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. 7, Issue 3, March 2019

Fast Phrase Search for Encrypted Cloud Storage

Varsha Pawar[1], Shalaka Shewale[1], Shrutika Vairal[1], Pooja Pawar[1], S. S. Kale[2]

B.E.Students, Department of Computer Engineering, Pune, NBN Sinhgad School of Engineering, Pune, India[1]

Professor, Department of Computer Engineering, NBN Sinhgad School of Engineering,

Pune, India[2]

ABSTRACT: In the development of cloud,data owners are inclined to outsource their data to cloud services.For privacy concerns, sensitive data should be encrypted before outsourcing. The storage and access of confidential documents have been identified as one of the centralproblems in the area. In particular, many researchers investigated solutions to search over encrypted documents stored on remote cloud servers. While many schemes have been proposed to perform conjunctive keyword search, less attention has been noted on more specialized searching techniques. In this paper, present a phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost.Technique uses a series of n-gram filters to support the functionality.Here integrity checking is performed by TPA that will reduce users' time to search and get time. If file is not available then TPA will inform to owner of that file.

KEYWORDS: Cloud storage, Conjunctive keyword search, Phrase search, Privacy, Security, Encryption

I.INTRODUCTION

I.I.Background:

Cloud storage enables large, scalable, and on demand network access to a shared pool of digital data resources. More companies their personal data to the cloud server, and utilize query services to easily access data anytime, anywhere and on any device. The cloud is designed to hold a large number of encrypted documents. With the advent of cloud computing, growing number of clients and leading organizations have started adapting to the private storage outsourcing. This allows resource constrained clients to privately store large amounts of encrypted data in cloud at low cost. However, this prevents one from searching.

I.II.MOTIVATION:-

On web large number of documents is stored in a cloud server, searching against a keyword will result into large number of documents, not related to topic. This motivates the idea of searching against a string, which allows the search to be more specific. proposed one of the earliest works on keyword searching. Their scheme uses public key encryption to allow keywords to be searchable without revealing data content. Waters et al. investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keyword searches. Other interesting problems, such as the ranking of search results so here need is search conjunctive keyword.

II. REVIEW OF LITERATURE

1. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search"Describe an approach for constructing searchable encrypted audit logs which can be combined with any number of existing approaches for creating tamper-resistant logs.Implemented an audit log for database queries that uses hash chains for integrity protection and identity- based encryption with extracted keywords to enable searching on the encrypted log.
2.Hoi Ting Poon and Ali Miri"A low storage phrase search scheme based on bloom filters for encrypted cloud servicesPropose a phrase search scheme, which takes advantage of the space efficiency of Bloom filters, for applications requiring a low storage cost.

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. 7, Issue 3, March 2019

3. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," Propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information.
4. H. Tuo and M. Wenping, "An effective fuzzy keyword search scheme in cloud computing,".Investigate the issue on fuzzy search over cloud data, then by using technique of filter, it improve a efficient keyword search scheme to achieve fuzzy searching with low cost, which is suit for practical cloud computing.
5. Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encryptedcloud data supporting synonym query,"Proposes an effective approach to solve the problem of multi-keyword ranked search over encrypted cloud data supporting synonym queries.performed to validate the approach, showing that the proposed solution is very effective and efficient for multi- keyword ranked searching in a cloud environment .
6. Michel Abdalla, MihirBellare, Dario Catalano, EikeKiltz, TadayoshiKohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier,and Haixia Shi. "Searchable Encryption Revisited ConsistencyTransform of an anonymous identity-based encryption (IBE) scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, we suggest three extensions of the basic notions considered here, namely anonymous hi-erarchical identity-based encryption, public-key encryption with temporary keyword search, and identity-based encryption with keyword search.
7. MihirBellare, Alexandra Boldyreva, and Adam ONeill. "Deterministic and Efficiently Searchable Encryption" One of our constructs, called RSA-DOAEP, has the added featureof being length preserving, so that it is the first example of a public-key cipher. We generalize this to obtain a notion of efficiently-searchable encryption schemes which permit more flexible privacy to search-time trade-offs via a technique called bucketization.
8.Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano "Public Key Encryption With Keyword Search"Proposed the method that will find weather message contain specific keyword or not.
9.Ning Cao, Cong Wang, Ming Li, KuiRen, and Wenjing Lou."Privacy-Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data" Solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing .It ranks the document according to matching result.
10. David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S Jutla, Hugo Krawczyk, Marcel-CatalinRosu, and Michael Steiner." Dynamic Searchable Encryption in Very-Large Databases" single-keyword searches and offers asymptotically optimal server index size, fully parallel searching, and minimal leakage. Our implementation effort brought to the for a several factors ignored by earlier coarse-grained theoretical performance analyses, including low-level space utilization, I/O parallelism and good put.

