KEYWORD BASED SEARCH USING PUBLIC KEY CIPHER TEXT

K. Jayasree[1], K. Madhu Sudhan Reddy[2]
[1]*Dept of MCA, SKIIMS, Kapugunneri, Affiliated to S.V.University, Tirupati*
[2]*Associative Professor, Dept of MCA, SKIIMS, Kapugunneri, Affiliated to S.V.University, Tirupati*

***Abstract*- Searchable Public-Key Ciphertexts with Hidden Structures for keyword search is as fast as possible without sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable ciphertexts 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 ciphertexts efficiently. Construct a SPCHS scheme from scratch in which the ciphertexts have a hidden star-like structure. The scheme is to be semantically secure in the Random Oracle model. The search complexity of is dependent on the actual number of the ciphertexts containing the queried keyword, rather than the number of all ciphertexts. SPCHS construct from anonymous identity-based encryption and collision-free full-identity malleable Identity-Based Key Encapsulation Mechanism with anonymity. Two collision-free full-identity malleable IBKEM instances are semantically secure and anonymous, respectively, in the RO and standard models. The latter instance enables us to construct an SPCHS scheme with semantic security in the standard model.**

***Index Terms*- Public–key searchable encryption, Semantic security, Identity–Based Encapsulation Mechanism (IBKEM), Identity–Based Encryption (IBE).**

I. INTRODUCTION

Keyword searchable ciphertexts with their hidden structures can be generated in the public key setting with a keyword search trapdoor, partial relations can be disclosed to guide the discovery of all matching ciphertexts. Semantic security is defined for both the keywords and the hidden structures. Worth noting that this new concept and its semantic security are suitable for keyword-searchable ciphertexts with any kind of hidden structures. In contrast, the concept of traditional PEKS does not contain any hidden structure among the PEKS ciphertexts. Correspondingly, its semantic security is only defined for the keywords. Following the SPCHS definition, construct a simple SPCHS from scratch in the random oracle model. The scheme generates keyword- searchable ciphertexts with a hidden star-like structure. The search performance mainly depends on the actual number of the ciphertexts containing the queried keyword. For security, the scheme is proven semantically secure based on the Decisional Bilinear Diffie Hellman (DBDH) assumption in the RO model.

II. EXISTING AND PROPOSED SYSTEM

A. Existing System:

Existing semantically secure PEKS schemes take search time linear with the total number of all cipher texts. This makes retrieval from large-scale databases prohibitive. Therefore, more efficient search performance is crucial for practically deploying PEKS schemes. One of the prominent works to accelerate the search over encrypted keywords in the public- key setting enabling search over encrypted keywords to be as efficient as the search for unencrypted keywords, such that a cipher text containing a given keyword can be retrieved in time

This is reasonable because the encrypted keywords can form a tree-like structure when stored according to their binary values. However, deterministic encryption has two inherent limitations. First, keyword privacy can be guaranteed only for keywords that are a priori hard to-guess by the adversary. Second, certain information of a message leaks inevitably via the ciphertext of the keywords since the encryption is deterministic. Hence, deterministic encryption is only applicable in special scenarios.

Disadvantages of Existing System:

Each sender should be able to generate the keyword- searchable cipher texts with the hidden star-like structure by the receiver's public-key, the server having a keyword search trapdoor should

be able to disclose partial relations, which is related to all matching cipher texts. Semantic security is preserved, if no keyword search trapdoor is known, all cipher texts are indistinguishable, and no information is leaked about the structure, and given a keyword search trapdoor, only the corresponding relations can be disclosed, and the matching cipher texts leak no information about the rest of cipher texts, except the fact that the rest do not contain the queried keyword.

The integrity of data is not possible in existing system

An existing system public verifier does not check the data in multi cloud.

B. Proposed System:

In proposed scheme, keyword searchable cipher texts with their hidden structures can be generated in the public key setting with a keyword search trapdoor, partial relations can be disclosed to guide the discovery of all matching cipher texts. Semantic security is defined for both the keywords and the hidden structures. Construct a simple SPCHS from scratch in the random oracle model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. The search performance mainly depends on the actual number of the ciphertexts containing the queried keyword.

A generic SPCHS construction is to generate keyword- searchable cipher texts with a hidden star-like structure. Generic SPCHS is inspired by several interesting observations on Identity-Based Key Encapsulation Mechanism (IBKEM). Build a generic SPCHS construction with Identity Based Encryption (IBE) and collision-free full- identity malleable IBKEM. The resulting SPCHS can generate keyword-searchable cipher texts with a hidden star-like structure. Moreover, if both the underlying IBKEM and IBE have semantic security and anonymity, the resulting SPCHS is semantically secure. As there are known IBE schemes in both the RO model and the standard model, an SPCHS construction is reduced to collision-free full-identity malleable IBKEM.

