IJMTST | Volume: 2 | Issue: 09 | September 2016 | ISSN: 2455-3778

SPCHS Construction for Expeditious Keyword Search in Cipher Text

L. Shivani[1] | D. Venkatesh[2] | Dr. Ramakrishna[3]

[1]PG Scholar, Department of IT, Sridevi Women's Engineering College, Hyderabad.
[2]Assistant Professor, Department of IT, Sridevi Women's Engineering College, Hyderabad.
[3]Professor and HOD, Department of IT, Sridevi Women's Engineering College, Hyderabad

ABSTRACT

The subsisting public-key encryption schemes which are semantically secure, take linear search time with the total number of cipher texts, thus making data retrieval from databases arduous or time consuming. So, in order to rectify the current quandary, the paper proposes SPCHS Methodology for Expeditious Keyword Search. In Searchable Public Key Cipher texts with Obnubilated Structures (SPCHS), the concept of obnubilated structures is introduced. Here, the concept of filtering is utilized efficiently. This in turn, makes data retrieval from sizably voluminous scale databases far more facile by reducing the time intricacy as well as ensuring efficient performance. The time involution of our scheme depends only on the genuine number of engendered cipher texts rather than all the number of cipher texts. Given a keyword for a file search, predicated on the filtering mechanism we designate the file extension or type which has to be returned thus ruling out all the other possibilities which not only makes probing more facile but withal preserves time involution. This article gives an overview about SPCHS Mechanism and the sundry methods adopted.

KEYWORDS: *Public-Key searchable encryption, semantic security. Obnubilated Structures, homogeneous attribute search*

I. INTRODUCTION

Predicated on the PUBLIC-KEY encryption with keyword search (PEKS), introduced by Boneh et al. in [1], the keyword-searchable cipher texts can be uploaded to the server by anyone who kens the receiver's public-key. The keyword search can then be entrusted by the receiver. To be more categorical, the keywords are extracted from the file first predicated on kindred attribute search [2]. Then, the file along with its extracted keywords is encrypted by the sender discretely to engender the corresponding cipher texts. The resultant cipher texts are then sent to the server. The receiver then entrusts a keyword search trapdoor to the server in order to receive the files containing the designated keyword. The server then returns the corresponding encrypted files to the receiver and he decrypts the corresponding files with his private key. The subsisting public-key encryption schemes which are semantically secure, take search time linear with the total number of cipher texts, thus making the data retrieval form databases arduous or time consuming. Ergo, in order to procure amended search performance and to reduce time involution, a more efficient search performance is crucial. In network communication at server side it is consequential to make some fine-tuned data available to certain users only. It is additionally consequential to keep identity of users secure who are accessing the content. In this simple method of data aegis we are getting the quandary at network communicated data receiver may want to keep data secure and receiver may want to bulwark it from administrator withal. The Public key encryption technique which was introduced gives us advantage that if anyone kens the receiver's public key can upload file and keyword to the server. The receiver gives ascendancy to the server for keyword search. While sending the file sender sends the file in encrypted format and culled keywords and content extracted from the file and outputted cipher text. When receiver wants any type of file having concrete keyword he gives a keyword for

search to the trapdoor at the server. Utilizer additionally gives categorical content search. Server commences the process of finding and server finds the file which is in an encrypted format and contained keyword queried by client without any cognizance of pristine contain of file and content withal and provides the file to the receiver. Receiver of the file will decrypt these file and if want this is a spam then can report to server additionally

II. Related Work

A. Subsisting system

Secure public-key searchable encryption schemes take search time linear with the total number of the cipher texts. This makes retrieval from sizably voluminous-scale databases prohibitive Subsisting semantically secure PEKS schemes take search time linear with the total number of all cipher texts. This betokens that the subsisting obnubilated structure of cipher texts stays confidential, since the local privacy only contains the relationship of the incipient engendered cipher texts.

Search on encrypted data has been investigated in recent years. From a Cryptographic perspective, the existing works fall into two categories, i.e., symmetric searchable encryption and public-key searchable encryption. Searchable symmetric encryption (SSE) [2] allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. Public Key Encryption with Keyword Search (PEKS) scheme enable one to search the encrypted data with a keyword without revealing any information and preserving its semantic security [1].[1]Proposed searchable public-key cipher texts with hidden structures (SPCHS) for keyword search as fast as possible without sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable cipher texts are structured by hidden relations, and with the search trapdoor corresponding to a keyword, the minimum information of the relations is disclosed to a search algorithm as the guidance to find all matching cipher texts efficiently. [2] Introduced a new encryption) schemes. The approach is highly parallelizable and dynamic. Previous the only method for achieving sub-linear time search is the inverted index approach, which requires the search algorithm to access a sequence of memory locations.

