ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Multi-Ranked Keyword Search for Encrypted Data in Cloud

Megha GS[1], Dr Arun Biradar [2]

P.G. Student, Department of Computer Science & Engineering, East West Institute of Technology, Bangalore, Karnataka, India[1]

Head of Department, Computer Science & Engineering, East West Institute of Technology, Bangalore, Karnataka, India[2]

ABSTRACT: **A**s the popularity of cloud computing increases, more number of data owners are inspired to store their data to cloud servers as it as great convenience and reduce cost of data management. Anyhow, sensitive data should be encrypted before storing for privacy requirements, which uses data utilization like keyword-based retrieval of document. In this paper, we present a multi-keyword ranked search over encrypted cloud data using Private searching schema which was proposed by Ostrovsky et al(referred to as the Ostrovsky scheme in this paper), which allows a user to retrive files of interest from an untrusted server without leaking any information.

KEYWORDS*:* cloud computing, Multi-keyword ranked, data utilization

I. INTRODUCTION

Cloud Computing is a emerging technology which provides shared computer processing resources and data to computers and other devices on demand.Due to the merits of cloud computing, e.g., cost-effectiveness, flexibility,backup and recovery,Quick deployment and scalability, more and more organizations choose to outsource their data for sharing in the cloud. As a typical cloud application, an organization subscribes the cloud services and authorizes its staff to share files in the cloud. Each file is described by a set of keywords, and the staff, as authorized users, can retrieve files of their interests by querying the cloud with certain keywords. In such an environment, how to protect user privacy from the cloud, which is a third party outside the security boundary of the organization, becomes a key problem. User privacy can be classified into search privacy and access privacy . Search privacy means that the cloud knows nothing about what the user is searching for, and access privacy means that the cloud knows nothing about which files are returned to the user. When the files are stored in the clear forms, a naive solution to protect user privacy is for the user to request all of the files from the cloud; this way, the cloud cannot know which files the user is really interested in. While this does provide the necessary privacy, the communication cost is high.Private searching was proposed by Ostrovsky et al. (referred to as the Ostrovsky scheme in this paper), which allows a user to retrieve files of interest from an untrusted server without leaking any information. However, the Ostrovsky scheme has a high computational cost, since it requires the cloud to process the query (perform homomorphic encryption) on *every* file in a collection.

II. LITERATURE SURVEY

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. of ACM CCS*, 2016.

In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on

SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction

R. Ostrovsky and W. Skeith, "Private searching on streaming data," in *Proc. of CRYPTO*, 2015.

In this paper, we consider the problem of private searching on streaming data, where we can efficiently implement searching for documents that satisfy a secret criteria (such as presence or absence of a hidden combination of hidden keywords) under various cryptographic assumptions. Our results can be viewed in a variety of ways: as a generalization of the notion of Private Information Retrieval (to more general queries and to a streaming environment); as positive results on privacy-preserving datamining; and as a delegation of hidden program computation.