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. 7, Issue 3, March 2019

III. SYSTEM ARCHITECTURE

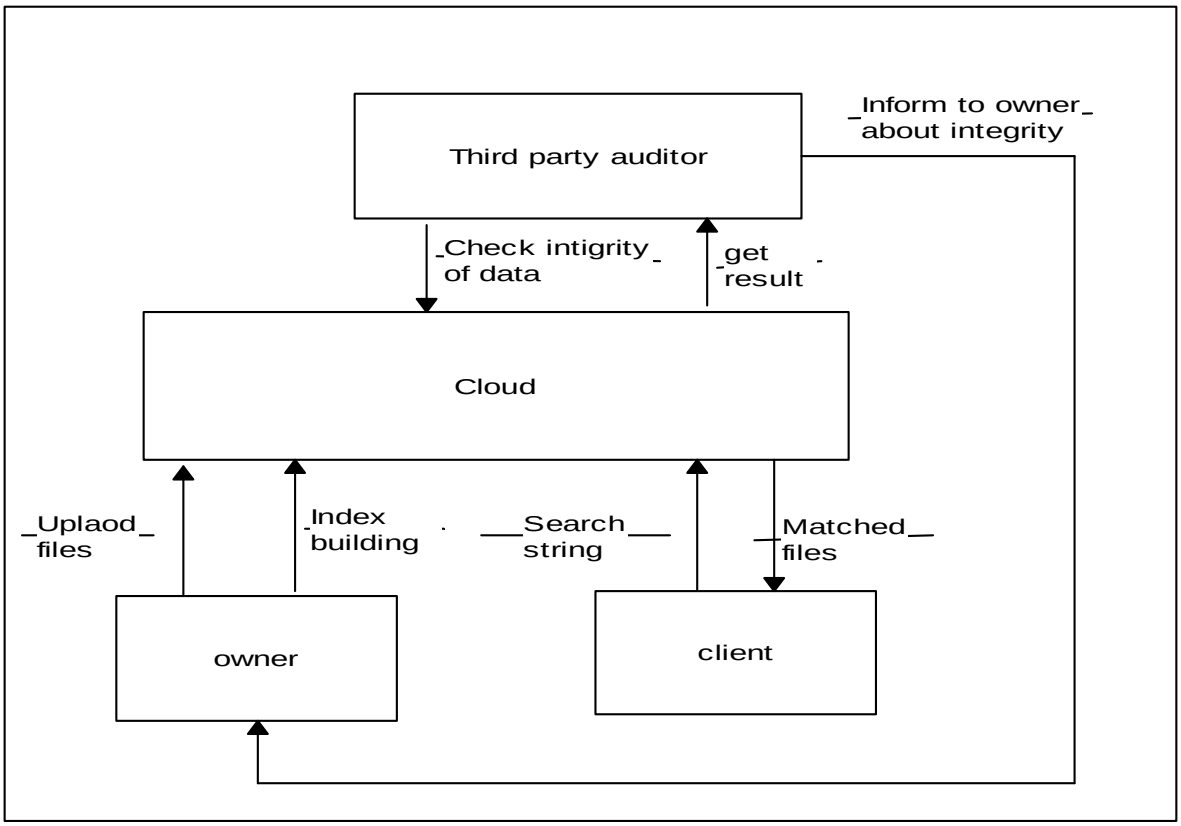


Fig.1: System architecture

System Overview:

Proposed system will provide security to data. present a phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost. Our technique uses a series of n-gram filters to support the functionality. In proposed system computing model, entities are involved such as data owners, data users and TPA (Third party auditor).Data owners have collection of files. Data owners upload the file then bloom filter will builds. Data owners encrypt files and outsource encrypted files to cloud server. When data client wants to search over files from cloud server, He enters string to search. System will give matched files. Then client send request for decryption key a , client will get that on mail. If key matches then only file will download to client. Then client have to enter key. then data client download files and decrypts these files. Third party auditor check integrity of data and inform to owner.

ADVANTAGES-

1. It provides searching in way proposed string search not only looks for those keywords, but also consider the order.
2. Provide multi keyword searching in secure way

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. 7, Issue 3, March 2019

IV. MATHEMATICAL MODEL

Set Theory:

Let us consider S as a system for automatically find best resources.

