IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-10 E-ISSN: 2347-2693

Design a Model in Alleviating Search Time in Large-Scale Database Retrieval

Adarana Thallapally[1*], P. Poojitha[2], Sridhar Manda[3]

[1*] Dept. of Computer Science and Engineering, SVS Group of Institutions, Bheemaram, Hanamkonda, India
[2]Dept. of Computer Science and Engineering, University PG College, KU, Subedari , Hanamkonda, India
[3]Dept. of Computer Science and Engineering, SVS Group of Institutions, Bheemaram, Hanamkonda, India

[*]*Corresponding Author: adarana2010@gmail.com, Ph. no: 9346465781*

Available online at: www.ijcseonline.org

Received: 28/Sep/2017, Revised: 07/Oct/2017, Accepted: 23/Oct/2017, Published: 30/Oct/2017

Abstract: The notion of traditional public-key encryption by keyword search does not hold any hidden structure between the public-key encryption by keyword search cipher-texts; respectively, its semantic security is just defined for the keywords. We are concerned in provision of efficient search performance devoid of sacrificing semantic security within public-key encryption by keyword search. In our work we introduce searchable public-key cipher-texts by hidden structures in support of keyword search as fast as feasible devoid of sacrificing semantic security regarding encrypted keywords. Our structure is inspired by quite a lot of interesting observations based on the mechanisms of on Identity-Based Key Encapsulation. In the proposed system, the entire keyword-searchable cipher-texts that are structured by hidden relations, and by search trapdoor that corresponds to a keyword, minimum data of relations is revealed to a search algorithm as management to discover the entire matching cipher-texts resourcefully.

Keywords— Public-key encryption by keyword search, Semantic security

I. INTRODUCTION

Traditional secured methods of public-key encryption by keyword search consider search time linear with total number of the entire cipher-texts. This makes recovery from major databases too expensive hence more resourceful search performance is essential for deploying public-key encryption by keyword search methods [1]. Public-key encryption by keyword search contains advantage that anyone who identifies receiver public key upload's keyword searchable cipher-texts towards server. For assuring of appropriate security, hidden star-like arrangement should protect semantic security of keywords, which point towards that partial relations are revealed only when equivalent keyword search trapdoor is recognized. Each of the sender have to be able to produce keyword-searchable cipher-texts with hidden star-likes arrangement by receiver public-key; the server contains keyword search trapdoor has to reveal partial relations, which is linked to the entire matching cipher-texts. Semantic security is preserved when no keyword search trapdoor is recognized, the entire cipher texts are impossible to differentiate, and no information is revealed concerning the structure, and when specified a keyword search trapdoor, only equivalent relations are disclosed, and matching cipher-texts leak no data regarding rest of cipher-texts, except the information that rest do not include queried keyword [2][3]. The search complexity of our system is based on actual number of cipher-texts that includes queried keyword, to a certain extent than number of the entire cipher-texts. In our work we propose searchable public-key cipher-texts by hidden structures in support of keyword search as fast as feasible devoid of sacrificing semantic security regarding encrypted keywords. Our proposed structures are inspired by quite a lot of interesting observations based on the mechanisms of on Identity-Based Key Encapsulation. In the proposed system, the entire keyword-searchable cipher-texts that are structured by hidden relations, and by search trapdoor that corresponds to a keyword, minimum data of relations is revealed to a search algorithm as management to discover the entire matching cipher-texts resourcefully. The system generates keyword-searchable cipher-texts by means of hidden structure like star and has search complexity mostly linear with exact number of cipher-texts that includes queried keyword. We build searchable public-key cipher-texts by hidden structure from the scratch where cipher-texts contain a concealed star-like structure.

II. METHODOLOGY

In public-key encryption by keyword search each of the sender independently encrypts file as well as its extracted keywords and send the cipher-texts towards a server; when

© 2017, IJCSE All Rights Reserved

receiver wants to get back files that contains a particular keyword, he delegates a keyword search trapdoor towards server; which finds encrypted files that contains queried keyword devoid of knowing original files and returns matching encrypted files towards the receiver; at last, receiver decrypts the encrypted files. The searchable public-key cipher-texts by hidden structures in support of keyword search as fast as feasible was introduced devoid of sacrificing semantic security regarding encrypted keywords. Existing methods of semantically secure public-key searchable encryption consider search time linear with total number of cipher-texts which makes recovery from important databases un-affordable. Semantic security is described for keywords as well as hidden structures [4]. This new concept as well as its semantic security is appropriate for keyword-searchable cipher texts by any kind of concealed structures. We construct searchable public-key cipher-texts by hidden structure from scratch where cipher-texts contain a concealed star-like structure. Semantic security of the proposed system captures confidentiality of keywords and invisibility of hidden structures. For security, scheme is confirmed semantically secured on the basis of Decisions Bilinear Diffie-Hellman assumption. The search difficulty of our system is based on actual number of cipher-texts that includes queried keyword, to a certain extent than number of the entire cipher-texts [5]. Hidden star-like arrangement should protect semantic security of keywords for assuring of appropriate security, which point towards that partial relations are revealed only when equivalent keyword search trapdoor is recognized. The search performance mostly depends on actual cipher-texts that contain queried keyword.

