INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SEARCHABLE ENCRYPTION TECHNIQUES ON CLOUD DATA STORAGE: A REVIEW

ISHUTA U. WANKHEDE[1], DR. SANDEEP R. SIRSAT[2]

1. Faculty Member (CHB), Department of Computer Science, G.S. Science, Arts & Commerce College, Khamgaon, Dist. Buldana (M.S., India).
2. Associate Professor & HOD, Department of Computer Science, G.S. Science, Arts & Commerce College, Khamgaon, Dist. Buldana (M.S., India).

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Cloud Computing has gained enormous popularity since its advent. It's been a boon for the IT sector. Cloud technology has been widely admired and promoted owing to its flexibility and ease of use. However, it has also been criticized for lack of trust and risks pertaining to security issues. One of the most important services provided by cloud is data storage and backup. Several encryption schemes have been proposed that guarantee the integrity and security of user data in cloud. But it is not possible to perform search on data once it is encrypted. As a solution to this problem, a new approach called Searchable Encryption was introduced which facilitate direct search on the encrypted data. This paper discusses the need of Searchable Encryption schemes and accounts several attempts made in this regards.

Keywords: Searchable Encryption, Fuzzy Keyword Search, Ranked Keyword Search, Multi-Keyword Search, Similarity Keyword Search

Corresponding Author: MS. ISHUTA U. WANKHEDE

Access Online On:

www.ijpret.com

How to Cite This Article:

Ishuta U. Wankhede, IJPRET, 2016; Volume 4 (9): 713-724

PAPER-QR CODE

1. INTRODUCTION

Today is the era of Big Data. As per official statistics, nearly 2.5 quintillion bytes of data is generated each day. Cloud has emerged as opportunity to occupy this enormous data and manipulate it remotely. Most of the IT companies, business firms, and government organizations have migrated their data on cloud. Such data is usually sensitive in nature and hence, cannot be stored in plaintext. Data Encryption schemes guarantee the integrity and safety of the user data. But such schemes leave no scope for the most basic and useful operation over data- searching. We cannot perform direct search on the encrypted data.

Data search is one of the most basic operations. There is no meaning to store a data if it cannot be searched. For searching the encrypted data stored over the remote cloud, entire data first on your local machine and then systematic search can be carried out. This solution is very naive and computationally costlier. A new approach of encryption came forth to solve this problem. It was called Searchable Encryption (SE).

SE allows us to search the encrypted data without decrypting it. The files to be stored over the cloud are first scan for keywords. The keywords are locally indexed. When user wants to search the cloud, he provides the description targeted search. The words in this description are matched with the keywords sorted earlier. These matches are noted and the corresponding files are presented to the user. There are various ways in which this technique can be implemented. The paper discusses various methods under this approach. Section II accounts different schemes and approaches to Searchable Encryption. Section III explains these schemes in brief. Section IV concludes the paper while Section V accounts for the future research prospects.

I. Related work

Song et. al. [36] were first to explore the problem of searching on encrypted data. They used a fast and efficient two layered encryption which requires O(n) operations to query a document of length n. This system was supported by the introduction of oblivious RAMs [16, 32]. The first index-based SSE was proposed by Goh et. al. [15]. It uses a special data structure called as ‘Secure Index’ which can search out a word in the document within unit time complexity. Search can only be conducted using a secret key which generates trapdoor used to query the index. Curtmola et. al. [9] proposed another two inverted index-based SSEs with search time cost O(1). They use an encrypted hash table composed of a series of inverted keyword lists where the head of each list corresponds to a keyword. However, updating the index is very inefficient in this scheme. The only SSE supporting conjunctive keyword search is Golle et. al. [17]. This algorithm is based on elliptic curve and consumes high computational resources.

