 ISSN: 2454-4248
15 – 19

Symmetric Searchable Encryption Scheme for String Identification

Puja Bachhav
PG Student,Department of Computer Engineering
GHRIET, Wagholi , Pune , India
pujabachhav1818@gmail.com

Prof. Rachana Sable
Assistant Professor, Department of Computer Engg
GHRIET, Wagholi, Pune, India
rachana.sable@raisoni.net

Abstract: Searchable Encryption (SE) allows a user to upload data to the cloud and to search it in a remote fashion while preserving the privacy of both the data and the queries. In this paper, we provide an efficient and the very easy to implement Symmetric Searchable Encryption Scheme i.e. (SSE). This algorithm takes the one round of communication as O(n) times of computations over n number of documents . We also introduced a new type of Search Pattern Privacy, which provides a measure of security over the leakage form trapdoor. We also suggest the modifications of our scheme for string search which cannot accomplish the adaptive indistinguishability formula [1]. The present method provides the functionality while keeping contents of the documents confidential, either it has linear difficulty in the total size of the paper or needs to remove keywords when the documents are stored [5]. We also propose modifications in our scheme so that the scheme can be used over the active adversaries at the cost of multiple rounds of transmission and the memory space [1]. We can also prove our scheme over different commercial datasets. Also in this paper, we use the Hash chaining method instead of chain of encryption function for index generation which makes it suitable for light weight applications. We are the first to propose measure trapdoors in Symmetric Searchable Encryption for the string search [1].

***Index Terms**: Cloud Storage, Database Security, Private information Retrieval, Searchable encryption, secure index.*

*****

I. INTRODUCTION

The cloud is designed to grab a large amount of encrypted documents. With the occurrence of the cloud computing, growing number of clients and the leading organizations have started adopting the private cache outsourcing [1]. Also the cloud computing allows companies and automatics to outsource their data and the computation. But in most SE schemes, a small amount of information crack is often tolerated in series to achieve some level of quantity [9]. Searchable Encryption (SE) schemes allow a cloud user to outsource some cipher data and to further delegate the search operations against the encrypted data to the CSP. Acceptance of the Cloud computing [10] is threatened by unresolved security problem that influence both the Cloud provider as well as the cloud user. To ensure the data privacy, the users generally encrypt the data before outsource it on to the cloud but it makes very effective data application is a very challenging task [10]. In this paper, we also interested in the solutions which are communication-efficient and the same time, regard the complete privacy of Alice [8].

The keyword search is not always useful in the searching text, and there is a request for searching the texts for the random string as mentioned previously [5]. The searchable symmetric encryption lies between the server managing an encrypted index and the client (user). In order to protect the data security, the users generally encrypt their data before uploading them to the cloud [3]. Searchable Encryption is one of the basic foundation for the data utilization in the cloud computing. We design and implement the proof of concept prototype and test our scheme with the real dataset of files containing about 120,000 keywords and more than 100,000 documents to analyze the performance of the scheme. The benefits of cloud services such as increased availability and flexibility come at a high cost in terms of new security and privacy challenges [9]. When we compared with the related work there was a large amount of work on searching on encrypted data. The private information retrieval (PIR) is an associated problem that is concerned with the communication- efficient revival of public [8].

II. LITERATURE SURVEY

[1] 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.

[2] Ghosh Ray , I. Rahulamathavan , Y. and Rajarajan, M. 2018. A new lightweight symmetric searchable encryption scheme for string identification .IEEE Transactions on Cloud Computing , doi:10.1109/TCC.2018.2820014

 ISSN: 2454-4248
15 – 19

[3] Cedric Van Rompay ,Refik Molva, Melek Onen EURECOM , France A leakage – abuse attack against multi-user searchable encryption , May 11 2017

[4]Shahzaib Tahir, Yogachandran Rahulamathavn ,Muttukrishnan Rajarajan A New Secure and Lightweight Searchable Encr yption Scheme over Encrypted Cloud Data IEEE transactions on Emerging Topics in Computing, August 2017.

[5] Arora, S.S. Tyagi Analysis of Symmetric Searchable Encryption and data retrieval in cloud computing. International Journal of Computer Applications (0975 – 8887) Volume 127 – No.12, October 2015.

Searchable Encryption has been focus for many leading research groups and several results are proposed. Cloud computing allows users to share the cloud data securely with the other users and outsource computing to cloud servers [3].

In [2], SSE schemes are developed for string search. The first SSE scheme for phrase search and this scheme work in two phases, each taking one round of communication. Single user searchable encryption (SUSE). Subsequently , a number of various SE schemes have been proposed for different purposes, including using conjunctive keyword search or fuzzy keyword search to extend the searching functionality [4].

