ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on Searchable Encryption Techniques for Efficient Data Sharing Over Cloud Encrypted Data.

Prajakta Dimble.

M.E Student, Dept. of Computer Engineering, SKNCOE, Savitribai Phule University of Pune, Pune, India

ABSTRACT: Cloud computing has acquired more recognition within the international because of its flexibility and monetary savings. There are plenty of benefits like easy to get access, control over resources, minimized fee for a consumer as well as businesses are provided via cloud computing. Although having such benefits still cloud customers are facing protection challenge about data which is being outsourced.Because facts proprietor loose his control over records while records are being outsourced so extra security is needed for the outsourced information from the illegal user and malicious users get access to the data over the cloud. The primary security worries provided by the cloud vendors are virtualization and firewalls which are not able to protect privateness of records. To resolve above hassle, we advise a rating search cloud version so one can provide extra privateness and it additionally presents safety over encrypted cloud records where cloud person & cloud server store will now not get known approximately keywords and trapdoors. The trouble of efficient ranked keyword search is solved by various privacy preserving searchable encryption scheme.

KEYWORDS: Cloud computing, privacy issues, searchable encryption, multi-keyword ranked search, privacy preserving.

I. INTRODUCTION

The cloud storage system is used for the purpose of long-term storage services over the Internet. There is a collection of storage servers. Whenever cloud user store their data in third parties cloud system though it will cause security issues to confidentiality of their data. Data hiding techniques provide protection to data secret but it has some restriction to provide some functionality because some operations don't support over hidden information. virtualization and firewalls are the major security concerns provided by cloud Service providers, that would give assurance to data owners, still data owner's data privacy is not going to protect from the cloud service provider itself by using above techniques, since the CSP has control over hardware of cloud, various software , and data owners data. Data confidentiality against CSP can be achieved by usingdata hidden techniques, that cloud user can hide sensitive data before sending it outside. The challenging problem is the utilization of data based on plain text keyword search over encrypted data. This issue can be solved, here we can download all the hidden data and by using the hidden key we can create the original data, but this seems practically difficult because of extra overhead. Solution to above extra overhead is data should be get encrypted before sending to CSP. There is a large amount of increase in cloud users because of the storage efficiency and availability of simple computational models in the cloud. It causes a huge amount of information is being added into cloud servers. So the finding required document file into this bulk of information is the most challenging and time-consuming task. Searching and retrieving specific document over encrypted data is not much easier task. Data is in encrypted forms only so while retrieving such encrypted file user is forced to search in encrypted form only. It causes the data retrieval time efficiency problem.

It is unreliable to access files without any relevance, although it affects the cost of computation. Overall there is need of advance efficient ranked search method to obtain the efficiency in ranked searching over encrypted data; the query can be formed using multiple keywords so that we can achieve required relevant data.

II. RELATED WORK

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski [3] in this paper comparison between cloud computing and conventional computing is explained. functional and non-functional opportunities of cloud storage are determined.

C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou [4] This paper provides the solution to the problem of supporting efficient ranked keyword search, to achieve effective utilization of encrypted data which is stored remotely in cloud computing.it denotes that using existing searchable encryption scheme there is difficulty in achieving efficiency in ranked search. This causes the security issue, to provide the solution to this problem it derives an efficient one-to-many order-preserving mapping function which provides effectively searchable encryption scheme.it gives direction to work on ranked keyword search over encrypted data basically on multiple keywords.
In this scheme to calculate the score an IDF factor is being used, still, the new scheme needs to be designed for preserving the order when summing up scores for all the given keywords. attribute-based encryption is needed to provide fine- grained access control in our multi-user settings.

D.Song, D.Wagner, and A.Perrig,[5], this paper proposed the scheme which supports secret query that is a secret word search request is made by the user to server , however, a server should not get known about a secret word. the simple and fast algorithm reduce space and communication overhead. mail and file server are required to store the information. It should be stored in encrypted form to reduce security and privacy overhead. to avoid overhead the scheme provides provable secrecy for encryption so that the server which is not trustworthy can't learn anything about plain text the controlled searching is provided. without the user’s authorization, an arbitrary word can't be searched by a untrusted server.

Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky[6],proposed most secure searchable symmetric encryption which overcomes all existing security issues. In this technique, data could be outsourced to other party and also privacy is maintained. This technique provides a solution to the problem of searchable symmetric encryption. In this paper, several searchable encryption schemes are explained. Two searchable encryption schemes are proposed that are efficiently searchable encryption and adaptive searchable encryption also multi-user and multi-key SSE schemes are defined in this paper.

C. Wang, N. Cao, J. Li, K. Ren, and W. Lou,[7],[8] in this paper boolean keyword search technique is proposed. It provides a solution to efficient ranked keyword search problem. As a result by using this technique Encrypted data which is stored remotely utilized effectively in cloud computing. It focuses on effective searching and secures ranked keyword searching over encrypted data. keyword searching is done using SSE technique. TF x IDF rules are used for ranking function. OPSE cryptosystem is proposed for security purpose.

P. Golle, J. Staddon, and B. Waters [9], proposed scheme which supports queries with conjunctive keyword over encrypted data. Boolean keyword search problem is solved by this scheme. It proposed secure cloud model for Conjunctive keyword encrypted data search. In this paper it defines two techniques first technique defines communication cost over no. of documents whose security is provided by using the Decisional Diffie-Hellman (DDH) assumption. Second technique defines communication cost on no. of keywords whose security dependable on hardness assumption.

J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou [10], in this paper, provides a technique which solves problem of maintaining keyword privacy and fuzzy keyword search over encrypted cloud data is done effectively. The wildcard-based scheme is used for fuzzy keywords search. system utilization improved by using Fuzzy keyword search. Here keywords are predefined .these predefined keywords matched with returned files. as a result, efficiency is obtained while retrieving the file.

P. Xu, H. Jin, Q. Wu, and W. Wang [11], in this paper probabilistic public key system is explained. multiple users conveniently search ciphertexts using this technique. This system provides the multi-keyword search with the fuzzy search. For keyword searching In previous systems, the dictionary is used For keyword searching which consists of

DOI: 10.15680/IJIRCCE.2016. 0411192

predefined keywords. a hash function is used to provide an index of keywords which has been searched. This hash function provides protective fuzzy search.

B. Wang, S. Yu, W. Lou, and Y. T. Hou [12], in this paper, secure multi-keyword fuzzy search technique is adopted by implementing the locality-sensitive hashing function.

N. Cao, C. Wang, M. Li, K. Ren, and W. Lou [13] in this paper solution is provided to solve the problem of multi-keyword ranked search over encrypted cloud data and they additionally concern with conserving strict system-wise privacy within the cloud computing paradigm. This searchable encryption schemes are utilized to attain various rigorous privacy needs in two different threat models. The coordinate matching technique is employed to capture the connection of information between data documents and requested query. This method is employed to find a variety of keywords within the document. To aim this purpose author were proposing multi keyword search technique. this system produces overheads as Compare to different multi-keyword ranked searching technique.

W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li [14], this paper focuses on the most challenging scenario where the outsourced dataset distributed to multiple users from multiple owners. In this paper, authors describe attribute-based keyword search scheme. efficient user revocation scheme is proposed to enable scalable fine level search authorization. The major concerns about privacy needs are the semantic security of keywords and unlinkability of Trapdoors. This systems drawback is security is not provided to the access pattern because of its high level of complexity. Fine level search and scalability are achieved by this scheme.

T. Jung, X. Y. Li, Z. Wan, and M. Wan [15] addressed the user privacy problem in cloud storage, attribute-based privilege control scheme is proposed in this system. multiple authorities are employed to attain fine level privilege control additionally it provides anonymity control while applying privilege control

