ISSN 2395-1621

Multi-keyword Ranked Search Over Encrypted Cloud Data

[#1]Mr.Sanjay V.Rane, [#2]Mr.Mangesh N.Jangale, [#3]Mr.Govardhan D.Mane
[#4]Mr.Avdhut B.More, [#5]Prof. A. H. Raut

[1]sanjayrane589@gmail.com,
[2]mangeshjangale9@gmail.com

[#1234]Department of Computer Engineering,
[#5]Prof. Department of Computer Engineering,

JSPM's
Imperial College Of Engineering & Research, Wagholi
Pune, India.

ABSTRACT

Now a days cloud computing has become more popular, so more information possessors are actuated to their information to cloud servers for great convenience and less monetary value in data management. In this project the problem of a secure multi-keyword search on cloud is solved by using encryption of data before it actually used. Here, we used deep search learning and keyword based algorithm for searching the file search.

Keywords: KNN, Encryption, Cloud Computing, keyword based search.

ARTICLE INFO

Article History

Received: 9th December 2017

Received in revised form :

9th December 2017

Accepted: 13th December 2017

Published online :

13th December 2017

I. INTRODUCTION

Cloud Computing is a new but increasingly mature model of enterprise IT infrastructure that provides on-demand high quality applications and services from a shared pool of configuration computing resources. The cloud customers, individuals or enterprises, can outsource their local complex data system into the cloud to avoid the costs of building and maintaining a private storage infrastructure. However, some problems may be caused in this circumstance since the Cloud Service Provider (CSP) possesses full control of the outsourced data. Unauthorized operation on the outsourced data may exist on account of curiosity or profit. To protect the privacy of sensitive information, sensitive data (e.g., emails, photo albums, personal health records, financial records, etc.) should be encrypted by the data owner before outsourcing, which makes the traditional and efficient plaintext keyword search technique useless. The simple and awkward method of downloading all the data and decrypting locally is obviously impractical. So, two aspects should be concentrated on to explore privacy-preserving effective search service. Firstly, ranked search, which can enable data users to find the most relevant information quickly, is a very important issue.

Cloud computing is one way of computing. Here the computing resources are shared by many users. The benefits of cloud can be extended from individual users to organizations. The data storage in cloud is one among them. The virtualization of hardware and software resources in cloud nullifies the financial investment for owning the data warehouse and its maintenance. Many cloud platforms like Google Drive, iCloud, SkyDrive, Amazon S3, Dropbox and Microsoft Azure provide storage services. Security and privacy concerns have been the major challenges in cloud computing. The hardware and software security mechanisms like firewalls etc. have been used by cloud provider. These solutions are not sufficient to protect data in cloud from unauthorized users because of low degree of transparency. Since the cloud user and the cloud provider are in the different trusted domain, the outsourced data may be exposed to the vulnerabilities. Thus, before storing the valuable data in cloud, the data needs to be encrypted. Data encryption assures the data confidentiality and integrity. To preserve the data privacy we need to design a searchable algorithm that works on encrypted data.

II. PROBLEM STATEMENT

Even with most advantages of cloud services, outsourcing sensitive information to remote servers brings privacy concern. The cloud service providers that keep data for users may access user's sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt data before outsourcing which is costly. In order to overcome this problem we have developed this system.

III. LITERATURE SURVEY

cloud computing transforms the way information technology(IT) is expended and oversaw, promising enhanced expense efficiencies, quickened development, speedier time-to-market, and the capacity to scale applications on interest (Leighton, 2009).[1] As per Gartner, while the buildup developed exponentially amid 2008 and proceeded since, it is clear that there is a noteworthy movement towards the cloud computing model and that the advantages may be significant (Gartner Hype-Cycle, 2012). Be that as it may, as the cloud's state processing is rising and growing quickly both theoretically and actually, the legitimate/contractual, monetary, administration quality, inter-operability, security and protection issues still posture critical difficulties. In this part, we depict different services and organization models of distributed computing and recognize significant difficulties.

[2]We consider the issue of building a safe cloud storage services on top of an open cloud foundation where the service provider is not totally trusted by the user. We depict, at an abnormal state, a few architectures that consolidate late and non-standard cryptographic primitives with a specific end goal to accomplish our objective. We review the benefits such a construction modeling would give to both customers and service providers and give an outline of late advances in cryptography roused specifically by cloud storage. We propose the first completely homomorphic encryption scheme, taking care of a focal open issue in cryptography. Such a plan permits one to figure subjective capacities over encypted data without the decoding key – i.e., given encryptions E(m1),...,E(mt) of m1,...,mt, one can efficiently process a smaller ciphertext that encrypts f(m1,...,mt) for any efficiently calculable capacity f. This issue was postured by Rivest et al. in 1978.

