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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

A Review on Searching Encrypted Data over Cloud

Dipti D. Mehare, Prof. A. V. Deorankar

M. Tech Student, Department of Computer Science, Government college of Engineering, Amravati Maharashtra, India

Associate Professor, Department of Information Technology, Government college of Engineering, Amravati Maharashtra, India

ABSTRACT: Cloud is an application which can be used by using Internet for storing, inserting and managing the data in very less cost. By considering the benefits and advantages of Cloud storage server users can manage their data in well organizations which is outsourced on the Cloud in Encrypted format to secure the data. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Generally keyword based searching approach is used and this is not efficient technique due to this single keyword searching technique is used. This paper provides various techniques for searching encrypted data on cloud. Also propose an effective and practical privacy-preserving computation outsourcing protocol for the encrypted data on cloud. The AES algorithm is utilized encryption and decryption purpose of multimedia files. Experiments on the real-world dataset show that our proposed schemes are efficient, effective and secure.

KEYWORDS: Searchable encryption, cloud computing, Keyword search, privacy preserving, security.

I. INTRODUCTION

The word "cloud" is used to describe the large data that is visually appears from a distance as a cloud. Cloud computing is the type of internet based computing that is used for sharing the devices and data to the computers or other devices. Cloud computing is the new model of IT infrastructure. Cloud computing services for business and end users. Cloud computing services can be private, public or hybrid. Private cloud services are delivered from business to internal users. In public cloud model different public cloud providers are involved Amazon web services, Microsoft Azure, Google Compute Engine, etc. Hybrid cloud is combination of public and private cloud. Cloud computing has been divided into three broad categories: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS). It refers to the manipulating, accessing and configuring to the applications online. It provides online data storage, infrastructure and applications.

As Cloud Computing grow into ubiquitous, more and more sensitive data are being centralized into the cloud, such as emails, individual health records, private albums and images, corporation business figures and facts, official and legal record, etc. By keeping their data into the cloud, the data vendors can be reassured from the load of data storage and management so as to enjoy the on-demand great eminence data storage facility. However, the point that data holders and cloud server are not in the identical confidential domain may put the contract out data at risk, as the cloud server may no lengthier be wholly trusted in such a cloud environment due to a sum of reasons: the cloud server may disclosure datamfacts to unlicensed bodies or be scythed. It follows that sensitive data generally should be encoded prior to contract out for data confidentiality and opposing unauthorized accesses. However, data typically have to be encoded before outsourcing, which marks better service utilization a very complex task assumed that there could be a huge volume of outsourced data records.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Furthermore, in Cloud Computing, data vendors may provide access of their outsourced data with an enormous number of users. The particular users might require to only access certain particular documents they are concerned for the time of a specified period. One of the most common techniques for access or retrieve the particular file and document is through keyword based search rather than repossessing all the encoded documents which is totally unfeasible in cloud computing concepts. But the existing keyword-based search techniques can only return files that contain the exact query keyword, and are unable to hit the files which contain semantic-relevant keywords. In order to reduce the above problem we are going to construct some possible solutions such as searchable encryption schemes, multi-keyword ranked search, fuzzy keyword search, authorized private keyword search, secure ranked keyword search. Also to solve the problem of semantic relevant keyword search the mechanism like semantic or extension keyword search has been designed.

This paper comprises of only data owner, data user, and cloud server. The data owner has a set of data files and wants to outsource it to the cloud. As these data files may contain sensitive information, the data owner encrypts the data before outsourcing due to privacy concerns. The data user is authorized by the data owner and searches the outsourced data files stored on the cloud via some input keywords. The cloud server stores the encrypted data files, and also handles search requests from the data user. Also provide requested data to user.

The confidential data can be accessible only for the data users which are authorized user and authentication is provided by the data owner by sharing the secret key to the user. For sharing secret key the "AES Algorithm" is used and in AES algorithm concept of symmetric key is used .AES algorithm is stronger and faster than triple DES.It provides full specification and design details .The AES is based on substitution and permutation network. AES performs all is computations on bytes rather than bits. AES treats the 128 bits of plaintext block as 16 bytes are arranged in four columns and four rows for processing as a matrix.