Many researchers explored search on public databases [8, 10, 11, 14, 21, 22, 30, 31]. This approach is termed as Public Data Retrieval (PIR) [8]. Asymmetric Searchable Encryption (ASE)

was introduced by Boneh et. al. [5]. They proposed two constructions applicable to small number of keywords. Search operations on unorganized data collected on server is explored in [15, 41]. Abdala et.al. [1] improved ASE further. They discussed the issue of inconsistency in Public Encryption Keyword Search (PEKS) and proposed three new schemes- Anonymous Hierarchical Identity based encryption (HIBE), Public Key Encryption (PKE) with temporary keyword search and Identity Based Encryption (IBE) with keyword search. Nateghizad et. al. [29] proposed algorithm based on indistinguishability under Adaptive Chosen Cyphertext Attack (IND-CCA2). However, it suffers from high search time having linear cost. Other works on ASE handle complex queries like conjunctive search [12, 36] and range queries [4, 35]. Several other schemes were proposed to compensate the weaknesses of ASE. Efficient ASE and Multiuser ASE were introduced by Curtmola et. al. [9]. Efficient ASE is efficient than plain ASE and operates faster with logarithmic time complexity. It uses a deterministic function which serves as tag. However, it inherits the vulnerability to dictionary attacks. Multiuser ASE is useful where multiple users conduct search on data owned by single user.

Li et. al. [24] proposed Wildcard based Fuzzy keyword Construction (WFKC). They set a predefined edit distance which could generate all the possible variants of the keyword. Symbol based Trie-traverse Search Scheme by Wang et al. [39] enhances the search efficiency more. It uses a multiway tree to store the Fuzzy Keyword Set over a Finite Symbol Set.

Dictionary Based Fuzzy Set was proposed by Liu et. al. [26]. They suggested choosing only valid keywords in the fuzzy set by checking them against dictionary. They too used fixed edit distance. But this scheme has no scope to detect synonyms for given keyword or different verb forms. E.g kill and assassinate or go, went, gone. Moh and Ho [28] proposed three different searching techniques. First is Synonym Based keyword Search (SBKS) which is improved version of WFKC. It uses Synonym Set. A Keyword Set is constructed by correcting spellings and then Synonym Set is built upon it. E.g. man is searched as man, male, masculine, human, etc. Second is Wikipedia Based Keyword Search (WBKS) which uses Wikipedia technique to match keywords. It helps to keep index size small. Third, Wikipedia Based Synonym Keyword Search (WBSKS) is hybrid of both above. It constructs the index like WBKS and Keyword Set like SBKS. Then term-frequency is computed and checked for similarity against WKS.

Wang et al. [38] first attempted Secure Ranked Keyword Search over encrypted cloud data. Ananthi et al.[2] proposed the ranking of the search results based on the keyword frequency occurring in each file. However, this reveals the frequency of the keyword in each file to the cloud server. Also, keyword frequency being used as the unique ranking metric brings inaccuracy for the ranking.

Cao et al. [6] first attempted Privacy-Preserving Multi-Keyword Ranked Search problem on clouds. They used coordinate matching to evaluate the similarity between files and search requests. They proposed use of inner product similarity to quantify the similarity measure. But

this scheme suffers from three drawbacks. First, it does not support keyword update. If data owners want to insert new keywords into the search, the entire encrypted keyword dictionary has to be rebuilt. Second is the out-of order problem. The scheme suggests that files with more matching keywords could be ranked lower than files with less matching keywords. But if some similar keywords have been matched many times then ranking will be biased and results will be inaccurate. Third, the time and storage complexity of the scheme demands improvement.

Xu et al. [42] adopted the Order Preserving Encryption (OPE) technique to encode relevance scores between keywords and files. They divided files into groups using coordinate matching and then ranked them on the summation of encoded relevance scores of the searched keywords.

Li et al. [25] proposed Multi-Keyword Ranked Query on Encrypted data (MKQE). They proposed the use of partitioned matrices for efficient updation of keyword list. Cao, et al, [6] designed a novel trapdoor generation algorithm, which effectively deals with dummy keywords. Sun et al. [37] introduced use the vector model, where each keyword has Term-Frequency x Inverse Document Frequency (TF×IDF) weight. Ibrahim et al. [18] suggested outsourcing encrypted keywords and files to two different cloud servers in order hide the association between them. Hore et al. [19] proposed color codes to create the index for encrypted files. Shen et al. [34] were first to use occurrences of a keyword to denote its weight in a file vector. Fu et al. [13] proposed to solve the Ranked Multi-Keyword Search over encrypted cloud data supporting synonym query. Zhang et al. [46, 44, 45] proposed to ensure Secure Ranked Multi-Keyword Search while supporting multiple data owners.