[3]Completely homomorphic encryption has various applications. For instance, it empowers private queries to a search engine– the user presents an encypted query and the search engine processes a brief encrypted answer while never taking a gander at the query in the clear. It likewise empowers looking on encrypted data – a user stores encypted files on a remote file server and can later have the server recover just files that (when decoded) fulfill some boolean limitation, despite the fact that the server can't unscramble the files all alone. All the more comprehensively, completely homomorphic encryption enhances the efficiency of secure m. We concentrate on the issue of looking on data that is encrypted using a public key system.

[5] Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email portal needs to test whether the email contains the keyword “urgent” so that it could course the email in like manner. Alice, then again does not wish to give the entryway the capacity to decrypt every one of her messages. We build a component that empowers Alice to give a key to the passage that empowers the entryway to test whether "urgent" is a keyword in the email without learning whatever else about the email. We allude to this component as Public Key Encryption with keyword Search.

IV. PROPOSED SYSTEM

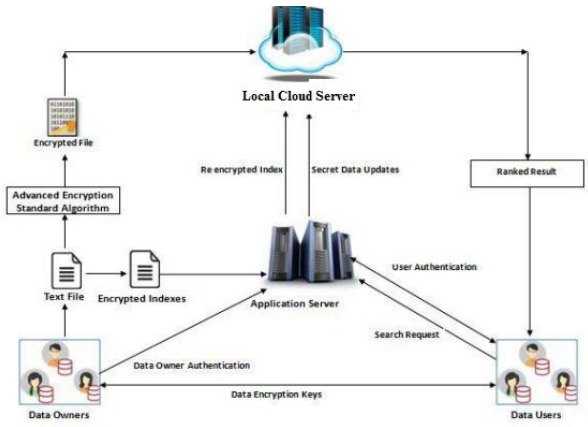

Fig 1. System architecture

1. Keyword Expansion

To enhance the accuracy of search results, the keywords are removed from outsourced content documents required to be stretched out by regular synonyms or comparable words, as cloud customers, searching information may be the synonyms of the predefined keywords.

2. Upload Encrypted Data

After expansion of keywords the data owner assist data with encrypting the document utilizing AES Algorithm and after that upload the encrypted document to the cloud for storage reason. This permits data owner to store their secret key in extremely secure way without presenting it to the clients of framework. For this, secret key is put away again in encrypted frame.

3. Search Module

This module helps clients to enter their query keyword to get the most important documents from set of uploaded documents. This module recovers the documents from cloud which coordinates the query keyword.

4. Download Ranked Results

Clients can download the resultant arrangement of documents just if he/she is approved client who has allowed consent from data owner to download specific document. Owner will send encrypted secret key and session key to client to decrypt the document.

Algorithm:

a. AES algorithm

AES is an iterative instead of Feistel cipher. It depends on "substitution–permutation network". It contains an arrangement of linked operations, some of which include supplanting inputs by particular yields (substitutions) and others include rearranging bits around (permutations). Strangely, AES plays out every one of its calculations on bytes instead of bits.

Steps for AES algorithm:

1. Create a random key for symmetric encryption of user facts.
2. Encrypt the records the use of this random key.
3. Encrypt the random key the use of asymmetric encryption.
4. Send the encrypted message and the encrypted key to the receiver of searched results.

Henceforth, AES treats the 128 bits of a plaintext obstruct as 16 bytes. These 16 bytes are organized in four columns and four rows for preparing as a matrix.

V. CONCLUSION

We have concluded that, A searching can be performed on the encrypted data without decrypting the whole data using above mentioned algorithms. The privacy of the user is maintained in an efficient manner.

REFERENCES

[1] K. Ren, C. Wang, Q. Wang et al., "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," Journal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advance in Cryptology Eurocrypt 2004.Springer,2004 pp. 506–522.

[6] K. Ren, and W. Lou "Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking"-2013

[7] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in *Dependable Systems and Networks (DSN), 2014 44th Annual*

[8] IEEE/IFIP International Conference on. IEEE, 2014, pp. 276–286.B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in *IEEE INFOCOM*, 2014.