II. FUNDAMENTALS

Framework

In case of searching encrypted data on cloud three blocks are very important while studying. First is Data owner, second is Data User and third is Cloud Server. The data owner encrypts the data before uploading them to the cloud server. To perform a search, the data user must be authorized by the data owner. The user generate a trapdoor function when the search request is sent to the cloud server. The server computes the ranked score based on the index and trapdoor.

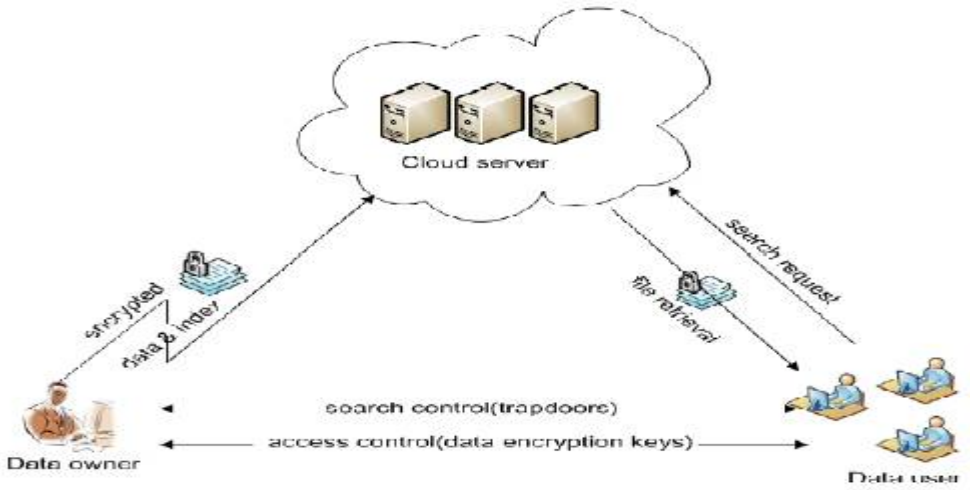

Fig no. 1 Framework of search encrypted cloud data

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

In this system architecture there are three main block Data owner, Data User , Semi trusted cloud server.

A. Data Owner

Data owner is the owner of the data which wants to outsource sensitive information to the cloud .As the data owner is outsourcing there sensitive information there is necessity privacy and security to the data. Data Owner has the collection of documents that can be in text format or multimedia files. First the data owner uploads the data or multimedia files on cloud. The data owner has collection of documents like F={f1,f2,f3,f4,……fn}.Then data owner has does the index generation. Index generation means data owner firstly builds the index I from document collection F and then it generates encrypted document collection. After generating the encrypted document data owner outsource the data to the cloud server and securely distribute secret key to the authorized data user.

B. Data User

Data user is the authorized user to access the document of the data owner. Firstly data user
download the data that he wants to access. Then data user can generate a trapdoor function to fetch the encrypted document from cloud server. Then data user can decrypt the data by using secret which is shared by the data owner the authorized user i.e. private key or public key. For sharing the secret key AES algorithm is used. In AES algorithm concept of symmetric key is used Semi trusted Cloud server.

C. Cloud server

Cloud server stores the encrypted documents collection and encrypted searchable tree index I
from data owner. Cloud server executes trapdoor function which is received from data user and finally it returns back corresponding collection of top k ranked search results for Encrypt document.

Scheme construction

In this scheme four things are very important: First is Key Generation, second is Index Generation, third is Trapdoor Generation and fourth is Search. Scheme is presented as follows.

Key Generation: The data owner randomly generates the secrete key to authorized data user for decrypting document from cloud.

Index Generation: The data owner has collection of documents like F={f1,f2,f3,f4,……fn}. Index generation means data owner firstly builds the index I from document collection F and then it generates encrypted document collection.

Trapdoor Generation: The data user can generate a trapdoor function to fetch the encrypted document from cloud server.

Search: Upon receiving the trapdoor, the cloud server computes the inner product of the trapdoor and the index, and returns the file.

III. RELATED WORK

A. Single keyword searchable encryption

In this scheme secure search over encrypted documents is proposed. When Data owner outsources his document on cloud, the document will get encrypted using AES and stored on cloud. After encryption when any other user wants to search that document, he will specify search query and trapdoor key. The search query will get processed to extract keywords. The keywords will be searched in every encrypted documents within the specified scope(document group as per the trapdoor key) to calculate document wise keywords weight(frequency).Keywords weight according search result re-ranking will be done. Finally search result will be delivered to user. If user wants to download document, he have to specify secrete key. If secrete key is verified, documents will be decrypted and delivered it to user.

