ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

A Fast and Secure Scheme for Search over Encrypted Data

Malihabi V P[1], Kiran V K[2]

PG Student, Dept. of CSE, NSSCE, Palakkad, India [1]

Assistant Professor, Dept. of CSE, NSSCE, Palakkad, India [2]

Abstract: Searchable encryption provides encryption and search at the same time. The current semantically secure searchable schemes provide search time linear with the total number of ciphertexts. This makes it less acceptable for large databases. Hence new techniques are adopted providing some hidden relations among the ciphertexts to improve the search efficiency. The search trapdoor finds out the first matching keyword and through hidden relations all the related ones could be found out. The search complexity now depends on the number of ciphertexts containing the queried keyword than on the total number of ciphertexts**.**

Keywords: public key-searchable encryption, Identity Based Encryption, Identity Based Key Encapsulation mechanism, Semantic security.

I. INTRODUCTION

Search on encrypted data has become an important problem in many fields of computer science like in security, cryptography, databases and privacy. This is due to the following factors. We are outsourcing more and more confidential data to the less trusted third parties for storage. This sensitive data needs to be encrypted before outsourcing. Existing methods like keyword based information retrieval on plain texts cannot be applied as such on the encrypted data. And some techniques need to be adopted for searching over the encrypted data.

In public key encryption with keyword search (PEKS), proposed by Boneh et al. in [1],anyone who knows the public key of a receiver can upload encrypted files with searchabe feature (using keywords)to a server. The server can search for files as per the request of the receiver using a trapdoor corresponding to a keyword and sends the files containing the queried keyword to him. The server is not able to learn the queried content in this. The receiver can decrypt the data using his private key which is only known to him.The authors of PEKS also proposed semantic security against chosen keyword attacks(SS-CKA). The adversary can generate ciphertexts of keywords and if having a keyword search trapdoor the adversary can exhaustively test for a match. This is chosen keyword attack (KGA) and particularly challenging when the keyword space is of no high min entropy.

Bellare et al.proposed deterministic encryption [2], which aimed at making search over encrypted data as efficient as on plaintext data.An encryption scheme is deterministic if the encryption algorithm is deterministic. But it has some limitations.It leaks some information via the ciphertexts of keywords since the encryption algorithm is deterministic.Also it can be applied only in cases of high min entropy keyword space.

II. RELATED WORK

The earlier work on searchable encryption can be divided into two: symmetric searchable encryption(SEKS) and public key searchable encryption(PEKS). Song et al. proposed the first practical symmetric searchable scheme [3].In this, word by word encryption is done for a file.The search time is linear with the document size.The first public key searchable encryption scheme was proposed by Boneh et al.[1]

Many efforts were done devoting to either provable security or better search performance. SEKS is extended to multisender scenarios, in some works realized fuzzy keyword search, further proposed dynamic searchable schemes. Symmetric schemes make use of symmetric primitives like block ciphers and pseudo random functions.

Asymmetric schemes have undergone many efforts to make it versatile.Conjuctive search, range search,subset search,similarity search, authorized search, fuzzy keyword search are the various types.In these,the search complexity is linear with the number of all ciphertexts.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Deterministic and efficiently searchable encryption [2] proposed by Bellare et al. provides accelerated search using a deterministic algorithm in public key settings and provides as strong as possible security.The encrypted keywords can form a tree like structure when stored according to their binary values. Search time is logarithmic in the total number of ciphertexts. But deterministic encryption can be used in special scenarios only where keywords are hard to guess by the adversary.

III.MOTIVATION

Searchable encryption is a relevant thing and so many researches are still going on it.This is because time and security are big concerns in many scenarios.The search over ciphertexts can be improved together with having semantic security if one can arrange the ciphertexts with some unseen relations in between.The linear search complexity of the existing schemes make it difficult to accept them.The star like arrangement among the ciphertexts has search time linear with the number of ciphertexts containing the queried keyword.

IV.PROBLEM DEFINITION & PRELIMINARIES

The existing semantically secure systems take search time linear with the total number of ciphertexts. Eventhough deterministic encryptions provides improved search time,it can be employed in special cases.So when we consider large databases, a faster search scheme is needed at the same time providing semantic security.The scheme make use of several interesting features of identity based encryption[4].

Identity Based Encryption(IBE):ID-based encryption,first proposed by Shamir, takes the identity of the receiver to generate the public key. The private key generator generates the private key according to the ID .IBE reduces the cost of certificate management through binding participant ID and public key. It was proposed to simplify key management.
Identity Based Key Encapsultion mechanism (IBKEM): Instead of providing the full functionality of an IBE, sometimes what only needed is to allow sender and receiver to agree on a common random session key.This is accomplished by an IBKEM.
Bilinear map: Used with IBE, a tool for pairing based cryptography. A bilinear map from G1 × G2 to Gt is a function $e : G_1 \times G_2 \rightarrow Gt$ such that for all $u \in G1$, $v \in G2$, a, $b \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$ .Thus they associate pairs of elements from G_1 and G_2 to an element in G_t.

