International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 6
ISSN: 2454-4248
29 – 32

Fast Keyword Search With Encryption

Ashwini Rajendra Kachare
M.E. Student
Department of Computer Science and Engineering
P.E.S.College of Engineering,
Aurangabad, India
kachare014@gmail.com

Prof. Manisha M. Ambekar
Associate Professor
Department of Computer Science and Engineering
P.E.S.College of Engineering,
Aurangabad, India
mmambekar@pescoe.ac.in

***Abstract*—** Paillier' Method is used in research and cloud protected outsourcing as well as privacy-preserving computation. In this paper we implement Pallier Method for providing security. Fast Keyword Search Perform on encrypted Data not directly on plain text, hence Security is given to database. In Multi-writer scenario Data sources upload Data on Different Resources .Data owner is responsible for generating tokens and encrypt data. Data owner and query source perform queries through a query processor. Data originated by data sources in which personal data and public data include, personal data search only authorized personal and public data search anyone who create their data source registration successfully. Cipher text length is created in between 16 digits to 256 digits, if data source search similar data on multiple time then every time query is encrypted using different numbers. Data in database stored using number of attribute. We focused on security in Pallier method .

Keywords- *Fast Keyword Search with Hidden Structure (FKCHS) Public key searchable encryption, Semantic security, Identity Based Encapsulation Mechanism (IBKEM), Identity Based Encryption (IBE),Data Owner(DO),Query Processor(QP),Data Source(DS),Hidden Vector Encryption(HVE),Master Public Key(MPK),Master Secrete Key(MSK), M-Token (MPK),P-Token(PTK),Identity Based Encryption(IBE), Secret Key (SK).*

*****

I. INTRODUCTION

Paillier anticipated a new encryption scheme include key generation, Tokens Generated such as Predicate token and Message token. In the Pallier Method using big integer encrypt data to encrypt a significance m € $Z_{n,}$ this property captures the idea according to which an third party should not able to learn any information whatever about a actual text, its length between 16 digit to 256 digit, given its encryption. Paillier's scheme is semantically secure.

In particular, a secluded search scheme aims to make sure that the server learns nothing concerning the data stored in the secluded folder or concerning the queries and the queried learns nothing further than the query consequences. These security goals can be official by means of the authentic perfect style of cryptographic description. The data owner manages access rights to the data originating from several data sources and collected in encrypted form on a possibly un trusted server. The query processor has direct physical access to the encrypted statistics as well as performs the queries on behalf of the query sources. we consider a threat model in which the data owner is the only fully trusted party. the data sources are trusted to upload significant data but they should not be able to read the data uploaded by other data sources. The query processor is honest-but-curious and it is expected to execute the prescribed code. the query sources be supposed to be able to learn only the cells they have been authorized to read by the data owner. This requirement extends to coalitions of query sources: a coalition can only learn the union of the cells they are authorized to read and no extra cell.

Of course, with the help of the query processor, they could learn, for example, which rows were selected by both queries they have been authorized to issue but, still, no extra cell from the table is revealed. We also protect the query sources from the query processor by not letting the query processor read the result of the queries issued by the query sources and we want the query processor not to learn the accurate number of selected rows. In other words the query processor and data source only learn data-access and query patterns and no explicit data, except the authorized cells, is disclosed.

A. *Multi-writer scenario*

Data owner, multiple data sources, multiple query sources, and one query processor included in this scenario. The data owner is admin and has all the rights. The query processor has directly connected to the encrypted data. The data owner is the only fully trusted party. The data sources are trusted party to upload data but they be supposed to not read the data uploaded by further data sources. The query processor is nothing but honest-but-curious. The query sources should be Select their access rights at the time of registration read, write or read write upload. Query processor and data source only learn data-access and query patterns and no explicit data, except the authorized cells, is disclosed. The data sources can encrypt data. In other words the capability to write (to encrypt) data is decoupled from the ability to query (to decrypt) data thus making our scenario innately a public-key one. I come across at the case in which data is visibly agreed in a table of rows with same number of cells.