This scheme did not contain an index. Thus, the search operation went through the entire document. Goh proposed a secure index using the Bloom filter in. Curtmola et al. gave the formal definition of the searchable encryption and proposed an index structure based on the inverted list in. Wang et al. solved the result ranking problem utilizing the keyword frequency and order-preserving encryption. Boneh et al. proposed the first searchable encryption scheme using the asymmetric encryption scheme. All of these works only supported the single keyword search over the encrypted data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

B. Authorized Private Keyword Searchable Encryption

In this scheme, we focus on the "multi-owner" setting, where the encrypted data are contributed by multiple owners and can be searched by multiple users. In this scheme, we systematically study the problem of authorized private keyword searches (APKS) over encrypted data in cloud computing. We make the following main contributions. First, we propose a fine-grained authorization framework in which every user obtain search capabilities under the authorization of local trusted authorities (LTAs), based on checking for user's *attributes*. Part of the authorization of a higher level LTA is delegated to its lower-level LTAs. The central TA's task is reduced to minimum, and can remain semioffline after initialization. Thus, our framework enjoys a high level of system scalability. Under the above framework, we propose two solutions for searching on encrypted data, namely APKS and APKS+. In APKS+, we enhance the query privacy by preventing that kind of attack with the help of additional proxy servers.

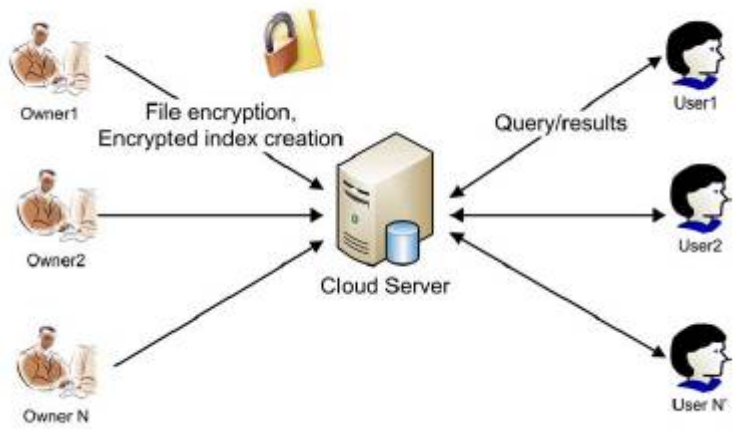

Fig no. 2. System model for multi-owner data outsourcing in cloud computing.

C. Fuzzy Keyword Searchable Encryption

In this scheme, we study a new computing paradigm, called, fuzzy search. Fuzzy search means when searching for relevant records, the system also tries to find those records that include words similar to the keywords in the query, even if they do not match exactly.

In this scheme, we focus on enabling effective privacy preserving fuzzy keyword search in cloud computing. For the first time, we formalize the problem of effective fuzzy keyword search over encrypted cloud data. Fuzzy keyword search greatly enhances system usability by returning the matching files when user's searching inputs exactly match. The predefined keyword or the closest possible matching files based on keyword similarity semantics, when exact match fails. More specifically, this scheme use edit distance to quantify keywords similarity and develop a novel technique, i.e., a wildcard-based technique, for the construction of fuzzy keyword sets.

D. Synonymous Keyword Searchable Encryption

In SBKS keywords are expanded with the synonyms of the keyword. SBKS captures the user true intention of the search by including keywords with similar meanings in the index and the search. The index construction of SBKS begins with the user application extracts distinct keywords from each data files. The user application will use the Synonym Set Construction (SSC) process to expand each extracted keyword into the synonym keyword set.