A new approach for designing SSE schemes that yields constructions with sub-linear search time but that has none of the limitations of the inverted index approach. In particular approach is simple, highly parallel and can easily handle updates. Scheme also achieves the following important properties: (a) it enjoys a strong notion of security, namely security against adaptive chosen-keyword attacks; (b) compared to existing sub-linear dynamic SSE schemes updates in our scheme do not leak any information, apart from information that can be inferred from previous search tokens; (c) it can be implemented efficiently in external memory (with logarithmic I/O overhead). The technique is simple and uses a red-black tree data structure. [3] Provides Asymmetric searchable encryption (ASE) schemes which support two special features, namely message recovery and flexible search authorization.

The message recovery feature requires that a cipher text not only allows the data owner to recover the plaintext but also allows third-party servers to search in it. The flexible searchable authorization feature requires that the data owner can authorize a third-party server in three different ways: (1) authorize the server to search any message at the data owner's interest by assigning a message-dependent trapdoor (i.e. the server can only determine whether the message encoded in the trapdoor is equal to the plaintext inside a cipher text); (2) authorize the server to search any message at the server's interests by assigning a master trapdoor (i.e. the server can choose a message at its will and see whether it is equal to the plaintext inside any cipher text); (3) authorize the server to perform both types of searches. [4]

Proposed PEKS, where a proxy server, who responds the keyword queries of a receiver, can know the content of keywords by implementing KGA. Moreover, it is efficient under the practical condition that the size of the keyword space is not more than the polynomial level. [6] Gives broader view on what can be achieved regarding trapdoor privacy in asymmetric searchable encryption schemes, and bridge the gap between previous definitions, which give limited privacy guarantees in practice against search patterns. The paper proposes the notion of Strong Search Pattern Privacy for PEKS and constructs a scheme that achieves this security notion.

B. Proposed system

Searchable Public-Key Cipher texts with Obnubilated Structures (SPCHS) for keyword search as expeditious as possible without

sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable cipher texts are structured by obnubilated cognations, and with the search trapdoor corresponding to a keyword, the minimum information of the cognations is disclosed to a search algorithm as the guidance to find all matching cipher texts efficiently. Proposed to encrypt structured data and a secure method to probe these data. To fortify the dynamic update of the encrypted data proposed the dynamic searchable symmetric encryption in and further enhanced its security in at the cost of immensely colossal index.

C. Advantages

Has the advantage that anyone who kens the receiver's public key can upload keyword-searchable cipher texts to a server. A wins in the SSCKSA game of the above SPCHS instance We construct a special keyword balanced binary tree as the index, and propose a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search with advantage AdvSS-CKSA SPCHS;A, in which A makes at most qt queries to oracle QTrap

III. Implementation

Utilizer

In our proposed architecture utilizer is end utilizer of our application, and data utilizer. Whenever he wants the data he can probe from our application, data retrieve from the data engine. While getting data performs decryption and most proximate-neighbors results at utilizer side.

Data Owner

In our proposed architecture admin is main utilizer of our application. He maintains the POI data. System will perform MOPE & Encryption & decryption operations. Owner Can Apportion Keys to users.

Location Privacy Module

As mentioned anteriorly, the dataset of points of in-tersest represents a paramount asset for the data owner, and a consequential source of revenue. Ergo, the coordinates of the points should not be kenned to the server. We surmise a veracious-but-curious cloud accommodation provider. In this model, the server executes correctly the given protocol for processing kNN queries, but will additionally endeavor to infer the location of the data points. It is thus obligatory to encrypt all information stored and processed at the server. To sanction query evaluation, a special type of encryption that sanctions processing on cipher texts is obligatory. In our case, we utilize the mOPE technique from .mope is a provably secure order-preserving encryption method

Database Outsourcing Module

The server receives the dataset of points of interest from the data owner in encrypted format, together with some adscititious encrypted data structures needed for query processing. The server receives kNN requests from the clients, processes them and returns the results. Albeit the cloud provider typically possesses potent computational resources, processing on encrypted data incurs a consequential processing overhead, so performance considerations at the cloud server represent a consequential. The client has a query point Q and wishes to find the point's most proximate neighbors. The client sends its encrypted location query to the server, and receives most proximate neighbors as a result. Note that, due to the fact that the data points are encrypted, the client withal needs to perform a minute part in the query processing itself.

IV. Scheme from Collision-Free Full – Identity Malleable IBKEM

A SPCHS scheme is formed with IBE Collision-free full -Identity Malleable IBKEM with semantic security [1]. Several interesting properties are identified i.e. collision-freeness and full-identity malleability in some IBKEM instances, and formalized these properties to build a SPCHS. Given are two collision-free full-identity malleable IBKEM instances that are completely secured. In IBKEM, a sender encapsulates a key K to an intended receiver ID. Of course, receiver ID can DE capsulate and obtain K, and the sender knows that receiver ID will obtain K. However, a non-intended receiver ID1 may also try to DE capsulate and obtain K1. [1] It is observed that:

1. It is usually the case that K and K1 are independent of each other from the view of the receivers.
2. In some IBKEM the sender may also know K1 obtained by receiver ID1.