B. *Approach*

The recent advances in Functional Encryption [1] provide a straightforward secure implementation of our scenario. More precisely, the data owner (DO) publishes the public key of a Functional Encryption scheme to be used by the data Sources (DS) to encrypt the rows. The data owner (DO) uses the

 ISSN: 2454-4248
29 – 32

associated secret key to compute the token needed to perform the query the Specific QS is authorized to perform. The query processor (QP) then plainly applies the token to the encrypted data and precedes the result. This advance has the advantage of sustaining any query that can be expressed by a small (polynomial) circuit [2], [3], [4] (and, actually, even more [5]). Unfortunately, these are to be seen more as feasibility results and unlikely to be, at this stage, of direct use in a practical system. Even for the set of queries of our attention, the state of the art in public-key practical encryption does not tender an adequate solution. Hidden Vector Encryption (HVE, see [8], [6], [7]) seems to flawlessly suit our setting. Roughly speaking, HVE allows to encrypt plaintext M with respect to attribute vector X =(X1,...,Xn) with components taken from an attribute space X. The landlord of the master secret key can generate tokens associated with vectors Y =(Y1,...,Yn) in which each component is either a "don't care symbol" or an element of X. A token associated with Y can be used to decrypt all cipher texts whose attribute vector X coincides with Y in all components that are not. HVE can be used to implement our scenario in a straightforward way: the DS encrypts each cell of the table by using the values in the other columns of the same row as attributes and the value in the cell itself as plaintext. Then, as it easily seen, every query that we wish to support directly maps to a vector Y and thus a QS requests the appropriate token to the DO. The QP is appropriate the token to each encrypted cell and returns the ones that are decrypted correctly. The simple implementation described above is not practical, though. First of all, the secret key of all the known implementations of HVE need O(n·log|X|) group elements each of size proportional to the security parameter. More importantly, the cipher text of one cell has length proportional to n · log|X| where n is the number of columns in a row. This implies that a row with n columns, once encrypted, will have length Ω(n2), clearly impractical. This second problem seems inherent since, obviously, a cipher text must be at least as long as its attributes. Our main technical contribution is based on the observation that cells of the same row are encrypted using the same attributes and thus we could hope to have an amortized encryption scheme that can be used to reduce the cumulative length of the cipher texts of the cells of a row.

II. LITERATURE SURVEY

A. *Strong Search Pattern Privacy for PEKS*

Arriaga.A, et al. [9] proposes the idea of brawny Search Pattern Privacy for PEKS and constructs a format that achieves this safety concept. He provides a broader view on trapdoor privacy in asymmetric searchable encryption, and bridge the space between presently existent definitions. He shows that two separate scenarios to replica trapdoor solitude one in the attendance of cipher texts that match trapdoors, and the other in the absence of such cipher texts. The idea of brawny Search prototype Privacy addresses solitude concerns up to the point where cipher texts similar the issued trapdoors become available, after which, search patterns can no longer be unseen from an attacker.

B. *Public Key Encryption with Keyword Search.*

Boneh.D, et al. [10] proposes searching on information that is encrypted using a public key scheme. He consider user nod who sends email to user Alice encrypted under Alice's public key. An email access wants to check whether the email contains the keyword vital so that it could way the email consequently. Alice, on the other hand does not wish to give the access the capability to decrypt all her post. Boneh.D explain and put up a mechanism that enables Alice to offer a key to the entrance that enables the entry to check whether the word vital is a keyword in the email without erudition anything else about the email. Boneh.D submits to this technique as public key encryption with keyword Search. The limitation of PEKS is to eliminate protected channel and encrypt various keywords. a new problem is to refresh frequently-used keywords. Enable search encrypted keywords lacking cooperation the safety of the unique data.