V. PROPOSED IDEA

In the proposed system giving importance to security as well as efficiency. Bulid SPCHS, as explained in [6], searchable public key ciphertexts with hidden structures as a solution to the existing system which can provide improved search together with semantic security. As shown in fig 1, all ciphertexts of the same keyword form a chain and with a keyword search trapdoor and the public head of the hidden star like structure,the server can find out the first matching ciphertext. From this, through some hidden relations all matching ciphertexts could be found out.
By forming a tree like structure among the ciphertexts, it is possible to have content search of encrypted data.For this the sequentially encrypted words of a file are stored in a tree like structure.

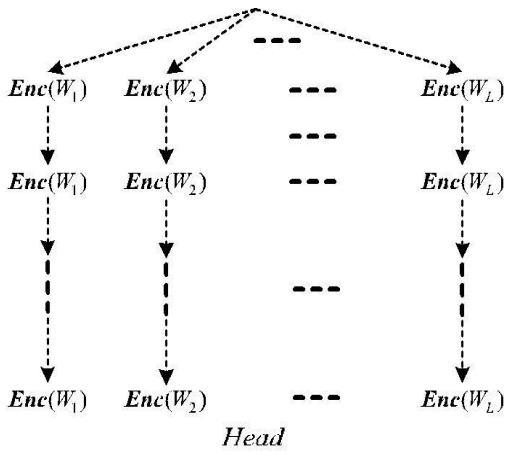

Fig. 1 Hidden structure in SPCHS

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

SPCHS consists of the following algorithms:

SystemSetup(1^k , W): This generates a public key- secret key pair (**PK**, **SK**).The inputs are a security parameter 1^k and a keyword space W, the key pair is produced probabilistically. **PK** includes the keyword space W and the ciphertext space C.
StructureInitialization(**PK**): By taking PK as input,A hidden structure is initialized with private and public parts (**Pri**, **Pub**) probabilistically.
StructuredEncryption(**PK**, w, **Pri**):It takes inputs **PK**, a keyword w from W and a the hidden structure private part **Pri** ..Pprobabilistically output the keyword-searchable ciphertext C for the input keyword .C is generated with the hidden structure.The private part Pri is updated.
Trapdoor(**SK**, W):It takes as inputs **SK** and a keyword W ∈ W.Output a keyword search trapdoor T_W of W .
StructuredSearch(**PK**, **Pub**, C, T_W): It takes **PK**, a hidden structure's public part **Pub**, all keyword searchable ciphertexts C and a keyword search trapdoor T_W of keyword W , as input ,reveals partial relations to help finding out the ciphertexts containing keyword W with the hidden structure.

The generic construction of SPCHS makes use of the concepts of IBE and several interesting features of collision free full identity malleable IBKEM.The definition of IBKEM is taken from [5].When both the IBE and IBKEM have semantic security and anonymity (identity privacy),the resulting SPCHS is semantically secure.If the IBKEM is anonymous,it preserves the anonymity of receivers.In collision free and full identity malleable IBKEM,if a sender sends an encapsulated key to an intended receiver ,clearly it decapsulates and obtain the key.But a non-intended receiver also try to decapsulate and obtain a different key by the collision freeness.By full identity malleable property , the sender even knows the different keys obtained by the receivers.

VI. COMPARISON & EXPECTED RESULT

When compare to deterministic encryption, SPCHS can provide more security even in cases of keyword space of no high min entropy.Hence it is suited for a general case and outperforms the PEKS schemes available so far. The semantic security is defined for ciphertexts and the hidden structure.

VII. CONCLUSION & FUTURE WORK

SPCHS outperforms the existing schemes of PEKS by providing as fast as possible search with semantic security..SPCHS forms a basis for solving challenging problems in public key searchable encryption. By setting the last pointer always pointing to the head of the hidden structure, it is possible to verify the retrieval completeness. SPCHS provides privacy to the keywords and invisibility to the hidden structure.
The future work includes the implementation of content search by forming a hidden tree like structure using the SPCHS concepts.This type of content search can be used to filter the encrypted spams.

ACKNOWLEDGMENT

First and foremost I thank the almighty god for helping me to fulfil this work. I also extend my sincere thanks from the depth of my heart to my guide Mr Kiran V K, Assistant Professor, Department of Computer Science, NSSCE Palakkad for enlightening me through his valuable guidance, help and suggestions. I would also like to extend my gratitude to all my friends, dears and nears for helping me to make this work a success.

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. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE S&P, May 2000, pp. 44–55.
[4] 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.
[5] M. Izabachène and D. Pointcheval, "New anonymity notions for identity-based encryption," in Security and Cryptography for Networks (Lecture Notes in Computer Science), vol. 5229, R. Ostrovsky, R. D. Prisco, and I. Visconti, Eds. Berlin, Germany: Springer-Verlag, 2008, pp. 375–391.
[6] Peng Xu,Qianhong Wu,"Generating Searchable public key ciphertexts with hidden structures for fast keyword search",IEEE,2015