A multi user setting for SSE has also been studied. SSE in a multi-user setting addresses the following scenario:

A data owner stores data on a server and clients other than the data owner retrieve these from the server [5].

Kissel [5] proposed an SSE scheme that supports phrase search and requires one communication round. This scheme reveals the appearance positions of keywords to a server to check whether two words appear successively.

In [3] Schemes for secure outsourcing of client data with search capability are being increasingly marketed and deployed. In the literature, schemes for accomplishing this efficiently are called Searchable Encryption (SE). They achieve high efficiency with provable security by means of a quantifiable leakage profile. However, the degree to which SE leakage can be exploited by an adversary is not well understood. To address this, we present a characterization of the leakage profiles of in-the-wild searchable encryption products and SE schemes in the literature, and present attack models based on an adversarial server's prior knowledge.

III. EXISTING SYSTEM:

Searchable encryption has been the focus for many leading research groups and several results authors d•efined computational and statistical relaxations of the existing notion of perfect consistency and provided a new scheme that was statistically consistent [1]. They also proposed a transYformation of an anonymous identity based encryption scheme (IBE) to a secure public key encryption with keyword search scheme (PEKS) that guarantees consistency [5].

Authors introduced as-strong as-possible meanings of privacy and a few developments for public key base encryption plans where the encryption algorithm is deterministic. In a similar work, new strategies were proposed for database encryption that grant quick (for example sub-direct, and in actuality logarithmic, time) seek while provably giving security that is as solid as conceivable subject to this fast search requirement.

IV. PROPOSED METHODOLOGY

We address the issue of string seek utilizing symmetric searchable encryption against the active adversary, who by trap can put a record of his decision in the archive accumulations. We propose a change of our plan to manage active adversary safely at the expense of keeping up a rundown of catchphrases at the customer's end and two rounds of communications.

SSE plans for string search, the index tables are produced by making linked-lists comparing to keywords, where data's identified with event of the watchword in I-th report is put away in I-th node alongside the key, say ki+1, and is encrypted with a key Which prompts a succession of encryption capacities for creating the list and a grouping of decryption capacities while searching.

In what follows, we will signify message sending parties by X, a message accepting party will be denoted by Y, and a server/storage supplier will be signified by S.

Definition: A Public Key Storage with Keyword Search consists of the following probabilistic polynomial time aXlgorithms and protocols:

KeyGen(1s): Outputs public and private keys, Apublic and Aprivate of length s.

SendX,S(M, K, Apublic) This is either a non- interactive or interactive two-party protocol that allows to send the message M to a server , encrypted under some public key Apublic, and also associates M with each keyword in the set K. The values M, K are private inputs that only the message-sending party X holds.

RetrieveY,S(w, Aprivate): This is a two party protocol between a user Y and a server thSat retrieves all messageYs associated with the keyword w for the user . The inputs w, Aprivate are private inputs held only by. This protocol also removes the retrieved messages from the server and properly maintains the keyword references [3].