This can be referred to the former property as collision-freeness and to the latter as full-identity malleability. An IBKEM scheme contains some properties, depending on this property it is said to be collision-free full-identity malleable if it possesses both properties. If both underlying IBKEM and IBE have semantic security and the privacy of receiver's identities, the SPCHS is

semantically secure containing this properties. Collision-free full-identity malleable IBKEM [1]:
1. K and ID = Sender encapsulate key K to an intended receiver ID, of course receiver ID can be DE capsulated to obtain K.
2. K1 and ID1= Non-intended receiver ID1 will also try to DE capsulate to obtain K1.

Two cases are observed:
1. Collision-free - It is case that K and K1 are independent of each other from receiver view.
2. Full-identity malleability -In some IBKEM, the sender may also know K1 obtained by receiver ID1.

Semantic security to SPCHS, includes the probabilistic polynomial time (PPT) Adversary that is allowed to know all structure public parts, query the private part of chosen structure, Query the trapdoor for keywords and query cipher texts of keywords.SS-CKSA is Semantic Security of SPCHS to Chosen Keyword and Structure Attack [10]; the adversary will choose two challenge keyword-structure pairs. This SS-CKSA security means that for cipher texts of one of two challenge keyword structure pair.

V. SPCHS Construction

The SPCHS definition consists of five algorithms[1].
Step 1: System Setup{W, 1k}, the system inputs keyword space W and security parameter 1k.Run the pair of master keys (PK, SK) = Setup (1k,ID). It outputs the pair of master public and secret key {PK, SK}where, PK contains keyword W cipher texts C.
Step 2: Structure Initialization{PK}, the system inputs the public key and generates the encapsulated key. Initialize the hidden structure. It outputs the hidden relation {Pri, Pub} and initializing a hidden structure.
Step 3: Structured Encryption{PK,W,Pri}, inputs the PK,W,Pri. Search for the keyword in Pri and output the cipher text with keyword W and update Pri. Where, Pri is hidden relation in C.
Step 4: Trapdoor {SK, W}, inputs the secret key and keyword W and gives keyword search trapdoor Tw of W
Step 5: Structure Search{PK,Pub,C,Tw}, inputs the public key, Pub, C, Tw. And discloses partial relation to find out cipher texts containing keywords W with hidden structure

The generic SPCHS is constructed based on the properties observed in the IBKEM.