Advantages of Proposed System:

IBKEM schemes to construct Verifiable Random Functions. One of these IBKEM schemes is anonymous and collision- free full identity malleable in the RO model utilized the approximation of multilinear maps to construct a standard- model version of Boneh-and-Franklin IBE scheme. Transform this IBE scheme into a collision-free full-identity malleable IBKEM scheme with semantic security and anonymity in the standard model. Hence, this new IBKEM scheme allows us to build SPCHS schemes secure in the standard model with the same search performance as the previous SPCHS construction from scratch in the RO model. Each client has a private correspond to his identity such as name, id or any. The public verifier allow the user to correspond to his identity such as private Key.

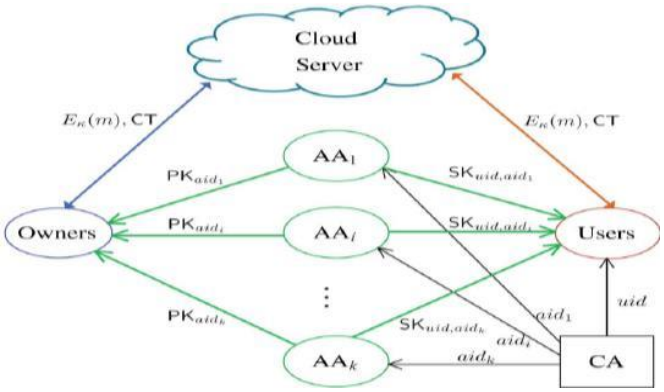


Fig: 1 System Architecture

III. MODULES

- **Data provider**

In this module, the data provider uploads their data in the Data server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file. The data owner establishes the public system parameter via Setup and generates a aggregate key/master-secret key pair.

- **Data Server**

The **Data** server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests multiple files at the same time to access.

- **END User**

In this module, the user can only access the data file with the encrypted key. Files it can be Text File. The user can access the multiple files from Server via Key Aggregate Server using Aggregate Key. So malicious users may collude with each other to get sensitive files by using un authorized key.

- **Verifier**

In this module, the verifies authorizes an end users and also maintains the log about end users search and data owner files data.

IV. I B K E M ALGORITHM

Formalize collision-free full-identity malleable IBKEM and a generic SPCHS construction from IBKEM. Our generic construction also relies on a notion of collision-free full- identity malleable IBKEM. Take the random value as an input of the algorithm.

IBKEM Consists of Four Algorithms:

1. Setup $_{IBKEM}$ (1^k, ID_{IBKEM})

Take as inputs a security parameter 1^k and an identity space
ID_{IBKEM} , and probabilistically output the master public-and- secret-keys pair(PK_{IBKEM} , SK_{IBKEM}) , where PK_{IBKEM} includes the identity space ID_{IBKEM}, the encapsulated key space K_{IBKEM} and the encapsulation space C_{IBKEM}.

2. Extract$_{IBKEM}$ (SK_{IBKEM}, ID)

Take as inputs SK_{IBKEM} and an identity ID € ID_{IBKEM}, and
output a decryption key $\hat{S}_{ID}$ of ID.

3. Encaps$_{IBKEM}$ (PK_{IBKEM}, ID, r)

Take as inputs PK_{IBKEM}, an identity ID € ID_{IBKEM} and a random value r, and deterministically output a key-and-encapsulation pair
($\hat{Y}$, $\hat{C}$) of ID.

4. Decaps$_{IBKEM}$ ($\hat{S}_{ID}$, $\hat{C}$)

Take as inputs the decryption key $\hat{S}_{ID^1}$ of identity ID^1 and an
encapsulation $\hat{C}$, and output an encapsulated key or _ , if the encapsulation is invalid.

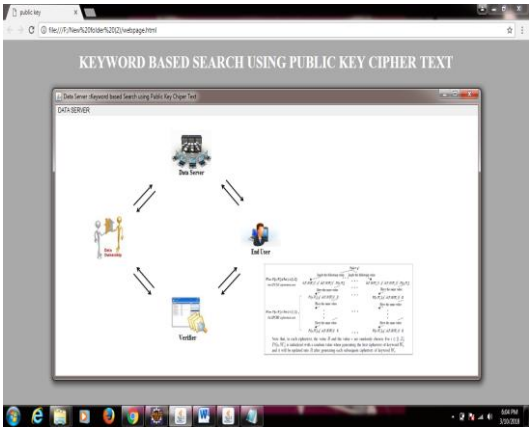
An IBKEM scheme must be consistent in the sense that for any
($\hat{Y}$, $\hat{C}$) = Encaps$_{IBKEM}$ (PK_{IBKEM}, ID, r) , Decaps$_{IBKEM}$ ($\hat{S}_{ID}$, $\hat{C}$) = $\hat{Y}$
holds if ID^1 = ID, except with a negligible probability in the
security parameter k.

