WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# A Symmetric Encrypted Data Identification Using String Incorporated Trapdoors Key

***P. Nithiya[1], Mr. R. Ambikapathy[2]***

[1]Master of Computer Application, Krishnasamy College of Engineering &Technology, Cuddalore
[2]MCA.M.Phil., Assistant Professor, Master of Computer Application, Krishnasamy College of engineering & Technology, Cuddalore.

**ABSTRACT**

A quick and simple symmetric searchable encrypted technique for string searches that only requires one round of communication and a limited amount of calculations over documents is presented in this research. This approach, in contrast to earlier ones, generates indexes using hash chains rather than a sequence of encryption operations, making it appropriate for lightweight applications. The server only learns what it can from the past when it comes to the frequency and relative placements of the words being searched, unlike prior SSE string search systems. This is the first application to suggest trapdoors for string searches in SSE. The major goal is to offer tangible evidence of our scheme's non-adaptive security against an honest but curious server based on the definitions. We also want to present a new concept called search pattern privacy, which provides a measure of security against leaking from trapdoors. Under the notion of search pattern indistinguishability, it is demonstrated that the technique is secure. It explains why the SSE scheme for string search cannot meet the mentioned adaptive indistinguishability criteria and also suggests changes to the scheme so that it can be used against active adversaries at the expense of more communication rounds and memory usage. The scheme is then validated using two different commercial datasets.

## I. INTRODUCTION

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 Here we take an example which will be extended throughout the paper to illustrate our algorithms and data structures

It may be noted that in traditional SE schemes, this is treated as multi-keyword search for keywords : this, is, a, and demonstration.The drawback of this approach is that the adjacency of the words is not considered. However, the proposed string search not only looks for those keywords, but also consider the order. We will continue using this example in the subsections of Section IV to explain different phases of our proposed scheme.

The same non-adaptive security by using a sequence of hashing instead of encryption operations which is faster and suitable for lightweight applications. In schemes are proposed that enables efficient searching for an arbitrary string that may not be extracted as keywords at the cost of leaking some information for the sake of efficiency. In [25], authors introduced a SSE scheme that allows both encrypted phrase searches and proximity ranked multi-keyword searches to encrypted datasets on untrusted cloud. In authors propose a faster way of secure string search based on bloom filters. It may be noted that our approach is based on index based scheme and we prove it to be non adaptively secure according

Our scheme achieves searches in one communication round and requires times computations for searching a string in n documents,which is optimal. Also the scheme requires no storage on the client side and storage on the server side for the n- document collection. Lastly, the scheme guarantees minimal leakage in a sense that server directly knows nothing about the frequency of the words being searched and their relative positions in the documents except what it can learn from the history of search. Unlike the index generation techniques (sequence of encryptions of a key) used in, we use the hash-chain technique, which is faster, and is thus suitable for lightweight applications.

For the first time we address the problem of string search using symmetric searchable encryption against the active adversary, who by trick can place a document of his choice in the document collections. We propose a modification of our scheme to deal with active adversary securely at the cost of maintaining a list of keywords at the client's end and two rounds of communications. We also implement the scheme against two different commercial datasets.

## II. RELATED WORKS

Abdalla et al. [1] revisit searchable encryption, exploring consistency properties and its relation to anonymous identity-based encryption. The work also covers extensions to improve the overall functionality.Cao et al. [2] focus on privacy-preserving multi-keyword ranked search over encrypted cloud data,

presenting techniques to securely search for multiple keywords in encrypted data stored in the cloud.Cash et al. [3] discuss leakage-abuse attacks against searchable encryption, highlighting potential vulnerabilities and proposing countermeasures to enhance security.Cash et al. [4] address the challenges of dynamic searchable encryption in very-large databases, presenting data structures and implementation strategies to efficiently handle dynamic updates.Cash et al. [5] propose highly-scalable searchable symmetric encryption with support for Boolean queries, allowing efficient and secure searching with Boolean logic.Cash and Tessaro [6] examine the locality of searchable symmetric encryption, focusing on the efficiency of search operations with respect to data organization.Curtmola et al. [7] present improved definitions and efficient constructions for searchable symmetric encryption, enhancing the privacy and security guarantees of the encryption schemes.Kamara and Papamanthou [8] propose dynamic searchable symmetric encryption, enabling secure and efficient searching with dynamic updates to the encrypted data.Katz and Lindell [9] provide a comprehensive introduction to modern cryptography, offering fundamental concepts and principles in the field.Li et al. [10] explore lightweight phrase search with symmetric searchable encryption in cloud storage, offering solutions for efficient searching of phrases in encrypted data.

## III. PROPOSEDWORK EXPLANATION

In this proposed system we have introduced the notion of search pattern security and have shown our scheme to be secure under search pattern indistinguishability definition. The novelty of our scheme is that although the index is generated by the client at the beginning, and remains same for the same dataset through out the process and thus static in nature.

The SSE for string search. In the SSE, the client encrypts the data and stores it on the cloud. It may be noted that client can organize the data in an arbitrary manner and can maintain additional data structures to achieve desired data efficiently. In this process, the initial client side computation is thus as large as the data, but subsequent computations to access data is less for both client and the cloud server.