C. Deterministic and Efficiently Searchable Encryption

Bellare.M, et al. [11] obtainable as-strong-as-possible explanation of privacy, and building attain them, for public-key encryption schemes where the encryption algorithm is deterministic. conclude as a result database encryption procedure that allow speedy search while provably provided that privacy that is as strong as possible topic to this fast search constraint. Collect substance easier this to get a thought of efficiently-searchable encryption schemes which allow more flexible privacy to search-time trade-offs by a technique called bucket tization. Restriction of this paper is only given that privacy for plaintexts that have high min entropy.

D. *usually indefinite IBE Based on the Quadratic Residuosity declaration*

Ateniese.G, et al. [12] introduce the first universally anonymous, thus key-private, IBE safety is based on the standard quadratic residuosity statement. The main feature characterizing universal anonymity is the capacity to divide the role of the sender of encrypted messages from the role of the anonymzer. An encryption scheme is universally secret if cipher texts can be made unidentified by anyone and not just by whoever formed the cipher texts. particularly, a universally anonymizable public key encryption scheme consists of a typical public-key encryption scheme and two additional algorithms one is used to anonymize cipher texts, which takes as input only the public key of the receiver, and the other is used by the receiver to decrypt anonym zed cipher texts. It is more luxurious and still depending on pairing-based assumptions.

E. *Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles.*

Boneh.D, et al. [13] collect two accomplished peculiarity base Encryption system that has restricted characteristics secure without the random oracle form in groups set with a bilinear map. Selective identity protected IBE is a slightly weaker safety model than the standard protection model for IBE. First

 ISSN: 2454-4248
29 – 32

plot is based on the decisional bilinear DiffieHellman theory, and extend to give a discerning identity Hierarchical IBE secure without random oracles. Second system is based on a connected assumption called the bilinear Diffie-Hellman inversion assumption. Observe that a selective-ID secure IBE system implies a completely safe IBE system but the resultant security reduction is not polynomial. The system is quite impractical and should only be viewed beneficial evidence that such constructions are indeed possible. The question of constructing a completely secure IBE system with a tight reduction in the standard model remains open.

III. EXISTING SYSTEM

A.Amortized Orthogonality Encryption

In an Orthogonality Encryption system [14], a cipher text ct computed with admiration to a master public key MPK is associated with a plaintext M and an characteristic vector X. The carrier of the master covert key MSK joined with MPK can generate, for any feature vector *S*, two dissimilar tokens: a P-token PTOK S and an M-token MTOKS. If we try to decrypt ct by using PTOK S, study whether X and *S* are orthogonal and nothing else. On the other hand, if we try to decrypt ct by using MTOK S, obtain the plaintext M if X and S are orthogonal; otherwise, we get no information about X and M. Roughly speaking, an Amortized Orthogonality Encryption system (an AOE scheme, in short) allow for efficient encryption of several plaintexts with admiration to quality vectors that diverge in few components producing a very compact cumulative cipher text (whence, Amortized). More precisely, we have the following syntax for an AOE scheme.
The master secret key consists of one couple (MPK0, MSK0) of master public and covert key for the attribute vector of length l and n pairs, (MPK1, MSK1),…… , (MPKn, MSKn),one for each quality vector of length k. Message Mi, for i = 1, . . . , n, is then encrypted with the master public key obtained by concatenating MPK 0 and MPK i. However, to keep away from having to recompute the encryption of the first l attributes, the same arbitrariness is used for all cipher texts thus provision with the need of repeating the cipher text part matching to the first l common attributes. In general, the use of related randomness for different cipher texts completely breaks the security of an encryption scheme show that for our specific construction this does not happen mainly due to the fact that independent master secret keys have enough entropy.

C Disadvantages of Existing System

1) Cipher text Length was Equal to Input Length.
2) Query Processor was Directly Connected to Actual Plain Text.
3) Data Encrypted using Private Key and Decryption with the help of Private Key.
4) Maximum Time was required for Key Generation, Encryption, M Token, P Token.