Liu et al. [27] proposed a privacy preserving COoperative Private Searching (COPS) protocol. COPS adopts the Paillier encryption to encode the search requests. It allows operations to be carried out on cipher-texts directly without prior decryption. Zhang et al. [43] achieved secure distributed keyword search in geo-distributed clouds**.** Their proposed schemes facilitate secure and efficient distributed multi-keyword search which maximize robustness, availability, and usability of the search system. Park et al. [33] were first to work for Similarity Keyword Search. They proposed encrypted each character in a keyword. They proposed two schemes out of which the first scheme achieves perfect similarity search privacy, while the second scheme ensures high efficiency at the expense of security guarantee.

Wang et al. [40] proposed construction of storage efficient Similarity Keyword Set for a given file collection by using the edit distance. Kuzu et al. [23] proposed construction of a secure index based on a novel technique called Locality Sensitive Hashing(LSH), which is widely used for fast plain-text based similarity search.

II. Overview of Search over Encrypted Data

Many researchers have contributed to the area of conducting search over encrypted data. Drawbacks and inefficiencies of one method have been the inspiration for new approach. We summarize these different approaches to SE in this section.

A. Single Keyword Searchable Encryption

The Searchable Encryption is a two-step process. First the files to be stored are scanned for important words called tokens or keywords. Various methods can be used to filter the keywords like- most occurring uncommon words in the text or the words in the title or name of the document. Once the list of keywords is finalized, it is properly indexed (alphabetically or as per the relevancy with the text). Each keyword is assigned separate pointer for each file containing the keyword. The second step encrypts the index of keywords and the data. The data can be encrypted using any available encryption technique while the index is encrypted using the

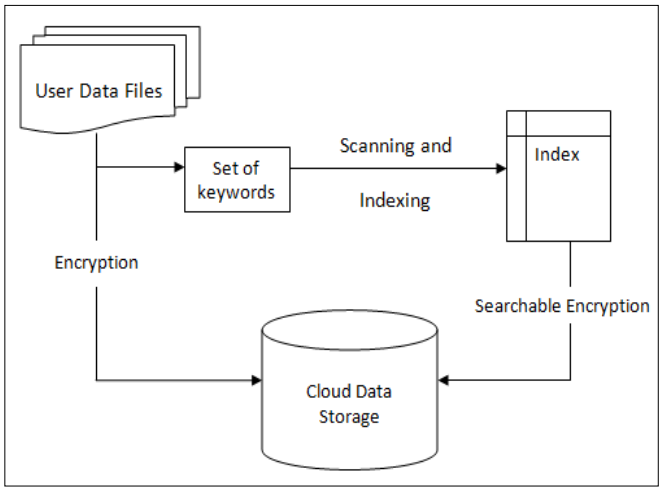

Fig.1. Searchable Encryption

Searchable Encryption. When search is to be performed, the index is fired with the tokens. Only the users who have the key to the encrypted data can generate the tokens. These tokens are matched against the entries from the index and the corresponding pointers are retrieved which link the user to the documents containing the keyword. There are two types of Searchable Encryption depending upon single user or multiuser scenarios for data generation and search.

i. Symmetric Searchable encryption(SSE)

SSE is useful when the user has to carry out search on the data generated by itself. It uses efficient data structures and is quite secure. This approach is more desirable for the private databases.

ii. Asymmetric Searchable encryption(ASE)

ASE is used when data is generated by one group and the search is carried out by another group. It is less secure as it reveals the keyword under the Dictionary attack. But in spite of being inefficient and slower than SSE, it applies to wider array of situations.

