International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 04th Febraury 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

Title: Privacy Preserving Ranked Keyword Search Over Encrypted Cloud Data.

Volume 07, Issue 02, Page No: 1 - 4
Paper Authors

***MADHAVI.DANDA, Y.LEELA KRISHNA.**

* Dept of CSE, Sai Thirumala NVR Engineering College.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

PRIVACY PRESERVING RANKED KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA

***MADHAVI.DANDA, **Y.LEELA KRISHNA**
*PG Scholar, Dept of CSE, Sai Thirumala NVR Engineering College
**Assistant Professor, Dept of CSE, Sai Thirumala NVR Engineering College
leelakrishnayalavarthi@gmail.com madhavi.danda521@gmail.com

ABSTRACT:
We present a plan that talks about secure rank based catchphrase look over an encoded cloud information. The information that must be outsourced is scrambled utilizing symmetric encryption calculation for information privacy. The record document of the watchword set that must be sought is outsourced to the neighborhood trusted server where the catchphrase set that is created from the information documents is likewise put away. This is done as such that any un-trusted server can't find out about the information with the assistance of the list framed. The file is made with the assistance of Aho-Corasick various strings coordinating calculation which coordinates the pre-characterized set of watchwords with data in the information records to list them and store applicable information in B+ trees. At whatever point the client looks for a watchword, the demand is sent to the neighborhood put stock in server and the listed information is alluded. The records are recorded in light of the specific significance criteria. Client asks for the expected records to the un-confided in server. The parameters required for positioning is got from the information put away while ordering. In view of the positioning, the documents are recovered from the un-confided in server and showed to the client. The proposed framework can be stretched out to help Boolean pursuit and Fuzzy catchphrase search techniques.

Keywords: Symmetric Encryption algorithm, Rank based search, multiple string matching, relevance scoring, privacy preserving, and cloud computing

INTRODUCTION

Cloud Processing is the advancing innovation that has changed the method for figuring in IT Enterprise. It conveys the product and information to the unified server farms from where a huge group of clients can get to data on pay per utilize premise. This postures security dangers over the information put away. Information classification might be bargained which must be dealt with. So it winds up noticeably important to scramble the information before outsourcing it to the cloud server. This makes information usage a testing assignment. Customary seeking systems give Boolean hunt to look over encoded information, which isn't pertinent when the quantity of clients and the quantity of information records put away in the cloud is substantial. They additionally force two noteworthy issues, one being the post-handling that must be finished by the clients to locate the

pertinent archive in require and the other is the system movement that is unfortunate in show situation when every one of the documents coordinating with catchphrases is recovered. Be that as it may, this paper proposes positioned catchphrase look through that beats these issues.

The paper is detailed as takes after. The related work is abridged in Section 2. The proposed framework and engineering outline is shrouded in Section 3. The plan is part into encryption module, string coordinating module, ordering module and positioning module which are additionally talked about under Section 3. Segment 4 gives the substance about future thoughts and recommendations.

2. RELATED WORKS

It is an imperative research issue to empower the cloud specialist co-op to productively scan for the catchphrase in encoded documents and furnish client with proficient query output keeping up information protection in the meantime. We have examined on the accompanying papers.

2.1 Practical Technique for Search over Encrypted Cloud Data

This paper talks about on consecutive examining look procedure [1] that hunts over scrambled information put away in cloud without losing information secrecy. The method is provably secure and disengages the inquiry result whereby the server doesn't know anything other the item.

It additionally underpins functionalities, for example, controlled looking by server, concealed inquiry bolster for client which scans for a word without uncovering it to the server. With accessible symmetric encryption [7] and pseudorandom arrangement producing components that are secure, encoded information can be viably examined and looked without losing information protection. The plan that is proposed is adaptable that it can be additionally stretched out to help look questions that are joined with Boolean administrators, vicinity inquiries, questions that contain consistent articulation, checking for watchword nearness et cetera. In any case, if there should arise an occurrence of extensive reports and situations that request colossal volumes of capacity, the method has high time multifaceted nature.