 ISSN: 2454-4248
15 – 19

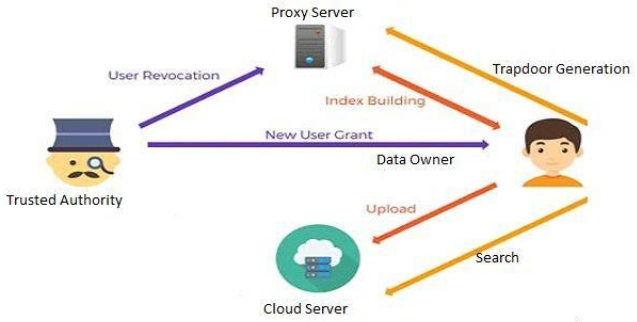


Fig. Architecture of Proposed System

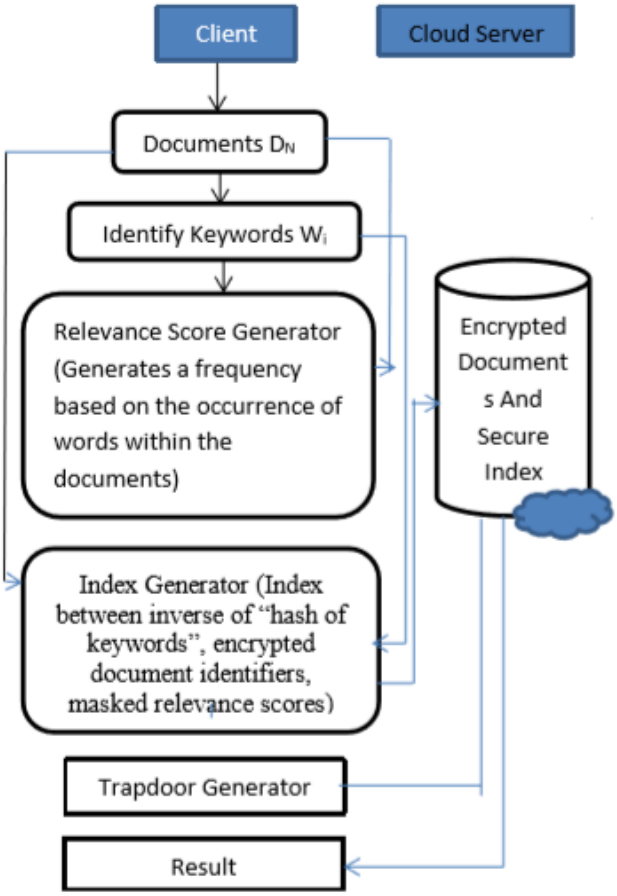
In our proposed system framework we are going to address the problem of String search using Symmetric reduces searchable encryption against the active adversary. Who by trick place a document of his choice in the document collections.
As shown in Figure, our system consists of four players: a trusted authority, a cloud server, a proxy server and a user/data owner.

1. Cloud server (CS)
A Cloud server teems with tremendous storage room and rich computational assets, which is generally worked by the Cloud service provider, for example, Amazon and Microsoft.

2. Proxy server (PS)
An proxy server is acquainted with facilitate user's secure use of Cloud service, which can be sent inside every enterprise (e.g., under the supervision of Chief Data Protection Officer of an association).

3. System Setup
A trusted Authority calls setup to acquire an public key PK and an master secret key MSK. At that point he picks an irregular number β ε Zp and sets Kmk= β as the search maste key. After the generation of these three keys , the trusted specialist sends the public key PK to a cloud server and keeps the master secret key MSK and the search master key Kmk secret.

V.ALGORITHM



Private-key searchable encryption:
In the setting of searching on private-key-encr ypted data, the user himself encr ypts the data, so he can organize it in an arbitrary way (before encr yption) and include additional data structures to allow for efficient access of relevant data[5].

Public-key searchable encryption.
In the setting of searching on public-key- encr ypted data, users who encr ypt the data (and send it to the server) can be different from the owner of the decr yption key.

Data Owner:-
In this module client used our system with admin's authenticates user id and authenticate password. System just checked client will have an authorization to access into system.

Cloud Server:-
In this module cloud provides all the
required information to the server which will needs for user.

Authentication:-

 ISSN: 2454-4248
15 – 19

This will validate the applicable documents to the encrypted keywords and recognize to the information owner.

Advantages of Proposed System:

- Symmetric Searchable Encryption scheme, the server is relied upon to pick up nothing about the search queries and information accumulations.
- Symmetric Searchable Encryption scheme this by utilizing symmetric cryptographic natives rather than heavy calculations of public key encryption at the expense of little spillage of data.
- SSE construction, achieving sub linear search time and introduced the notion of non-adaptive and adaptive in distinguishability definitions of security for SSE .
- A lower efforts for to generate result i.e. retrieved desired information from cloud.
- As an outcome, numerous ABE (Attribute Based Encryption) schemes have been proposed for different purposes, for example, expanding the usefulness or enhancing the security or effectiveness of the framework.
- It the execution time.
- It improves the speed of data retrieval operations.
- It enhances the efficiency

Algorithms [14]:

Phase 1 : Key Gen

a) Input: A security parameter λ

b)KeyGen: Generate keys K, ks{0,1} λ pCSPRNG(1 λ)

c)Output: Master key K and session key ks

Phase 2: Build_Index

a)Input: A set of documents D and a master key K, a Hash function H(.)

b)Initialization:

Initialize dynamic 2D Array A

Scan D and build W, a set of unique and distinct keywords occurring in D.