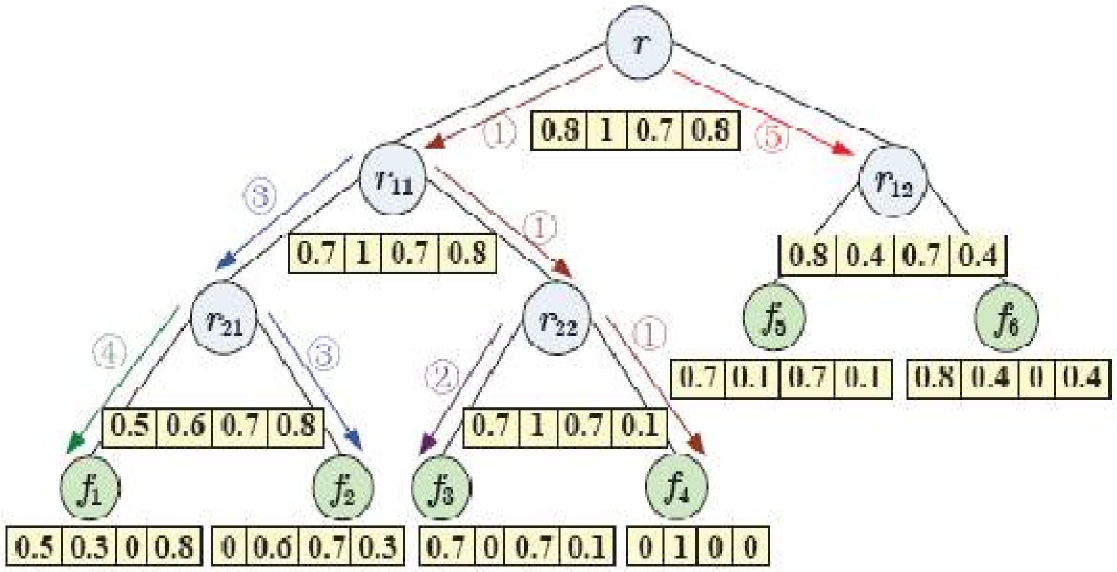
III. SYSTEM MODEL

User Module:

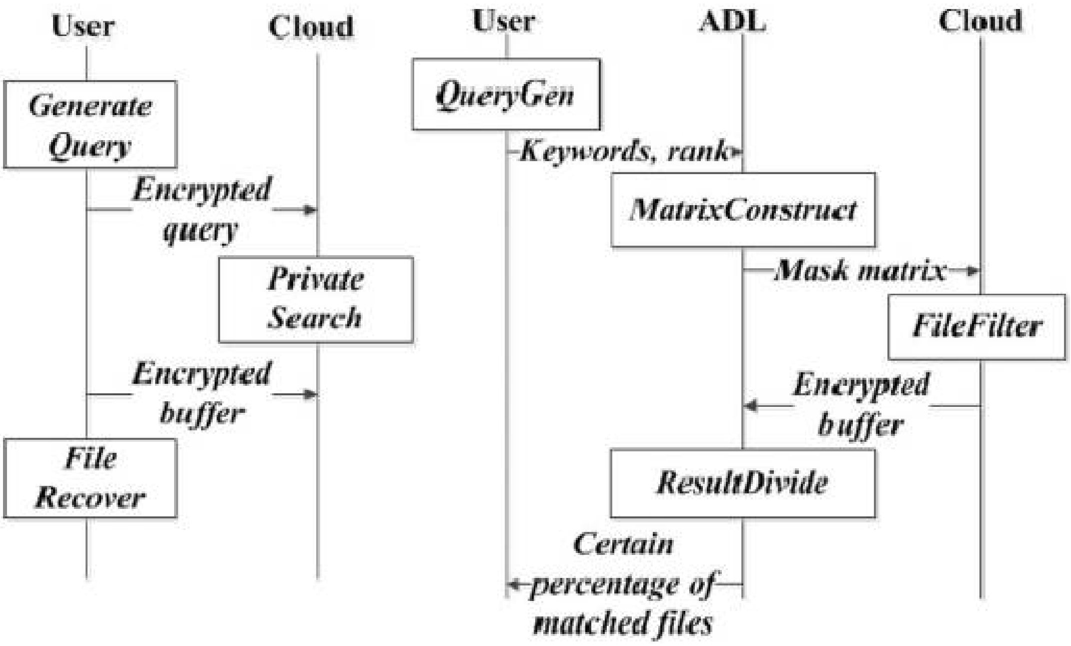
All the authenticated users will be having access to the cloud system. Every user should have an account or they should first register to get access to the system.

Multidimensional Index Tree

Most multidimensional indexing algorithms are derived from R-tree like algorithms , where the axis-aligned minimum bounding region (MBR) is the construction block for indexing the multidimensional data. For 2D data, an MBR is a rectangle. For higher dimensions, the shape of MBR is extended to hyper-cube. the MBRs in the R-tree for a 2D dataset, where each node is bounded by a node MBR. The R-tree range query An authorised user can login using Username and Password. Upon sending a file to cloud server, a secret key for the encrypted block of file will be generated and it will be shared to Admin. The sender himself has to provide the secret key in order to download that block of file.