The SSC process will first add the keyword to the keyword set and check the keyword against dictionary to determine if the keyword is misspelled. If the keyword is misspelled, spell check will be performed on the keyword to generate a list of keyword suggestions with correct spellings. Each keyword in the list of keyword suggestions will be added to the keyword set. After the spell check, the keyword set will go through synonym dictionary to retrieve all synonyms of

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

each keyword in the keyword set. The SSC process will return all distinct synonyms retrieved and all distinct keywords in the keyword set to form the synonym keyword set. Then Each keyword in the synonym keyword set will be hashed with a secure hash function to create a trapdoor. An index entry will be created for each trapdoor. The index construction will end when all the keywords extracted from the data files have been processed with index entries created. All the index entries will form an index file that will be updated to the cloud storage.The cloud computing server will search the index by comparing the trapdoor in each index entry to each trapdoor in the list. The cloud computing server will return all matched index entries back to the user application. The user application will decrypt the information portion of the index entry and return the information to the data users.

IV. CONCLUSIONS

In this paper, a secure and efficient Search Schemes are proposed. In which it Support single as well as Multi-keyword search. We constricted special algorithm that is "AES" algorithm for encryption of files using symmetric key. We address single keyword search as well as s multi-keyword fuzzy and synonymous search over encrypted data with user data privacy protection. Developers can provide the facility of user revocation by providing new secure keys to the required to the authorized users. Once user provides the search query, all the documents that hold the exact query keyword or the semantically related keyword are listed. The user after accessing the file, if he/she finds the file relevant to their search query the user can provide the rating to that file. The user can provide either higher or the lower rating to the document based on the relevance he/she finds with the document. If same query is provided by any user for the next time, the document with higher rating will be resulted first. The aim of adding all the features to the cloud search service is that the cloud consumers can search the most relevant products or data by using the designed system.

REFERENCES

1. 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.
2. Zhangjie Fu, Member, IEEE, Xinle Wu, Qian Wang "Enabling Central Keyword-based Semantic Extension Search over Encrypted Outsourced Data" 2017 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
3. Wenjing Lou, Chair, Thomas, Y.Hou,Ing-Ray Chen, Danfeng Yao, David Evans " Search over Encrypted Data in Cloud Computing" 2016.
4. Zhnghua Sheng:Zhigiang ma:Lin Gu :Ang Li," A Privacy Protecting File System on public cloud Storage Cloud and Services Computing",2011.
5. Ibrahim,A;Hai Jin,Yassin A;Dewingzocs, "Secure Rank -Ordered Search Of Multi-keyword search of multi-keyword trapdoor over encrypted cloud data",2012.
6. chengyu Hu; pengtao Liu ,"Public key Encryption with Ranked Multi-keyword Search" ,2013
7. Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE,and Qian Wang, Member, IEEE," A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL: PP NO: 99 YEAR 2015
8. S.Johnston Cloud computing._ [Online]. Available: https://commons.wikimedia.org/wiki/File:Cloud_computing.svg#/media/File:Cloud_computing.svg
9. C. Strachey, Time sharing in large fast computers,_ in Communications of the ACM,vol. 2, no. 7. ASSOC COMPUTING MACHINERY 1515 BROADWAY, NEW YORK,NY 10036, 1959, pp. 12_13.
10. Standard, _National bureau of standards (us), federal information processing standards publication 46, national technical information service, spring_eld, va, april1997,_ Federal Register, March, vol. 17, 1975.
11. Jin Li†, Qian Wang† , Cong Wang†, Ning Cao‡ , Kui Ren† , and Wenjing Lou‡ "Fuzzy Keyword Search over Encrypted Data in Cloud Computing" presented as part of the Mini-Conference at IEEE INFOCOM 2010
12. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of IEEE Symposium on Security and Privacy'00*, 2000.
13. Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proc. of ACNS'05*, 2005.
14. 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
15. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010,pp. 253–262.
16. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 2013, pp.71–82.
17. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2014.
18. Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou,"Searchable encryption over feature-rich data," IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1–1, DOI: 10.1109/TDSC.2016.2 593 444, 2016.
19. W. Song, B. Wang, Q. Wang, C. Shi, W. Lou, and Z. Peng, "Publicly verifiable computation of polynomials over outsourced data with multiple sources," IEEE Transactions on Information Forensics and Security,vol. PP, no. 99, pp. 1–1, DOI: 10.1109/TIFS.2017.2 705 628, 2017.
20. S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing sift: Privacy preserving outsourcing computation of feature extractions over encrypted image data," IEEE Trans. on Image Processing, vol. 25, no. 7, pp.3411–3425, 2016.