Initialize Prime number p of size ��+1 bits .

c)Build Index I:

for 1<t<|Wi|

let aHk (Wi)

compute a-1 and store it in A[1][t]

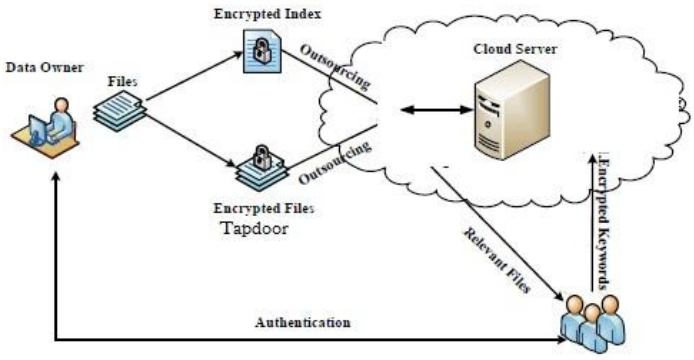
compute Ek (id(DN)), store it in A[t][1];

calculate the RF for each Wi occurring in DN using equation (1) and store the value at the respective locations within A;

Mask (RF):

For 1<m<number of columns in A For 1<n<number of rows in A A[n+1][m+1]=A[n+1][m+1]* random values d)Output: Index table I [14]

VI. SYSTEM ARCHITECTURE:



VII. SYSTEM REQUIREMENTS:

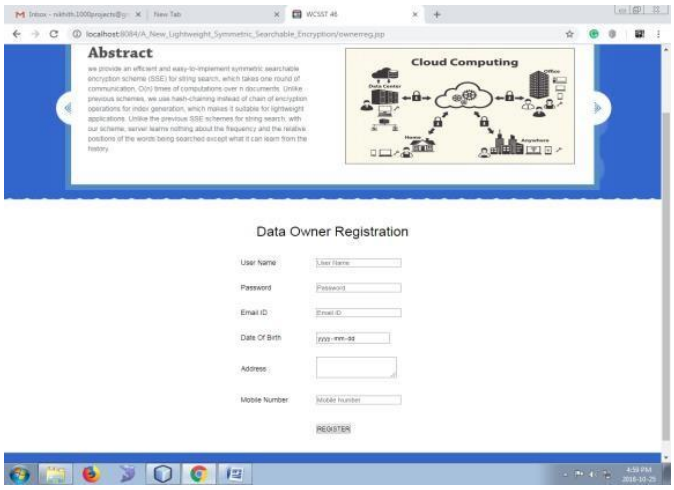
Hardware Requirements:

System	: Pentium Dual Core.
Hard Disk	: 120 GB.
Monitor	: 15'' LED
Input Devices	: Keyboard, Mouse
Ram	:1GB.

Software Requirements:

Operating system	: Windows 7.
Coding Language	:JAVA/J2EE
Tool	: Net beans 7.2.1
Database	: MYSQL

VIII. RESULTS



 ISSN: 2454-4248
15 – 19

IX. CONCLUSION

The proposed system developing an efficient implementation to achieve an encrypted search in a mobile cloud. Also we propose a recent work on leakage-abuse attacks paved the way for a better understanding of privacy in SE.

X. REFERENCES

[1]. 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.

[2]. Dan Boneh, Eyal Kushilevitz, Rafail Ostrovsky, andWilliam E Skeith III. Public Key Encryption That Allows PIR Queries. In Annual International Cryptology Conference, pages 50–67. Springer, 2007.

[3]. 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.

[4]. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC press, 2014.

[5]. Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos Keromytis, and Steve Bellovin. Blind Seer: A Scalable Private DBMS. In 2014 IEEE Symposium on Security and Privacy, pages 359–374. IEEE, 2014.

[6]. Hoi Ting Poon and Ali Miri. Fast phrase search for encrypted cloud storage. IEEE Transactions on Cloud Computing, 2017.

[7]. Emil Stefanov, Charalampos Papamanthou, and laine Shi. Practical Dynamic Searchable ncryption With Small Leakage. In NDSS, volume 4, pages 23–26, 2014.

[8]. D. Boneh, G. Crescenzo, R. Ostrovsky, G. ersiano. Public Key Encryption with Keyword earch. EUROCRYPT 2004: 506-522

[9]. D. Cash, P. Grubbs, J. Perry, and T. istenpart. Leakage-Abuse Attacks Against earchable Encryption. In Proceedings of the 2nd ACM SIGSAC Conference on Computer and ommunications Security, Denver, CO, USA, October 12-6, 2015, pages 668–679, 2015.

[10]. 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.

[11]. Ghosh Ray , I. Rahulamathavan , Y. and Rajarajan, M. 2018. A new lightweight symmetric searchable encryption scheme for string

[12]. 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.

[13]. Ghosh Ray , I. Rahulamathavan , Y. and Rajarajan, M. 2018. A new lightweight symmetric searchable encryption scheme for string.

[14]. eprint.iacr.org