IV PROPOSED SYSTEM

A.Pallier Cryptosystem

Pallier Cryptosystem is asymmetric algorithm for public key cryptography. The difficulty of computing n-th remainder constituent is academic to be computationally hard. The decisional combined residuosity supposition is the intractability proposition upon which this cryptosystem is based.

Paillier's encryption possesses the following properties:
1) It's a public key system, which means encryption can be performed by anyone who knows the public key, while decryption can only be finished by the corresponding private key, known only to a trusted party.
2) It is probabilistic. In other words it is impossible for an opponent to tell whether two cipher texts are encryptions of the same plaintext or not.

The key generation scheme can be summarized as follows:
_ Choose two large prime numbers p and q such that

Public Key=(n,g)

n= p.q, GCD(pq,(p-1)(q-1))=1

$g \in z^{*}_{n^2}$

Private Key=(λ,μ)

λ = LCM(p-1,q-1)

$\mu = \left(\frac{g^{\lambda} \bmod n^2 - 1}{n} \right)^{-1} \bmod n$

Encryption

$c = g^{m}.r^{n} \bmod n^2, r \in z_n$

Decryption

$m = \frac{c^{\lambda} \bmod n^2 - 1}{n}.\mu \bmod n$

B. Hardware and Software Requirements

1) Hardware Requirements
System: Pentium V 2.4 GHz
Hard Disk: 500 GB
RAM: 1GB
Mouse: Optical mouse

2) *Software Requirements*
Operating System: Windows 8
JAVA NETBEAN
PHP MY SQL

C Advantages of Proposed System

1) Cipher text Length is Randomly Generated.
2) Query Processor is directly connected to Encrypted Data.

 ISSN: 2454-4248
29 – 32

3) Data Encrypted by using Private key and Decrypt Using Public key.
4) Minimum time is required for Key Generation, Encryption, M Token, P Token Time is Minimum.

E Tables

EXECUTION TIME IN MS FOR PALLIER CRYPTOSYSTEAM

Pallier Cryptosystem Method	Operation			
	Encryption (ms)	Key Generation (ms)	Generate M Token(ms)	Generate P Token(ms)
Rows	150	150	150	150
Time in ms	24	0.2	0.406	0.295

CONCLUSION

In this paper more focused on security, here actual data is encrypted, length of big integer is between 16 digit to 256 digit it decides the length of encryption. If send same query at different time it will encrypt it with different number. If a user keep sending same query multiple time it will create new encrypted number every time the query received. When user send a query, every time query will be encrypted when it user search the text and in database the text has been encrypted already by fix length. User query is encrypted and the text encrypted already whose difference will be calculated and that will answer of user of query.

REFERENCES

[1] D. Boneh, A. Sahai, and B. Waters. Functional encryption: a new vision for public-key cryptography. *Commun. ACM*, 55(11):56–64

[2] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters.Candidate indistinguishability obfuscation and functional encryption for all circuits. In *FOCS 2013*, pages 40–49..

[3] P. Ananth, Z. Brakerski, G. Segev, and V. Vaikuntanathan. From selective to adaptive security in functional encryption. In *CRYPTO 2015*, volume 9216 of *LNCS*

[4] P. V. Ananth and A. Sahai. Functional encryption for Turing machines. In *TCC 2016-A*, volume 9562 of *LNCS*

[5] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC 2007*, pages 535–554.

[6] A. De Caro, V. Iovino, and G. Persiano. Fully secure hidden vector encryption. In *Pairing 2012*, volume 7708 of *LNCS*

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

[8] V. Iovino and G. Persiano. Hidden-vector encryption with groups of prime order. In *Pairing 2008*, volume 5209 of *LNCS*.
.

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

[10] 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.

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

[12] 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.

[13] 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.