user is a normal means to keep away from information leakage. On the other hand, restricted computational power on user side

as well as high computational transparency prevents information security. In our work we make a focus on tackling of issues regarding of data privacy by means of searchable symmetric encryption. In our work, we initiate the concepts of similarity relevance as well as scheme robustness to put together privacy issue in searchable encryption method, and resolve the insecurity difficulty by means of proposing a two-round searchable encryption method. Novel technologies in cryptography as well as information retrieval community are utilized, that includes homomorphic encryption as well as vector space representation. The vector space representation helps to provide sufficient search accuracy [4]. Homomorphic encryption make easy users to involve in ranking process as majority of computing work is finished on server side by means of operations just on cipher-text. In the proposed method, the most of computing work is made on the cloud whereas user play a part in in ranking, which assurance top-k multi-keyword recovery over encrypted cloud information by means of high protection as well as realistic effectiveness. We make a consideration of a cloud computing scheme hosting data service in which three separate entities are involved such as Cloud server, Data owner as well as Data user. The cloud server hosts data storage of third-party and get back services [5]. While data might hold sensitive information, cloud servers cannot be completely entrusted in defending information hence for this reason; outsourced files have to be encrypted. Any kind of information leak that would have an effect on data privacy is viewed as undesirable.

3. AN OVERVIEW OF PROPOSED SYSTEM:

The cloud server in our work is imagined as honest-but-curious; a representation broadly used in searchable methods of symmetric encryption and considered by that cloud server will openly follow considered procedure however is curious to analyze hosted data as well as received queries to find out extra information. We put together privacy issue from feature of similarity relevance as well as scheme robustness. In our work we make a focus on tackling of issues regarding of data privacy by means of searchable symmetric encryption. We inspect that server-side ranking on basis of order-preserving encryption unavoidably

leak data privacy. To get rid of the leakage, we suggest a two-round searchable encryption scheme that support top-k multi-keyword recovery. In the proposed two-round searchable encryption scheme, we make use of a vector space model as well as homomorphic encryption. In proposed scheme, data owner encrypts searchable index by homomorphic encryption. When cloud server obtain query consisting of multi-keyword, it work out scores from encrypted index hat is stored on cloud, and returns encrypted scores of files towards data user. The vector space representation helps to make available enough search accuracy, and homomorphic encryption facilitate users to involve in ranking process while mainstream of computing work is completed on server side by means of operations just on cipher-text. Thus information leak can be removed and data security is guaranteed. Traditional methods of Searchable methods of symmetric encryption make use of server-side ranking on order-preserving encryption to get better the effectiveness of retrieval above encrypted cloud data. On the other hand, server-side ranking basis of order-preserving encryption unavoidably leak data privacy which is considered inflexible in security-oriented third-party cloud computing situation, to be precise security cannot be trade off for effectiveness. To attain data confidentiality, ranking has to be left to user side. Conventional schemes of user-side, however, fill heavy computational burden as well as high communication transparency on user side, because of interaction connecting server and user together with searchable index return as well as ranking score calculation [6]. Hence methods of user side ranking are challenged by means of practical usage. An additional server-siding method may be an improved explanation towards privacy issues.

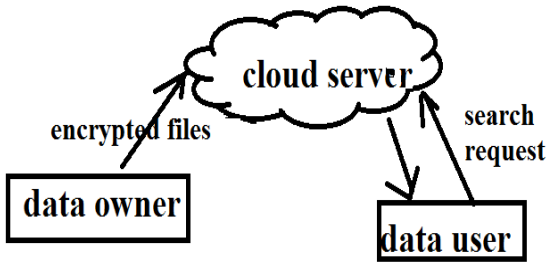

Fig1: an overview of recovery of encrypted cloud data

4. CONCLUSION:

For ensuring of privacy, users regularly encrypt data earlier than outsourcing it to cloud, which obtain enormous challenges to effectual data consumption. We propose a

novel searchable encryption system, where novel technologies within cryptography community and information retrieval community are utilized, including homomorphic encryption as well as vector space model. We name system as a two round searchable encryption, because ranking is made at user side whereas scoring calculation is made at server side. The vector space representation provide enough search accurateness, and homomorphic encryption facilitate users to involve in ranking process while mainstream of computing work is completed on server side by means of operations just on cipher-text as a consequence information leak can be removed and data security is assured. In proposed technique, most of computing work is made on cloud whereas user play a part in ranking, which assurance top-k multi-keyword recovery over encrypted cloud information by means of high protection as well as realistic efficiency.

REFERENCES

[1] AHN, "Romney hits Obama for security information leakage," http://gantdaily.com/2012/ 07/25/romney-hits-obama-for-security-information-leakage/, 2012

[2] Cloud Security Alliance, "Top threats to cloud computing," http://www.cloudsecurity alliance. org, 2010

[3] C. Leslie, "NSA has massive database of Americans' phone calls," http://usatoday30.usatoday.com/news/washington/2006-05-10/.

[4] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," in Gilbert, H. (ed.) EUROCRYPT. LNCS, vol. 6110, pp. 24-43, 2010.

[5] M. Perc, "Evolution of the most common English words and phrases over the centuries," the Journal of the Royal Society Interface, 2012. / mec/2003-2004/.

[6] O. Regev, "New lattice-based cryptographic constructions," JACM 51(6), pp. 899-942, 2004.