International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Generating Searchable Public-Key Encrypted texts with Hidden Structures for Fast Keyword Search

Vuggam Navya [1] & Bagam Laxmaiah[2]

[1]M-Tech Dept of CSE Sarada Institute Of Technology And Science , Khammam.

[2]Associate Professor & HOD Dept of CSE Sarada Institute Of Technology And Science , Khammam

Abstract: Now days a security over internet quandary is increases day by day .Existing system get search time astronomically immense with the whole no of cipher texts. That makes recuperation from comprehensive database adamant. To ameliorate this quandary, this paper propose searchable public key cipher texts with unseen structure for keyword explore as expeditious as feasible destitute of sacrificing semantic security of the encrypted keywords. In SPCHS, every one keyword searchable cipher text are orchestrated by unseen relative, and with the search trapdoor subsequent to a keyword, the most minuscule amount in sequence of the cognations is relate to a look for algorithm as the supervision to discover all corresponding cipher text capably. We build a SPCHS conception from scrape in which the cipher text contains a concealed star like structure. We demonstrate our system to be semantically secure in the Arbitrary Oracle (RO) model. The search intricacy of the proposed scheme depended upon the authentic no of cipher text rather than the no of all cipher text. Lastly we present a generic SPCHS construction from unidentified identity predicated encryption and clash free full identity malleable identity predicated key encapsulation mechanism with anonymity.

Keywords: Searchable Public-Key, Public-key searchable encryption, semantic security, identity-predicated key encapsulation mechanism, identity predicated encryption

1. INTRODUCTION

Predicated on the PUBLIC-KEY encryption with keyword search (PEKS), introduced by Boneh et al. in, 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 homogeneous 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 ameliorated search performance and to reduce time

2. RELATED WORK

Subsisting system

One of the prominent works to expedite the search over encrypted keywords in the public-key setting is deterministic encryption introduced by Bellare et al.An encryption scheme is deterministic if the encryption algorithm is deterministic. Bellare et al. fixate on 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 involution logarithmic in the total number of all cipher texts. This is plausible because the encrypted keywords can compose a tree-like structure when stored according to their binary values. Search on encrypted data has been extensively investigated in recent years. From a cryptographic perspective, the subsisting works fall into two categories, i.e., symmetric searchable encryption and public-key searchable encryption.

Disadvantages of subsisting system

Subsisting semantically secure PEKS schemes take search time linear with the total number of all cipher texts. This makes retrieval from astronomically immense-scale databases prohibitive. Consequently, more efficient search performance is crucial for virtually deploying PEKS schemes. Deterministic encryption has two innate constraints. First, keyword privacy can be ensured only for keywords that are a priori hard to conjecture by the adversary (i.e., keywords with high min-entropy to the adversary); second, certain information of a message leaks ineluctably via the ciphertext of the keywords since the encryption is deterministic. Hence, deterministic encryption is only applicable in special scenarios. The linear search involution of subsisting schemes is the major impediment to their adoption.

Proposed system

We are intrigued with providing highly efficient search performance without sacrificing semantic security in PEKS. We commence by formally defining the concept of Searchable Public-key Cipher texts with

Obnubilated Structures (SPCHS) and its semantic security. In this incipient concept, keyword searchable cipher texts with their obnubilated structures can be engendered in the public key setting; with a keyword search trapdoor, partial cognations can be disclosed to guide the revelation of all matching cipher texts. Semantic security is defined for both the keywords and the obnubilated structures. It is worth noting that this incipient concept and its semantic security are felicitous for keyword-searchable cipher texts with any kind of obnubilated structures. In contrast, the concept of traditional PEKS does not contain any obnubilated structure among the PEKS cipher texts correspondingly; its semantic security is only defined for the keywords.

Advantages of proposed system

We build a generic SPCHS construction with Identity-Predicated Encryption (IBE) and collision-free full-identity malleable IBKEM. The resulting SPCHS can engender keyword-searchable cipher texts with an obnubilated star-like structure. Moreover, if both the underlying IBKEM and IBE have semantic security and anonymity (i.e. the privacy of receivers' identities), the resulting SPCHS is semantically secure.

3. IMPLEMENTATION

Data owner Module

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

Data Utilizer Module

In this module, we develop the data utilizer module. It start by formally defining the concept of Searchable Public-key Cipher texts with Obnubilated Structures (SPCHS) and its semantic security. In this incipient concept, keyword searchable cipher texts with their obnubilated structures can be engendered in the public key setting; with a keyword search trapdoor, partial cognations can be disclosed to guide the revelation of all matching cipher texts.