B. Fuzzy Keyword Search

SSE and ASE could perform search based on a single keyword. This technique can give inaccurate results if the keywords are accidently replaced or misspelled. Fuzzy Keyword Search approach came forth to solve this problem. A Fuzzy Keyword Set is constructed which consist of words whose spellings match approximately with the spelling of keyword. Some popular Fuzzy Keyword Generation techniques are-

i. Wildcard based Fuzzy keyword Construction (WFKC)

WFKC specifies a parameter called Edit Distance which specifies the numbers of alphabets that can be altered in original keyword to generate a Fuzzy Keyword Set. The replaceable characters are called as Wildcards and they are denoted by '*'. E.g. if edit distance is one then the fuzzy set for keyword king will be {king, *king, *ing, k*ing ki*ng, kin*g, king*, king}. But the size of fuzzy set increases heavily with increase in edit distance.

ii. Gram based Search

Gram based search uses K-gram which is a sequence of k characters. For example, "any", "nyw", "ywa" and "way" are all the 3-grams of the word "anyway". During the indexing process, system first constructs the dictionary of all the k-grams in the collection. Posting lists for each k-grams are then generated. All of these posting lists compose the k gram index called safe index. This predefined index is then used to generate fuzzy keyword set.

iii. Symbol based Trie-traverse Search

This scheme uses a multiway tree to store the Fuzzy Keyword Set over a finite symbol set. All trapdoors sharing a common prefix have common nodes. The root is associated with an empty set and the symbols in a trapdoor can be recovered from the root to the leaf that ends the trapdoor. All fuzzy words in the trie can be found by a Depth First search.

C. Ranked Single Keyword Search

Ranked search enhances system usability by returning the matching files in a ranked order. It uses certain relevance criteria (e.g., Keyword frequency) to achieve privacy preserving data search service in cloud computing. It returns the most relevant files to the given keyword saving the communication cost for the search and providing better user experience.

Large numbers of data files are stored on the cloud. So, Ranked Keyword Search only returns the most relevant *k* files. An efficient one-to-many order-preserving mapping function is used and a relevance score is mapped to different encoded values. The corresponding order is preserved. Thus, the cloud server can rank the files according to the order of the encoded relevance scores without knowing the actual data of relevance scores.

D. Similarity Keyword Search

A Similarity Keyword Search returns all possible files that are similar to search requests. Such search is extremely useful when the user has less information about the item he has to search. All the keywords within a specific edit distance are put into a Similarity Keyword Set. Then the keywords in the similarity set and files are encrypted and outsourced to the cloud. To perform a search user first generates a Similarity Keyword Set, encrypts them and submits them to the cloud. The cloud searches all the files according to the received encrypted Keyword Set and returns the corresponding result set. The data user further decrypts data and obtains the desired files. To improve the search efficiency on the cloud a private trie-traverse searching index is also built in which a multi-way tree is constructed for storing the Similarity Keyword Set.

E. Multi-keyword Search

Multi-keyword search is more practical approach which allows users to specify more than one keyword. It helps to describes search request more accurately. The results of the Multi keyword search can be ranked as per relevance. A Ranked Multi-Keyword Search allows users to submit a search request with multiple keywords and to search the most relevant files corresponding to their search request.

Such schemes allow the cloud server to find top-k relevant files corresponding to a multi keyword query. The files stored in the cloud and the multi-keyword queries are both encrypted throughout the search process. The cloud cannot identify the query or the contents of files. Thus, data privacy and query privacy are both preserved.

III. CONCLUSION

Almost all the searchable symmetric encryption schemes expose the relationship between the file ID and the trapdoor. The attacker can keep track of the user search pattern. After certain number of search from the user, attacker might identify a set of documents that contain particular tokens relevant to the user. These keywords can then be guessed. An argument is made in these regards that this flaw is not of the cryptographic model but it is a problem pertaining to the usage of the service. The attacker may never actually break the encryption key but he keeps track of the usage of search technique and makes guess. Public key based schemes preserve this leakage by introducing randomness in the trapdoor generation. But, the tokens generated are deterministic in nature which means that looking upon a particular query the service provider can tell whether it has been repeated though he can know what exactly the query was. There are solutions to these problems but they are inefficient due to the computational cost. Also, most of the searchable encryption schemes work with single keyword search. Extending them to large scale cloud data causes heavy computation and storage cost. None the less, highly inaccurate results can be returned in case of spelling mistakes in keywords.

Fuzzy Keyword Search techniques do not consider how to rank the search result and relevance between the original keyword and the files, which may lead to incorrect ranking. Also, few methods increase the size of the Fuzzy Keyword Set exponentially. The Ranked Keyword Search is a brilliant concept. However, proper method is necessary to obtain accurate ranking. Multi-Keyword Search is very helpful in case of descriptive search. Its combination with Ranked Keyword Search is very much desirable.

