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 5, May 2019

A New Searchable Encryption Approach and Integrity Checking on Cloud Data

Swapnali Banne, Dr. S. A. Ubale

PG Student, Zeal College of Engineering and Research, Narhe, Pune, India

Guide, Zeal College of Engineering and Research, Narhe, Pune, India

ABSTRACT: With the development of cloud storage, more data owners are inclined to outsource their data to cloud services. For privacy concerns, sensitive data should be encrypted before outsourcing. This paper proposed an efficient and easy-to-implement symmetric searchable encryption scheme (SSE) for string search, which takes one round of communication also and O(n) times of computations over n documents. This system uses hash-chaining instead of chain of encryption operations for index generation, which makes it suitable for lightweight applications. also introduce a new notion of search pattern privacy, which gives a measure of security against the leakage from trapdoor. This system have shown that our scheme is secure under search pattern in distinguish ability definition.

KEYWORDS: Cloud storage, hash-chain, lightweight cryptography, Symmetric key, Searchable encryption, Security,

I.INTRODUCTION

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. This gives rise to a newly emerging field of research, called searchable encryption (SE). On web large number of documents are 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. Searching for string is a multi keyword search where the ordering of keywords is preserved. So in addition to the presence of all these keywords in a document, their ordering and adjacency are should consider while searching. In the SSE scheme, the server is expected to learn nothing about the search queries and data collections. SSE achieves this by using symmetric cryptographic primitives instead of heavy computations of public key encryption at the cost of small leakage of information

II. REVIEW OF LITERATURE

1. 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[5].

2.Transform of an anonymous identity-based encryption (IBE) scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, This system suggest three extensions of the basic notions considered here, namely anonymous hi-hierarchical identity-based encryption, public-key encryption with temporary keyword search, and identity-based encryption with keyword search[1].

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 5, May 2019

3.One of our constructs, called RSA-DOAEP, has the added feature of being length preserving, so that it is the first example of a public-key cipher. This system generalize this to obtain a notion of efficiently-search able encryption schemes which permit more flexible privacy to search-time trade-offs via a technique called bucketization[2].

4. defined the concept of a public key encryption with keyword search (PEKS) and gave two constructions. Constructinga PEKS is related to Identity Based Encryption(IBE),though PEKS seems to be harder to construct. This system showed that PEK Simplies Identity Based Encryption[3].

5. propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various string generation privacy requirements in two different threat models. To improve search experience of the data search service, This system further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given .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[4].

6. This paper presented the first SSE scheme that supports searching for an arbitrary string. The idea of OXT is to retrieve documents matching a token selected from a conjunction query, and then to perform an intersection with the other tokens. This system modified this idea to fit a string search setting as follows. The main idea of our scheme is to retrieve documents matching the first character of a query string, and then to check whether successive characters of the retrieved documents are equal to the second and subsequent characters of the query string. To implement this, This system utilize the fact that one can check whether a text contains a string as a substring by using a multiset[6].

7. present two constructions that This system show secure under our new definition. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions[7].

8. Proposed SSE scheme to satisfy all the properties outlined above. Our construction extends the inverted index approach in several non-trivial ways and introduces new techniques for the design of SSE[8].

9. Introduce the core principles of modern cryptography, with an emphasis on formal definitions, clear assumptions, and rigorous proofs of security. The book begins by focusing on private-key cryptography, including an extensive treatment of private-key encryption, message authentication codes, and hash functions. The authors also present design principles for widely used stream ciphers and block ciphers including RC4, DES, and AES, plus provide provable constructions of stream ciphers and block ciphers from lower-level primitives. The second half of the book covers public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, and El Gamal cryptosystems (and others), followed by a thorough treatment of several standardized public-key encryption and digital signature schemes. [9]

10. present a series of attacks that recover the plain text from DTE- and OPE-encrypted database columns using only the encrypted column and publicly-available auxiliary information. This study the concrete security provided by such systems. This system present a series of attacks that recover the plaintext from DTE- and OPE-encrypted database columns using only the encrypted column and publicly-available auxiliary information. This system consider well-known attacks, including frequency analysis and sorting, as well as new attacks based on combinatorial optimization. [10].