VI. Experimental Results

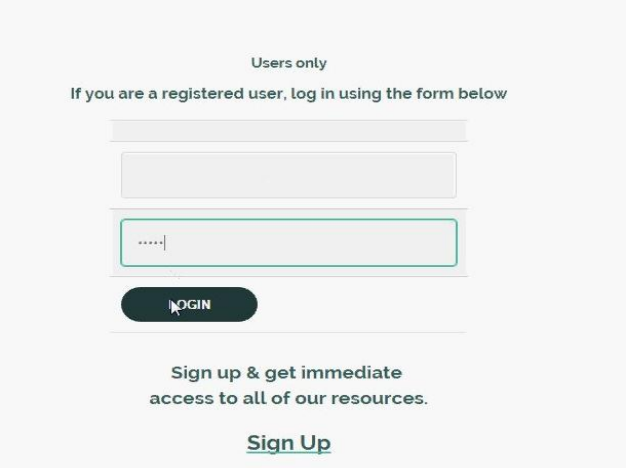

Fig:-1 User Authentication

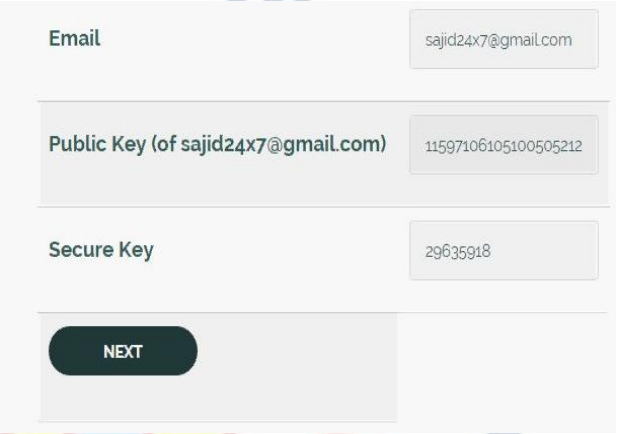

Fig:-2Key Generation

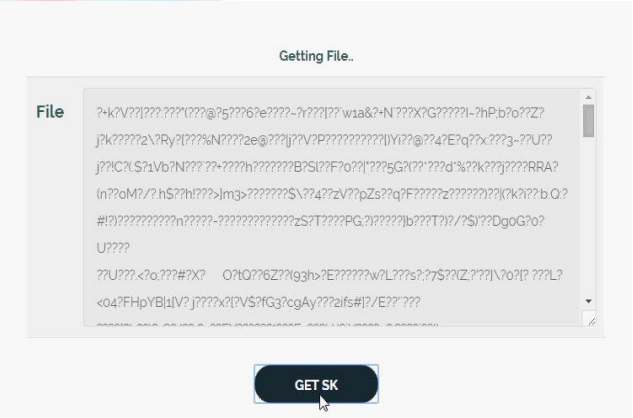

Fig:-3Encrypted File Data

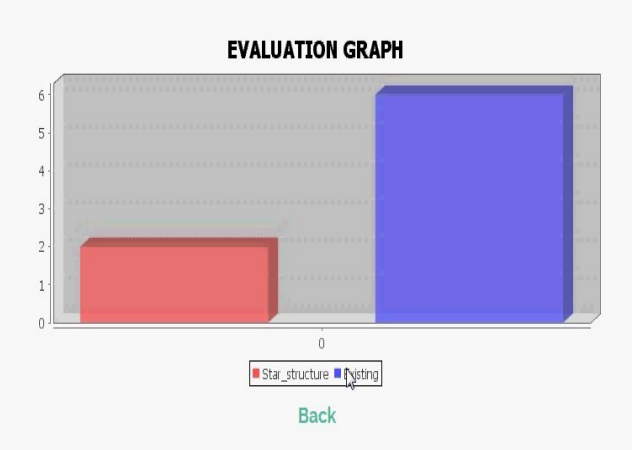

Fig:-4Evaluation Graph

VII. Conclusion

This article presented SPCHS Methodology for Expeditious Keyword Search as a variant of PEKS without sacrificing the semantic security for expeditious keyword search. This incipient concept sanctions the generation of keyword searchable cipher texts with the avail of obnubilated structure. The search algorithm of SPCHS discloses part of this obnubilated structure for guidance on ascertaining the cipher texts of the queried keyword given a keyword search trapdoor. Semantic security of SPCHS captures the privacy of the keywords as well as the invisibility of the obnubilated structure. It has search intricacy mainly linear with the genuine number of the cipher texts rather than the total number of cipher texts containing the queried keyword, thereby outperforming subsisting PEKS schemes. SPCHS seems to be a promising implement for solving some challengeable quandaries in public-key searchable encryption. One application may be to achieve retrieval plenariness verification by the formation of an obnubilated star like structure, which has not yet achieved in the subsisting PEKS schemes. Another application may be to filter the encrypted spams.

References

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology— EUROCRYPT (Lecture Notes in Computer Science), vol. 3027, C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer-Verlag, 2004, pp. 506–522.

[2] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 4622, A. Menezes, Ed. Berlin, Germany: Springer-Verlag, 2007, pp. 535–552.

[3] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in Advances in Cryptology— EUROCRYPT (Lecture Notes in Computer Science), vol. 3027, C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer-Verlag, 2004, pp. 223–238.

[4] X. Boyen and B. Waters, "Anonymous hierarchical identity based encryption (without random oracles)," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 4117, C. Dwork, Ed. Berlin, Germany: Springer-Verlag, 2006, pp. 290–307.

[5] C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 4004, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag,2006, pp. 445–464.

[6] G. Ateniese and P. Gasti, "Universally anonymous IBE based on the quadratic residuosity assumption," in Topics in Cryptology—CT-RSA (Lecture Notes in Computer Science), vol. 5473, M. Fischlin, Ed. Berlin, Germany: Springer-Verlag, 2009, pp. 32–47.

[7] L. Ducas, "Anonymity from asymmetry: New constructions for anonymous HIBE," in Topics in Cryptology—CT-RSA (Lecture Notes in Computer Science), vol. 5985, J. Pieprzyk, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 148–164.

[8] M. Abdalla, D. Catalano, and D. Fiore, "Verifiable random functions: Relations to identity-based key encapsulation and new constructions," J. Cryptol., vol. 27, no. 3, pp. 544–593, Jul. 2013.

[9] E. S. V. Freire, D. Hofheinz, K. G. Paterson, and C. Striecks, "Programmable Hash functions in the multi linear setting," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 8042, R. Canetti and J. A. Garay, Eds. Berlin, Germany: Springer-Verlag, 2013, pp. 513–530.

[10] S. Garg, C. Gentry, and S. Halevi, "Candidate multi linear maps from ideal lattices," in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 7881, T. Johansson and P. Q. Nguyen, Eds. Berlin, Germany: Springer-Verlag, 2013, pp. 1–17.