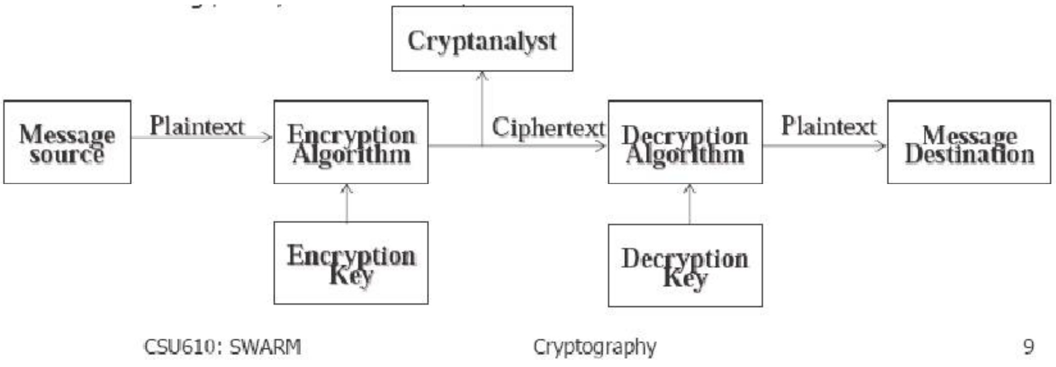


C Usecase diagram



IV. EXISTING SYSTEM

The existing techniques on keyword-based information retrieval, which are widely used on the plaintext data, cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is obviously impractical. All these multi keyword search schemes retrieve search results based on the existence of keywords, which cannot provide acceptable result ranking functionality. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval



DISADVANTAGES:
The main problem of existing system is it is restricted for single user authentication.

V. PROPOSED SYSTEM

The proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.Abundant works have been proposed under different threat models to achieve various search functionality,Recently, some dynamic schemes have been proposed to support inserting and deleting operations on document

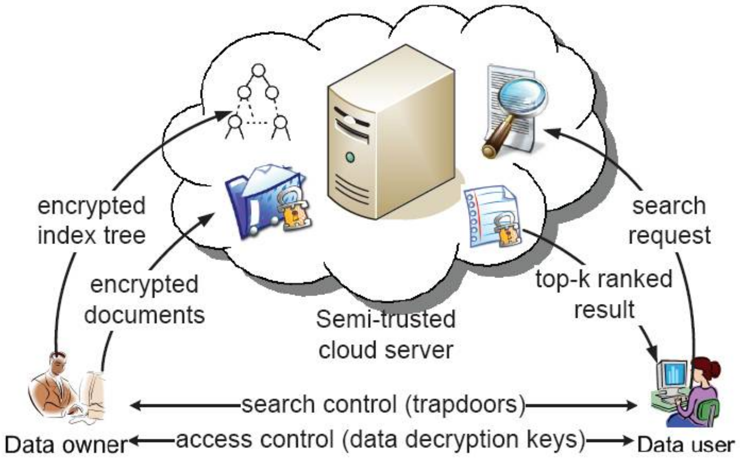


Fig. 1. The architecture of ranked search over encrypted cloud data

ADVANTAGES:
Despite of the various advantages of cloud services, outsourcing sensitive information such as e-mails, personal health records, company finance data, government documents, etc.

VI. CONCLUSION

The Distributed approache at Multi-Keyword Ranked Search over Encrypted Data provide an Efficient Search result over Encrypted Data for multiple users.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan-Feb.2012.
[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proc.Financ. Cryptography Data Secur., 2010, pp. 136–149.
[3] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation,Stanford Univ., Stanford, CA, USA, 2009.
[4] O. Goldreich and R. Ostrovsky, “Software protection and simulation on oblivious rams,” J. ACM, vol. 43, no. 3, pp. 431–473, 1996.
[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Adv. Cryptol.-Eurocrypt,2004, pp. 506–522.
[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, “Public key encryption that allows pir queries,” in Proc. Adv. Cryptol., 2007, pp. 50–67.
[7] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Secur. Privacy,2000, pp. 44–55.