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

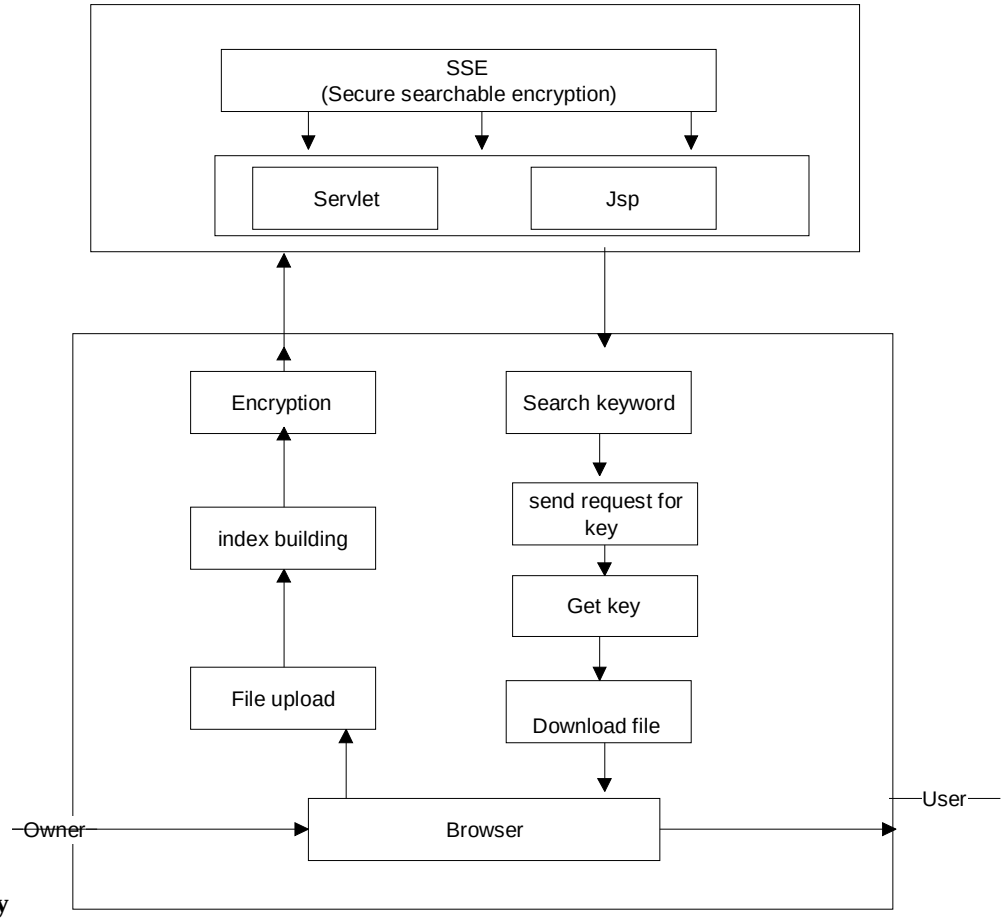
International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

III. PROPOSED SYSTEM



Methodology

Fig.1: System architecture

SYSTEM OVERVIEW-

Proposed system will provide security to data. Secure search protocol is propose in which cloud server can perform secure search trapdoors. provide an efficient and easy-to-implement symmetric searchable encryption scheme (SSE) for string search, In proposed system computing model, four entities are involved such as data owners, data users, cloud server and TPA .Data owners have collection of files. Data owners upload the file then indexes 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 and trapdoor , client will get that on mail. If key and trapdoor matches then only file will download to client. Then client have to enter and have to enter trapdoor . 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.

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 5, May 2019

2. Provide multi keyword searching in secure way

IV.ALGORITHM

Algorithm 1: HMAC-MD5 keyed-hashing algorithm

It's a cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K. Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication. generate a Message Authentication Code (MAC). This system are using the Mac class that provides the functionality of a "Message Authentication Code" (MAC) algorithm. In short, to generate a Message Authentication Code following are steps:

Step 1: Create a new KeyGenerator for the HmacMD5 algorithm.

Step 2: Generate a SecretKey, using generateKey() API method of KeyGenerator.

Step 3: Create a Mac object.

Step 4: Initialize the MAC with the above key, using init(Key key) API method of Mac.

Step 5: Create a new String message and get its byte array.

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.
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

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 5, May 2019

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.

Lightweight Symmetric Searchable Encryption :

1. KeyGen(1_) : KeyGen is a probabilistic key generation algorithm that is run by the client to setup the scheme (see Algorithm
1). It takes a security parameter ʎ, and returns a secret master key km and a mask-key k0 which are to be kept privately at client's end and a session key ks which is to be shared between
client and the server. Client also shares a ʎ, -bit prime p with the server.