IV. FUTURE SCOPE

Searchable encryption is most natural form of information retrieval from cloud. This area has vast scope for research. New models are expected that could curtail the search time complexities and facilitate easy updation of indexes. Much work is to be done on Similarity Keyword Search. Different encryption schemes can be combined to encrypt the indexes, keywords and data. The drawbacks of existing schemes need to be treated. There is a need of novel data structures and search algorithms for enhancing the efficiency. Work is expected in order to fetch the exact and ordered information desired by the user. The use of Proofs of Retrievability can be integrated in subsequent searching schemes.

When multiple data owners are involved, there are few challenges like how to distribute and manage secret keys for different data owners, how to efficiently generate trapdoors for data of different users and how to achieve decryption capability. The Fuzzy Keyword Search can be made more efficient if accurate and short Fuzzy Keyword Sets are generated. A practical Ranked Keyword Search system should enable Ranked Multi-Keyword Search as well. In spite of lots of research in Multi Keyword Search, there is no scheme which can defend statistical

attacks. A Similarity Keyword Search is quite challenging realm due to the security and privacy obstacles. Secure similarity search needs to be worked upon before it could be practically implemented. Such implementation needs efficiency, security, and robustness. Efforts are expected to achieve personalized search service.

REFERENCE:

1. Abdalla M., Bellare M., Catalano D., Kiltz E., Kohno T., Lange T., Malone-Lee J., Neven G., Paillier P., and Shi H., "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions", Journal of Cryptology, Vol. 21 Issue 3, Mar. 2008, pp- 350-391.

2. Ananthi, S., Sendil M. S. and Karthik S., "Privacy preserving keyword search over encrypted cloud data. In Advances in Computing and Communication, Springer Berlin Heidelberg 2011, pp. 480-487.

3. Boldyreva A., Chenette N., Lee Y., and ONeill A., "Order-preserving symmetric encryption", Proceedings of 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, 26-30 April, 2009, pp.224-241.

4. Boneh D. and Waters B., "Conjunctive, subset, and range queries on encrypted data", Proceedings of 4th Conference on Theory of cryptography TCC 2007, pp. 535-554.

5. Boneh D., Crescenzo G., Ostrovsky R. and Persiano G., "Public key encryption with keyword search", Proceedings of Int. Conference, Perugia, Italy, 30 Jun. - 3 Jul., 2008, pp. 1249-1259.

6. Cao N., Wang C., Li M., Ren K. and Lou, W., "Privacy-preserving multi-keyword ranked search over encrypted cloud data", INFOCOM, 2014 Proceedings IEEE, pp. 829-837.

7. Chang Y. C., Mitzenmacher M., "Privacy preserving keyword searches on remote encrypted data", Applied Cryptography and Network Security 2005, Springer.

8. Chor B., Goldreich O., Kushilevitz E. and Sudan M., "Private Information Retrieval", FOCS 95.

9. Curtmola R., Garay J., Kamara S., Ostrovsky R., "Searchable symmetric encryption: improved definitions and efficient constructions", Proceedings of the 13th ACM conference on Computer and communications security, ACM 2006.

10. Di Crescenzo G., Ishai Y., and Ostrovsky R., "Universal service-providers for database private information retrieval", Proccedings of the 17th Annual ACM Symposium on Principles of Distributed Computing 1998, pp. 91-100.

11. Di Crescenzo G., Malkin T., and Ostrovsky R.. Single-database private information retrieval implies oblivious transfer. In Advances in Cryptology - EUROCRYPT 2000, 2000.

12. Dodis Y., Katz J., Xu S. and Yung M., “Key-insulated public key cryptosystems," in Advances in Cryptology, Eurocrypt 2002, LNCS, Springer-Verlag, pp. 65-82, 2002.

13. Fu Z., Sun X., Linge N. and Zhou, L. (2014), “Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query”, Consumer Electronics, IEEE Transactions on, 60(1), 164-172.