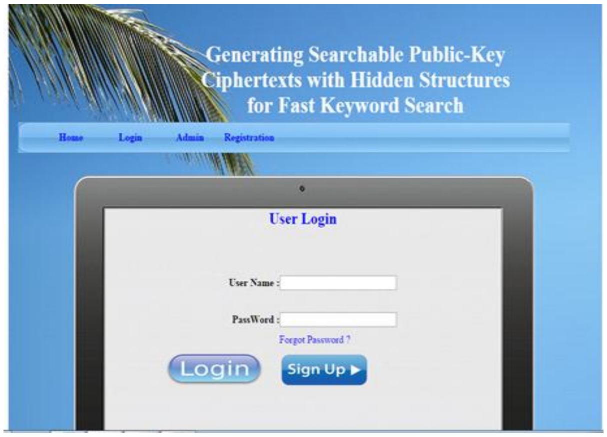
Encryption Module

Incognito identity-predicated broadcast encryption. A marginally more perplexed application is innominate identity-predicated broadcast encryption with efficient decryption. An analogous application was proposed respectively by Barth et al. and Libert et al. in the traditional public-key setting. With collision-free plenarily density malleable IBKEM, a sender engenders an identity predicated broadcast cipher text hC1, C2, (K1 1 jjSE(K1 2 ; F1)), :::, (KN 1 jjSE(KN 2 ; FN))i, where C1 and C2 are two IBKEM encapsulations,

Rank Search Module

It sanctions the search to be processed in logarithmic time, albeit the keyword search trapdoor has length linear with the size of the database. In integration to the above efforts devoted to either provable security or better search performance

4. EXPERIMENTAL RESULTS


Generating Searchable Public-Key
Ciphertexts with Hidden Structures
for Fast Keyword Search
Home
Login
Admin
Registration
Login
Sign Up ▸

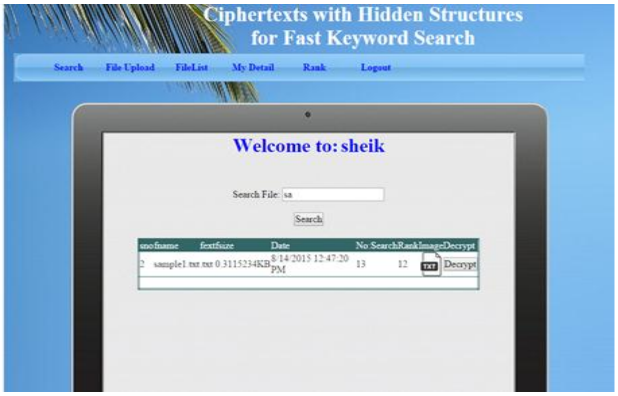
User Login

User Name :

PassWord :

Forgot Password ?

Fig:-1 authentication and authorization

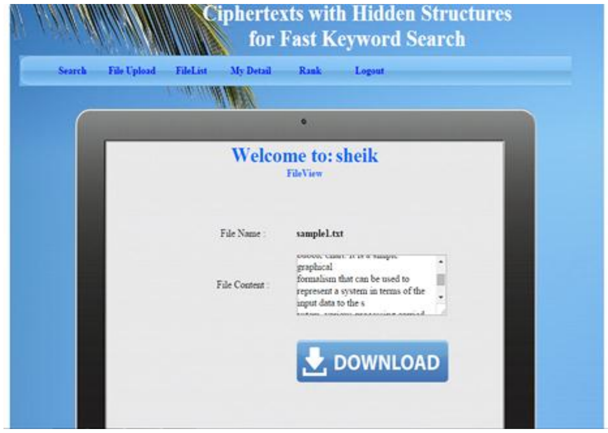


Welcome to: sheik

Search File: sa

sno	fname	fextfsize	Date	No:Search	Rank	Image	Decrypt
2	sample1.txt.txt	0.3115234KB	8/14/2015 12:47:20 PM	13	12	TXT	Decrypt

Fig:-2 Search Results



Welcome to: sheik

FileView

File Name : sample1.txt

File Content : graphical
formalism that can be used to
represent a system in terms of the
input data to the s

Fig:-3 File Download Page

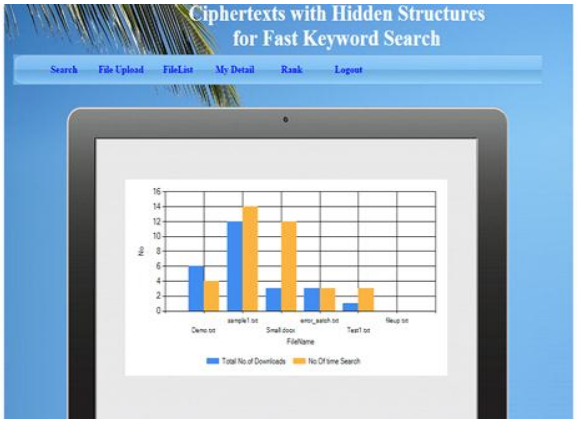
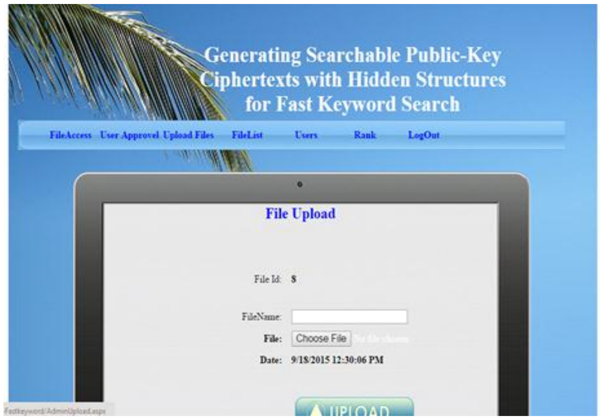