2.2 Public Key Encryption with Keyword Search

Dan Boneh proposed an answer for looking over the cloud information that is scrambled utilizing the Public key Crypto System [2].

The thought is to safely connect or label the related catchphrases alongside the each document. This will dodge the need to totally unscramble the record and spare the season of examining whole document to check if the catchphrase exists.

The record is scrambled utilizing an open key encryption calculation [2] and the catchphrases are encoded by PEKS calculation. To recover the archive containing catchphrase W, send just the Trapdoor (W) to server. He proposed two techniques for development of this plan, one utilizing the bilinear maps and other utilizing Jacobi images. The issue with this plan is that each tag of the considerable number of documents must be prepared for finding the match.

3. PROPOSED SYSTEM

We have proposed a proficient plan which empowers the Cloud Service Provider (CSP) to decide the documents that are identified with the catchphrases sought by the client, rank them and send the most pertinent records without knowing any data about the cloud. Our construction comprises of three elements: Data proprietor, Un-trusted cloud server and neighborhood put stock in server. The information proprietor is the one whose information is put away in cloud server and he is additionally approved to look over his documents. Cloud server is an un-trusted server which gives stockpiling administration where information proprietors store their archives in encoded frame. The trusted nearby server stores the record that is made for the documents. The framework engineering is appeared in Fig 1. We accept that authorization of users and keys used for encryption are managed by the local trusted server.

4.CONCLUSIONS

In this paper, we solve the problem of post processing overhead and unnecessary network traffic created when Boolean search techniques are used, by introducing the ranked keyword search scheme. The scheme generates indexes that help the user to search for his documents in a secure environment. The files matching the keyword search are further ranked based on the relevant score calculated with term frequency, file length etc. Further extensions to the project can be done by

1. Supporting multi user environment where there would be an extra entity in the scenario i.e., data user who is authorized to access other users files. The authorization mechanisms and key exchanges methods can be modified to support the same.

2. Tolerating minor typos and format inconsistencies that occur while typing the key words. This can be done by introducing fuzzy keyword mechanism discussed earlier.

3. Boolean Symmetric search technique can be included to support multiple keyword search without making any changes to the existing architecture.

5. REFERENCES

1. D. Song, D. Wagner, and A. Perrig.: “Practical Techniques for Searches on Encrypted Data.” in Proc. of IEEE Symposium on Security and Privacy‟ (2000).

2. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano.: “Public Key Encryption with Keyword Search.” in Proc. of EUROCRYP‟04, volume 3027 of LNCS. Springer (2004).

4. Y.-C. Chang and M. Mitzenmacher.: “Privacy Preserving Keyword Searches on Remote Encrypted Data.” in Proc. of ACNS‟05 (2005).

5. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou.: “Fuzzy Keyword Search over Encrypted Data in Cloud Computing.” in Proc. of IEEE INFOCOM‟10 Mini-Conference (2010).

6. C. Wang, N. Cao, K. Ren, and W. Lou.: “Enabling Secure and Efficient Ranked

Keyword Search over Outsourced Cloud Data." IEEE Transactions on parallel and distributed systems, vol. 23,no. 8 (2012).

7. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou.: "Secure Ranked Keyword Search over Encrypted Cloud Data." in Proc. of ICDCS‟10 (2010).

8. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky.: "Searchable Symmetric Encryption: Improved Definitions and Efficient Construction." in Proc. of ACM CCS‟06 (2006).

9. Remya Rajan.: "Efficient and Privacy Preserving Multi User Keyword Search for Cloud Storage Services." International Journal of Advanced Technology And Engineering Research (IJATER), ISSN 2250 - 3536,Vol 2,Issue 4 (2012).

10. Zeeshan Ahmed Khan, R.K Pateriya.: "Multiple Pattern String Matching Methodologies" A Comparative Analysis (2012).

11. I. H. Witten, A. Moffat, and T. C. Bell.: "Managing Gigabytes: Compressing and Indexing Documents and Images." Morgan Kaufmann Publishing, San Francisco (1999).