III. COMPARISON OF DIFFERENT SEARCHABLE ENCRYPTION TECHNIQUES

TABLE NO 1.COMPARISION OF DIFFERENT SEARCHABLE ENCRYPTION TECHNIQUES

Sr,no	Methods	Process used	Advantage	disadvantage
1	Practical techniques	Pseudo,random, function, Sequential scan, Cryptographic scheme	controlled and hidden search and query isolation is supported. easy and fast	Sequential scan is not efficient to the large data size. overhead occurs in Storing and updating the index.
2	Searchable encryption Scheme	Symmetric Public key encryption	secure search employed over encrypted data on cloud.	costly in terms of computation
3	Boolean Keyword Searchable encryption Scheme	Boolean keyword search using Boolean operators AND, OR and NOT.	comfortable enough to express small, easy information needs	excess network traffic. efficient document ranking is not supported.
4	Single Keyword Searchable Encryption Scheme	encrypted searchable index	keyword frequency utilization to rank results	not comfortable enough to precise complex information needs.
5	Ranked Keyword Searchable Encryption Scheme	Relevance score is employed to make a secure searchable index. order-preserving mapping function.	enhances system usability by returning the matching files in a ranked order concerning to certain relevance criteria. eliminate excess network traffic	compromise the privacy.

6	Fuzzy Keyword Searchable Encryption Scheme	wildcard-based technique.	eliminates the requirement for enumerating all the fuzzy keywords	Supports only Boolean keyword search. Huge storage complexity.
7	Plaintext Fuzzy Keyword Searchable Encryption Scheme	plaintext searching , string matching algorithm.	to find relevant information it allows user to search using try-and-see approach	statistics and dictionary attacks and fails to attain the search privacy.
8	conjunctive keyword Searchable Encryption scheme	Decisional Diffie-Hellman (DDH) and hardness assumption.	Solution to Boolean keyword search problem	Privacy overhead
9	Multi-keyword Searchable encryption Scheme	Provides secure index structure, generates secret trapdoors.	Documents confidentiality and privacy of index, trapdoor, trapdoor unlinkability.	(CSPs) that keep the data for users may access users sensitive infor- mation without authorization.

IV. Conclusion and Future Work

In this paper, we did the brief survey on various strategies for searching encrypted information over a cloud. Several searchable encryption techniques are analysed based on single keyword, Boolean keyword, fuzzy keyword, conjunctive keyword, multi-keyword, search based on similarity measures, attribute-based search etc. the majority of strategies has drawback with them that is they are taking longer time to search the information also they are facing some privacy issues .while multi keyword search techniques supports more privacy and efficient retrieval of data. Therefore a major analysis is important which will provide privacy and minimize the searching time over encrypted information in the cloud.

References

1. Chi Chen, Xiaojie Zhu, Peisong Shen, Jiankun Hu, Song Guo, Zahir Tari, Albert Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method" IEEE Transactions On Parallel And Distributed Systems, VOL. 27, NO. 4, APRIL 2016
2. Zhihua Xia, Xinhui Wang, Xingming Sun, and Qian Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data" IEEE Transactions On Parallel And Distributed Systems, VOL. 27, NO. 2, FEBRUARY 2016
3. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and M. Zaharia," A View of Cloud Computing", Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.
4. C.Wang, N. Cao, J. Li, K. Ren, andW. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data", Proc. IEEE 30th Intl Conf. Distributed Computing Systems (ICDCS 10), 2010.
5. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data", in Proc. of SP, 2000.
6. R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions", Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2006.
7. P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, pp. 31–45,Jun. 2004.
8. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, pp. 253–262,Jun. 2010.
9. 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, pp. 1467–1479, 2012.
10. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM'10, San Diego, CA,pp. 1–5, Mar. 2010.
11. P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Transactions onComputers, vol. 62, no. 11, pp. 2266–2277, 2013.
12. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in IEEE Infocom, Toronto, Canada, pp. 2112–2120,May 2014.

13. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy preserving multi-keyword ranked search over encrypted cloud data,” in Proc. IEEE Infocom’11, Shanghai, China, pp. 829–837,Apr. 2011.
14. W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,” in Proc.IEEE Infocom’14, Toronto, Canada, pp. 226–234,May 2014.
15. T. Jung, X. Y. Li, Z. Wan, and M. Wan, “Privacy preserving cloud data access with multi-authorities,” in Proc. IEEE Infocom’13, Turin, Italy, pp. 2625–2633,Apr. 2013.

BIOGRAPHY

Prajakta Dimble is a student of Master of Engineering in the Computer engineering Department, SKNCOE Pune,Savitribai Phule University of Pune. Her research interests are Cloud computing and Data mining.