S= {……

INPUT:

- Identify the inputs

F= {f_1, f_2, f_3 ….., f_n| 'F' as set of functions to execute commands.}

I= {i_1, i_2, i_3…|'I' sets of inputs to the function set }

O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets,}

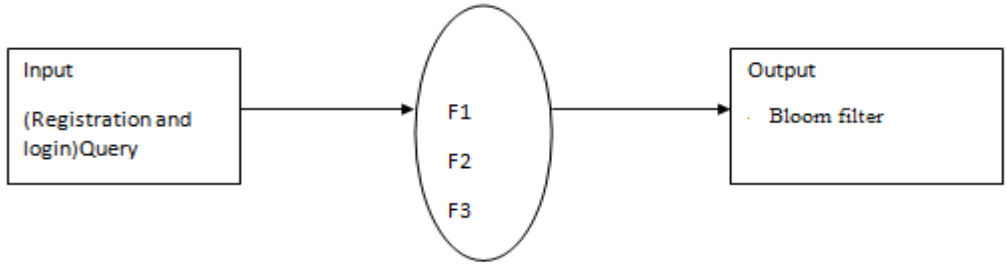
S= {I, F, O}

I = {Query submitted by the user, i.e. Enter keyword }

O = {Output of desired query, i.e. Matched files}

F = {Functions implemented to get the output, i.e. Bloom filter}

Mapping diagram



V. ALGORITHM

Algorithm 1:MD5 Algorithm:

The MD5 message digest algorithm is a most used hash function that produces a 128-bit hash value. Although the MD5 was originally designed to be used as a cryptographic hash function, it has been discovered that it suffers from extensive vulnerabilities. Still It can be used as a checksum to verify the integrity of the data, but only against inadvertent corruption. It is suitable for other non-cryptographic purposes, for example, to determine the partition of a particular key in a partitioned database.

1. Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files.
2. Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.

Steps:

Step 1 – append padded bits

Step 2: Append length

Step 3: Initialize MD Buffer-

Step 4 – Process message in 16-word blocks,

Step 5 – output

Algorithm 2:AES Algorithm For Encryption.

Introduction:

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so This system first convert the 128 bits into 16 bytes.The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data?the data to be encrypted. This array This system call the state array.

You take the following aes steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.

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. 7, Issue 3, March 2019

2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

Decryption:

1.Perform initial decryption round:

XorRoundKey
InvShiftRows
InvSubBytes

2.Perform nine full decryption rounds:

XorRoundKey
InvMixColumns
InvShiftRows
InvSubBytes

3.Perform final XorRoundKey

The same round keys are used in the same order.

VI. RESULT ANALYSIS

Number	File size	Time(ms)
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Table1: Shows file size and time (ms)to upload.

Above table 1 gives the information of uploading time for 30kb, 50kb, 100kb, 1mb and 3mb file size.

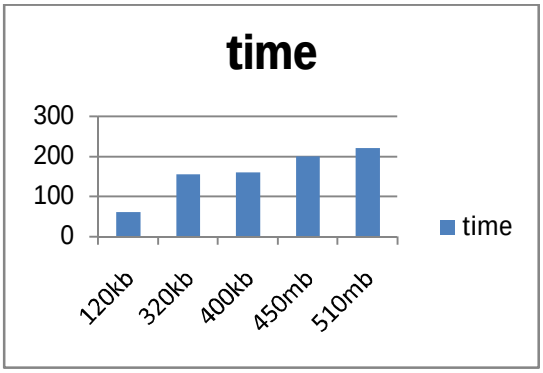


Figure.2 Shows file size on x axis and time (ms)to upload on Y-axis

VII. CONCLUSION

Proposed system propose a novel secure search presented a phrase search scheme basedon Bloom filter that is significantly faster than existing approaches, requiring only a single round of communication and Bloom filter

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. 7, Issue 3, March 2019

verifications. The solution addresses the high computational cost noted in by reformulating phrase search. The technique of constructing a Bloom filter index enables fast verification of Bloom filters in the same manner as indexing.The proposed solution can also be adjusted to achieve maximum speed or highspeed with a reasonable storage cost depending on the application. Integrity checking is performed by TPA.

REFERENCES

1. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in In proceedings of Eurocrypt, 2004, pp. 506–522.
2. Hoi Ting Poon and Ali Miri "A low storage phrase search scheme based on bloom filters for encrypted cloud services," to appear in IEEE International Conference on Cyber Security and Cloud Computing, 2015.
3. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," inProceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012, pp. 556–563.
4, H. Tuo and M. Wenping, "An effective fuzzy keyword search scheme in cloud computing," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 786–789.
5. Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.
6.Michel Abdalla, MihirBellare, Dario Catalano, EikeKiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable Encryption Revisited: Consistency Properties,Relation to Anonymous IBE, and Extensions. volume 21, pages 350–391. Springer, 2008.
7.MihirBellare, Alexandra Boldyreva, and Adam ONeill. Deterministic and Efficiently Searchable Encryption. In Annual International Cryptology Conference, pages 535–552. Springer, 2007.
8. Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public Key Encryption With Keyword Search. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 506–522. Springer, 2004.
9.Ning Cao, Cong Wang, Ming Li, KuiRen, and Wenjing Lou. Privacy- Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data. volume 25, pages 222–233. IEEE, 2014.
10.David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S Jutla, Hugo Krawczyk, Marcel-CatalinRosu, and Michael Steiner. Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation.volume 2014, page 853. Citeseer, 2014.