Fig:-4 Results on Graph


Generating Searchable Public-Key Ciphertexts with Hidden Structures for Fast Keyword Search

File Upload

File Id: 8

FileName:

File: Choose File

Date: 9/18/2015 12:30:06 PM

Fig:-5 Data Upload By Admin

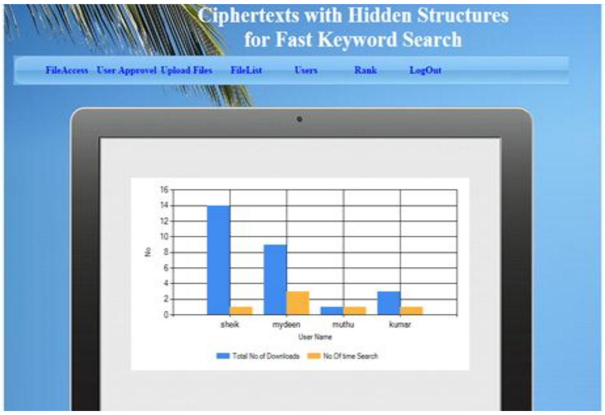

Ciphertexts with Hidden Structures for Fast Keyword Search

Fig:-6 Number of Downloads

5. CONCLUSION

We investigated expeditious keyword search in PEKS with semantic security. Proposed the concept of SPCHS as an alternate of PEKS. The incipient concept sanctions keyword searchable cipher text engendered with the obnubilated structure. Given keyword search trapdoor, search algorithm of SPCHS can disclose part of the obnubilated structure for guidance on ascertaining the cipher text of the queried keyword. Semantic security of SPCHS captures privacy of the keyword and invisibility of the obnubilated structures . The scheme engendered keywords searchable cipher texts with the obnubilated star like structure. The identified several intriguing properties that is collision freeness and full identity malleability in some IBKEM instances and formalized this properties to build a generic SPCHS construction. Applications may be achieve retrival plenariness verification which is the preeminent our comprehension and not been achieved in subsisting PEKS schemes. Another application may be understand public key encryption with the content search and kindred functionality realize by the symmetric searchable keyword encryption . Such kind of content searchable encryption is subsidiary the practice for e.g. Filter the encrypted spams. The obnubilated tree like structure between the sequentially encrypted words in the file. Obtain public key searchable encryption sanctioning content a search.

6. REFERENCES

[1] Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G.: Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J.(eds.) EUROCRYPT2004. LNCS, vol. 3027, pp. 506-522. Springer,Heidelberg (2004)

[2] Bellare M., Boldyreva A., O'Neill A.: Deterministic and Efficiently Searchable

Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp.535-552. Springer, Heidelberg (2007)

[3] Boneh D., Boyen X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT2004. LNCS, vol. 3027, pp. 223-238. Springer,Heidelberg (2004)

[4] Boyen X., Waters B. R.: Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In: Dwork C. (ed.) CRYPTO 2006. LNCS, vol.4117, pp. 290-307. Springer, Heidelberg (2006)

[5] Gentry C.: Practical Identity-Based Encyrption Without Random Oracles. In: Vaudenay S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004,pp.445-464.Springer, Heidelberg (2006)

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

[7] Ducas L.: Anonymity from Asymmetry: New Constructions for Anonymous HIBE. In: Pieprzyk J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 148-164.Springer, Heidelberg (2010)

[8] Abdalla M., Catalano D., Fiore D.: Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions. Journal ofCryptology, 27(3), pp. 544-593 (2013)

[9] Freire E.S.V., Hofheinz D., Paterson K.G., Striecks C.: Programmable Hash Functions in the Multilinear Setting. In: Canetti R., Garay J.A. (eds.) Advancesin Cryptology - CRYPTO 2013. LNCS, vol. 8042,pp. 513-530. Springer, Heidelberg (2013)

[10] Garg S., Gentry C., Halevi S.: Candidate Multilinear Maps from Ideal Lattices. In: Johansson T., Nguyen P. (eds.) Advances in CryptologyEUROCRYPT2013. LNCS, vol. 7881, pp. 1-17. Springer,Heidelberg (2013)

Authors Profile:

VUGGAM NAVYA

B.tech in Sarada Institute Of Technology And Science, Khammam, percentage is 71.39% , year of completed April 2014.M.tech[CSE] (Computer Science And Engineering) in Sarada Institute Of Technology And Science ,Khammam.

Mail id: vuggam.navya@gmail.com

Phone number : 9553059013

Guide Details:

Bagam Laxmaiah.

Experience: 7 years. **Qualification:** M -Tech from JNTU, Hyderabad. **Designation:** Associate Professor. **Working:** Head of Department, Sarada Institute of Technology & Science(SITS), Khammam.

Email-d: laxmanmtech99@gmail.com

Phone Number: 8106467177.