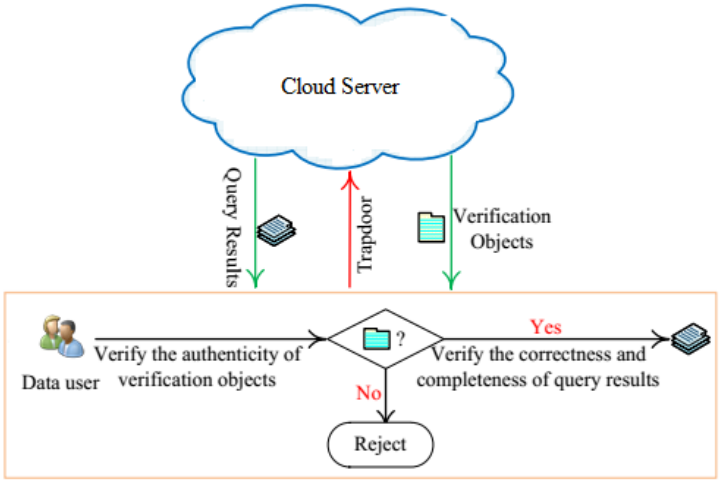



Fig.1 System Architecture

### *3.1 Data Owner*

In Data Owner module, Initially Data Owner must have to register their detail. After successful registration data owner can login and upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users. After request approval data owner will send the trapdoor key and verification object through mail.

### *3.2 Data User*

In Data User module, Initially Data Users must have to register their detail and after login he/she has to verify their login through secret key. Data Users can search all the files upload by data owners. He/she can send request to the files and then request will send to the data owners. If data owner approve the request then he/she will receive trapdoor, verification object and decryption key in registered mail

### *3.3 Cloud Server (CS)*

In Cloud Server module, Cloud Provider light weight can view all files details. Cloud can view all data owners and data users details.

## IV. RESULTS AND DISCUSSION

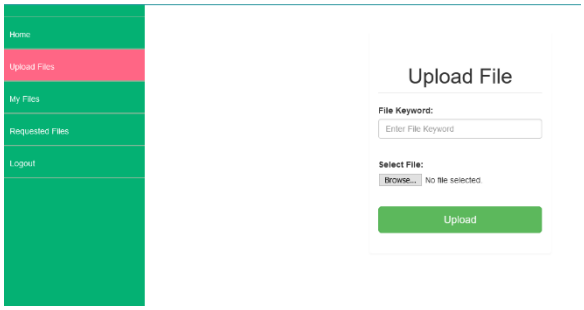
Owner login Page


This is home page

**User login**

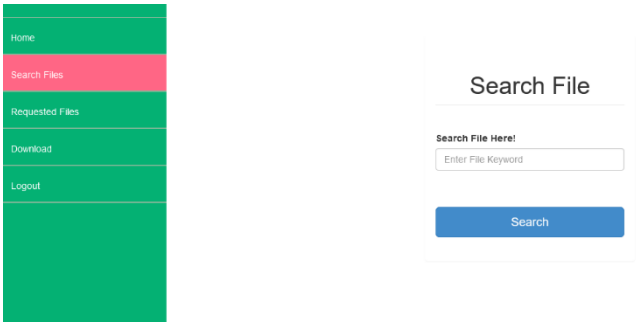

This is user login page

**Data owner for upload file**




This is upload page where Data owner is upload file

**User for search file**




This is  search page where User for search file

## V. CONCLUSION

The increasing number of documents stored in cloud, searching for the desired document can be a difficult and resource intensive task. One solution may be to use symmetric searchable encryption (SSE) which allows one party to outsource the storage of its data to another party (a cloud) privately while enabling to search selectively over it. In this paper we revisited the security definitions of and proposed a new lightweight SSE scheme for string search.

**REFERENCES**

[1] Michel Abdalla, Mihir Bellare, Dario Catalano, Tadayoshi Kohno, Tanja Lange and Haixia Shi. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. volume 21, pages 350–391. Springer, 2008.

[2] 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.

[3] David Cash, Paul Grubbs, Jason Perry, and Thomas Ristenpart. Leakage- Abuse Attacks Against Searchable Encryption. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 668–679. ACM, 2015.

[4] David Cash, 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.

[5] David Cash, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel- C˘at˘alin Ros¸u, and Michael Steiner. Highly-Scalable Searchable Symmetric Encryption With Support for Boolean Queries. In Advances in Cryptology–CRYPTO 2013, pages 353–373. Springer, 2013.

[6] David Cash and Stefano Tessaro. The Locality of Searchable Symmetric Encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 351–368. Springer, 2014.

[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]SenyKamara,Charalampos Papamanthou. 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] Mingchu Li, Wei Jia, Cheng Guo, Weifeng Sun, and Xin: Lightweight Phrase Search With Symmetric Searchable Encryption in Cloud Storage. In Information Technology-New Generations (ITNG), 2015 12th International Conference on, pages 174–178. IEEE, 2015.