The collision-free full-identity malleable IBKEM implies the following characteristics. They are all identities decryption keys can encapsulate the same encapsulation, all encapsulated keys are collision-free, the generator of the encapsulation can also compute these encapsulated keys, the encapsulated keys of different encapsulations are also collision-free.

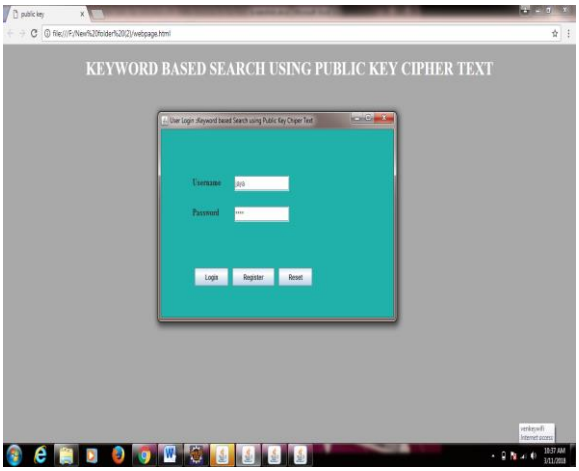
IBKEM is collision-free full-identity malleable, if there is an
efficient function FIM that for any ($\hat{Y}$, $\hat{C}$) = Encaps$_{IBKEM}$

V. SCREEN SHOTS:

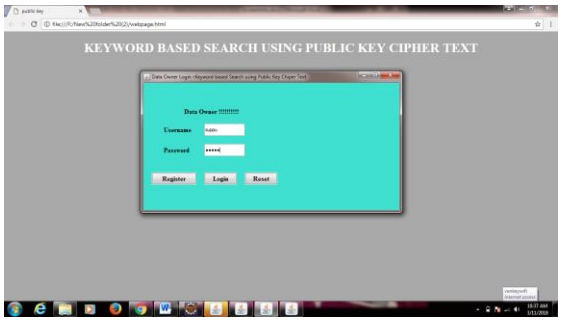
HOME PAGE:



USER LOGIN:



OWNER LOGIN:



VI. CONCLUSION

This project investigated as-fast-as-possible search in PEKS with semantic security. The concept of SPCHS as a variant of PEKS. New concept allows keyword-searchable ciphertexts to be generated with a hidden structure. Given a keyword search trapdoor, the search algorithm of SPCHS can disclose part of this hidden structure for guidance on finding out the ciphertexts of the queried keyword. Semantic security of SPCHS captures the privacy of the keywords and the invisibility of the hidden structures. An SPCHS scheme from scratch with semantic security in the RO model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. It has search complexity mainly linear with the exact number of the ciphertexts containing the queried keyword. It outperforms existing PEKS schemes with semantic security, whose search complexity is linear with the number of all ciphertexts. Collision-freeness and full-identity malleability in some IBKEM instances, and formalized these properties to build a generic SPCHS construction. Two collision-free full-identity malleable IBKEM instances, which are respectively secure in the RO and standard models. SPCHS seems a promising tool to solve some challenging problems in public-key searchable encryption.

REFERENCES

[1] Arriaga A.et al. (2014): Trapdoor Privacy In Asymmetric Searchable Encryption, In: AFRICACRYPT 2014. LNCS, vol. 8469, pp. 31-50.

[2] Ateniese G., Gasti P. (2009): Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In: Fischlin M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32-47.

[3] Bellare M.et al. (2007): Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535-552.

[4] Boneh D.et al. (2004): Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J.(eds.) EUROCRYPT 2004.LNCS, vol.3027, pp.506-522.

[5] Boneh D.et al. (2004): Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol.3027, pp. 223-238.

AUTHOR PROFILE:

AUTHOR 1:

K. Jayasree received Graduate Degree B.Sc Computer Science from Sri Venkateswara University, Tirupati in the year of 2012-2015. Pursuing Master of Computer Applications from Srikalahastiswara Institute of Information and Management Sciences, Srikalahasti, Afiliated to Sri Venkateswara University, Tirupati in the year of 2015-2018.

AUTHOR 2:

K. Madhu Sudhan Reddy working as an associative professor in Dept. of Computer Science, Srikalahastiswara Institute of Information and Management Sciences, Srikalahasti (AP) India. Received Master of Computer Applications from Sri Venakteswara University, Tirupati.