ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

*Visit: www.ijirset.com*

**Vol. 8, 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. We 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

**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. This gives rise to a newly emerging field of research, called searchable encryption (SE).

**I.II.MOTIVATION:-**

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.

## 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, we 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): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, 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. We 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. Proposed the method that will find weather message contain specific keyword or not[3].
5. 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. "propose the first encryption scheme that enables efficient searching for an arbitrary string. Although our scheme leaks some information for the sake of efficiency[6].
7. present two constructions that we 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. Study on cryptography of symmetric and asymmetric encryption[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[10].

## III. PROPOSED WORK

### PROPOSED SYSTEM ARCHITECTURE

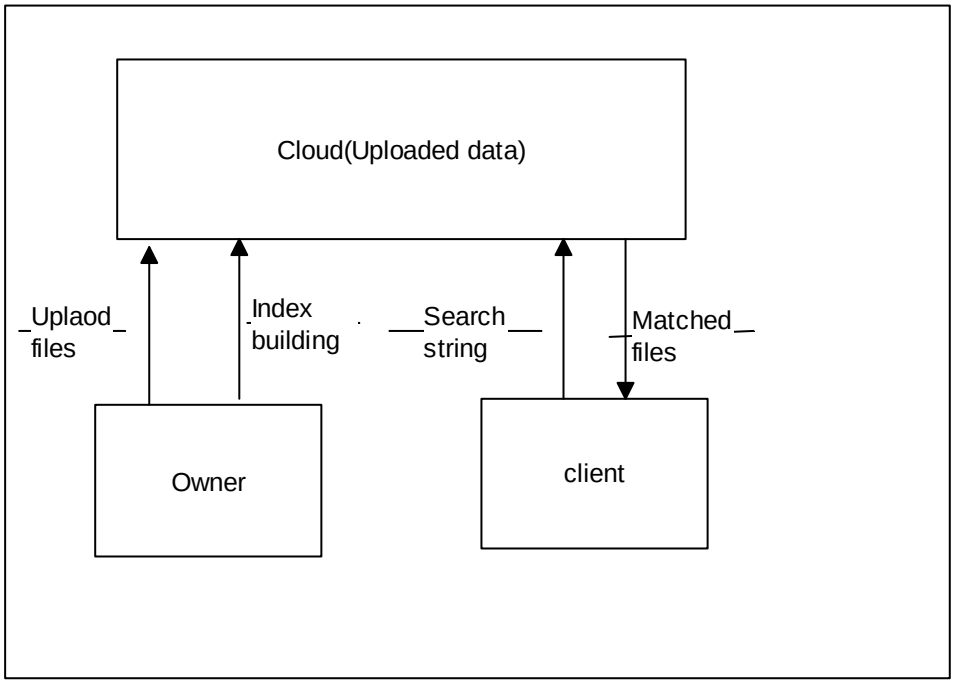


**Fig.1: System architecture**

**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

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

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.
2. Provide multi keyword searching in secure way

## IV. CONCLUSION

Proposed system propose a novel secure search protocol it introduce new security notion 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.
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.