2. BuildIndex(km; k0; ks; p) : BuildIndex is a probabilistic algorithm run by the client to generate SI .It takes km, k0, ks, p and returns SI. Since BuildIndex is randomized, This system write this as SI BuildIndex(km;k0;ks;p)

3. Trapdoor(km; ks; p; s) :Trapdoor is a probabilistic algorithm run by the client to generate a trapdoor for a given string of words s = (w1;w2; : : : ;wl). It takes km, k0, ks, p and s as
input and outputs t = (t1; t2; : : : ; tl), where ti is the trapdoor corresponding to the word wi. Since trapdoor is randomized, This system write this as t Trapdoor(km;k0;ks;p)(s) (see Algorithm

4. Search(SI; t) : Search is run by the server in order to search for the documents in D that contain the string s. It takes ks, SI and trapdoor t of the string s as inputs, and returns D(s), the set of identifiers of documents containing the string s

V. RESULT AND DISCUSSION

The proposed system string search, which takes one round of communication, O(n) times of computations over n documents. it gives efficient matched document according to entered string because it consider adjacency of keywords.

Sr.no	No.of documents	position integers Time in(ms)	Hash chaining Time in(ms)
1	1000	850	1010
2	2000	1050	1400
3	3000	1400	1900

Table 1. demonstrated the execution time for searching the entered keywords in no.of documents.

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 5, May 2019

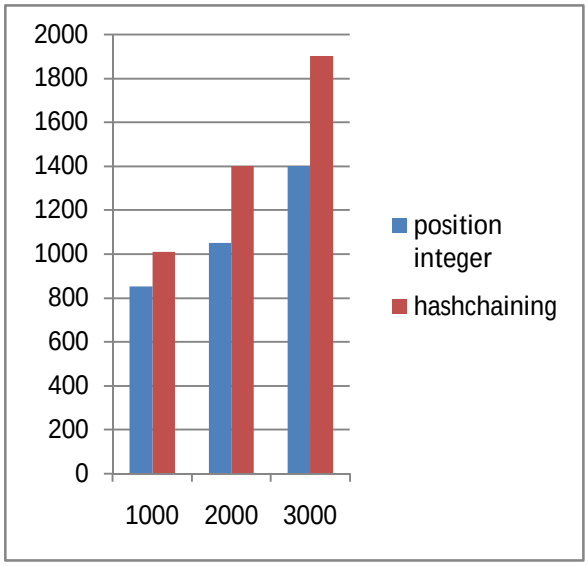


fig 2:Graph showed a pictorial representation of searching time for no.of documents. X- Axis contains no.of document and y-axis contain time in (ms).

Graph shows in proposed system shows how search time varies with respect to the number of documents. in our implementation, search time depends not only on the number of documents returned, but also on the number of documents in which the keywords to be searched are present. This is due to the fact that for efficient implementation, This system first check if all keywords are present in a document. If all key words are present in a document then and only then This system check for the adjacency. It may be noted that the major share of search time is taken by checking.

VI. CONCLUSION

Proposed system propose a novel secure search protocol. It introduce new security scheme in SSE, named, search pattern indistinguishability . It may be observed that with security, although the keywords are guaranteed to be secure from the possible leakage from index, however it does not guarantee the security from the possible leakage from trapdoor. Towards this, system first time introduce probabilistic trapdoor and prove that our scheme is secure under such criterion.

REFERENCES

1.Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, 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.
2.Mihir Bellare, Alexandra Boldyreva, and Adam ONeill. Deterministic and Efficiently Searchable Encryption. In Annual International Cryptology Conference, pages 535–552. Springer, 2007.
3. 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.
4. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. Privacy- Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data. volume 25, pages 222–233. IEEE, 2014.
5.David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. volume 2014, page 853. Citeseer, 2014.
6.Yoshinao Uchide and Noboru Kunihiro. Searchable symmetric encryption capable of searching for an arbitrary string. Wiley Online Library, 2016.
7. Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. volume 19, pages 895–934. IOS Press, 2011.

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 5, May 2019

8. Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic Searchable Symmetric Encryption. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 965–976. ACM, 2012.
9. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC press, 2014.
10. Muhammad Naveed, Seny Kamara, and Charles V Wright. Inference Attacks on Property-Preserving Encrypted Databases. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 644–655. ACM, 2015.