III. AN OVERVIEW OF PROPOSED SYSTEM

Our general searchable public-key cipher-texts by hidden structures is inspired by quite a lot of interesting observations based on the mechanisms of on Identity-Based Key Encapsulation. In Identity-Based Key Encapsulation a sender encapsulates a key towards a projected receiver ID which de-capsulate and get hold of key. Our work examines as-fast-as-possible search within public-key encryption by keyword search by semantic security. Semantic security is maintained when no keyword search trapdoor is recognized, the entire cipher texts are impossible to differentiate, and no information is revealed concerning the structure, and when specified a keyword search trapdoor, only equivalent relations are disclosed, and matching cipher-texts leak no data regarding rest of cipher-texts, except the information that rest do not include queried keyword. We are concerned in provision of generic searchable public-key cipher-texts by hidden structures to make keyword-searchable cipher texts by hidden star-like structure. Proposed concept permits keyword-searchable cipher-texts to be produced by means of a hidden structure and in this, entire keyword-searchable cipher-texts that are structured by hidden relations, and by search trapdoor that corresponds to a keyword, minimum data of relations is revealed to a search algorithm as management to discover the entire matching cipher-texts. When specifies a keyword search trapdoor, the search algorithm of the proposed system reveals a part of this concealed arrangement for management on finding out cipher-texts of queried keyword. Semantic security of the proposed system captures confidentiality of keywords and invisibility of hidden structures. The proposed system generates keyword-searchable cipher-texts by means of hidden structure like star. Particularly, by means of forming hidden ring-like arrangement, that is letting very last hidden pointer constantly point to head, one can obtain public-key encryption by keyword search allowing making sure totality of retrieved cipher-texts by means of checking whether pointers of returned cipher-texts forms a ring. It has search complexity mostly linear with exact number of cipher-texts that includes queried keyword. The system outperforms existing public-key encryption by keyword search methods by means of semantic security, whose complexity of search is linear with number of the entire cipher-texts. The proposed system seems a capable tool for solving of some problems within public-key searchable encryption [6]. One application might be to attain recovery completeness verification which, has not been attained within existing public-key encryption by keyword search methods.

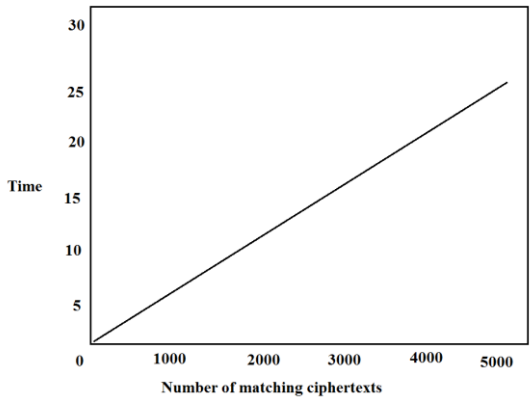

Fig1: Time cost of proposed system

IV. CONCLUSION:

We introduce searchable public-key cipher-texts by hidden structures in support of keyword search as fast as feasible devoid of sacrificing semantic security regarding encrypted keywords. We build searchable public-key cipher-texts by hidden structure from the scratch where cipher-texts contain a concealed star-like structure. For promising of suitable security, hidden star-like arrangement should protect semantic security of keywords, which point towards that

© 2017, IJCSE All Rights Reserved

partial relations are revealed only when equivalent keyword search trapdoor is recognized. The search complexity of our scheme is based on actual number of cipher-texts that includes queried keyword, to a certain extent than number of the entire cipher-texts. For making sure of appropriate security, hidden star-like arrangement should protect semantic security of keywords, which point towards that partial relations are revealed only when equivalent keyword search trapdoor is recognized. In this system, the complete keyword-searchable cipher-texts that are structured by hidden relations, and by search trapdoor that corresponds to a keyword, minimum data of relations is revealed to a search algorithm as management to discover the entire matching cipher-texts resourcefully.

REFERENCES

[1] 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).

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

[3] 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.) Advances in Cryptology - CRYPTO 2013. LNCS, vol. 8042, pp. 513-530. Springer, Heidelberg (2013)

[4] Bellovin S. M., Cheswick W.R.*: "Privacy-Enhanced Searches Using Encrypted Bloom Filters. Cryptography"* ePrint Archive, Report 2004/022 (2004)

[5] Agrawal R., Kiernan J., Srikant R., Xu Y.: *"Order Preserving Encryption for Numeric Data"*. In: Proceedings of the 2004 ACM SIGMOD international conference on Management of data, pp. 563-574. ACM (2004)

[6] Chang Y.-C., Mitzenmacher M.: *"Privacy Preserving Keyword Searches on Remote Encrypted Data"*. In: Ioannidis J., Keromytis A. and Yung M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 442-455. Springer, Heidelberg (2005).

Authors Profile

Mrs.Adarana Woking as an Assstant Professor in SVS Group of Institutions, Bheemaram, Hanamkonda, Warangal, in the department of Computer Science and Engineering, having 8 years of teaching experience, M.Tech completed in 2013, B.Tech from JNTUH completed in 2008. Intrested research area is "Cloud Computing, Data Mining, IoT.

Mrs.Palakala Poojiha Woking as an Lecturer in University PG College, Subedari, affiliated to KU,Warangal,in the department of Computer Science and Engineering, having 7 years of teaching experience, completed M.Tech completed in 2013,Intrested research area is "Cloud Computing, Data Mining, IoT, Big Data.

Mr.Sridhar Manda Woking as an Assstant Professor in SVS Group of Institutions, Bheemaram, Hanamkonda, Warangal, in the department of Computer Science and Engineering, having 10 years of teaching experience, doing Ph.D in University of Mysore.

© 2017, IJCSE All Rights Reserved