14. Gertner Y., Ishai Y., Kushilevitz E., and Malkin T., “Protecting data privacy in private in-formation retrieval schemes”, Procceedings of the 30th Annual ACM Symposium on the Theory of Computing, pp. 151-160, 1998.

15. Goh E., “Secure indexes,” Technical Report 2003, CiteseerX Beta, http://eprint.iacr.org/2003/216.pdf.

16. Goldreich O. and Ostrovsky R., “Software protection and simulation by oblivious RAMs”, JACM, 1996.

17. Golle P., Staddon J., and Waters B., “ Secure conjunctive keyword search over encrypted data”, Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, Newyork, USA edited by Steven M. Bellovin, Rosario Gennaro, Angelos Keromytis, Moti Yung .

18. Ibrahim A., Jin H., Yassin A. and Zou, D., “Secure rank-ordered search of multi-keyword trapdoor over encrypted cloud data”, Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific (pp. 263-270).

19. Hore B., Mehrotra S., and Tsudik G., “A privacy-preserving index for range queries”, Proceedings of the 30th Int. Conference on Very large data bases-Vol. 30, pp-720-731.

20. Kamara S. and Lauter K., “Cryptographic Cloud Storage”, Springer Link, vol. 6054, pp 136-149.

21. Kushilevitz E.and Ostrovsky R., “Replication is not needed: Single Database, Computationally- Private Information Retrieval”, in FOCS 97.

22. Kushilevitz E. and Ostrovsky R., “One-way Trapdoor Permutations are Sufficient for Non-Trivial Single-Database Computationally-Private Information Retrieva”, Proc. of EURO-CRYPT '00, 2000.

23. Kuzu M., Islam M. S., and Kantarcioglu M., “Efficient similarity search over en-crypted data”, Proc. IEEE 28th Int. Conf. Data Eng. ,Apr. 2012, pp. 11561167.

24. Li J., Wang Q., Wang C., Cao N., Ren K. and Lou W., “Fuzzy Keyword Search over Encrypted Data in Cloud Computing”, In INFOCOM, 2010 Proceedings IEEE, pp. 1-5

25. Li R., Xu Z., Kang W., Yow K. C.and Xu, C., "Efficient multi-keyword ranked query over encrypted data in cloud computing. Future Generation Computer Systems", Future Generation Computer Systems 30, 179-190.

26. Liu C., Zhu L., Li L., Tan Y., "Fuzzy keyword search on encrypted cloud storage data with small index," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, 2011, pp 269-273.

27. Liu Q., Tan C. C., Wu J. and Wang G., "Cooperative private searching in clouds", Journal of Parallel and Distributed Computing 2012, Vol. 72, Issue 8, pp. 1019-1031.

28. Moh T. and Ho K., "Efficient Semantic Search over Encrypted Data in Cloud Computing", Proceedings of International Conference on High Performance Computing & Simulation HPCS-2014, 21-25 July 2014, IEEE, pp- 382-390.

29. Nateghizad M., Bakhtiari M., Mohd. Maarof A., "Secure Searchable Based Asymmetric Encryption in Cloud Computing", Int. Journal of Advance Software Computing Appl. 2014, Vol.6, Issue 1, pp. 678-564.

30. Naor M. and Pinkas B., "Oblivious transfer and polynomial evaluation", Proc. of the 31th Annual ACM Symposium on the Theory of Computing, pp. 245.

31. Ogata W. and Kurosawa K., "Oblivious Conjunctive keyword search", Journal of Complexity 2014, Vol. 20, Issue 2-3, pp. 356-371.

32. Ostrovsky R., "Software protection and simulation on oblivious RAMs", MIT Ph.D. Thesis, 1992.

33. Park H. A., Kim B. H., Lee D. H., Chung Y. D. and Zhan J., "Secure similarity search. In Granular Computing", IEEE International Conference on GRC Nov. 2007, pp. 598-598. I

34. Shen Z., Shu J. and Xue, W., "Preferred keyword search over encrypted data in cloud computing", Quality of Service (IWQoS), 2013 IEEE.

35. Shi E., Bethencourt J., Chan T-H. H., Song D. and Perrig A., "Multi-dimensional range query over encrypted data", Proceedings of the 2007 IEEE Symposium on Security and Privacy SP 2007, pp-350-364.

36. Song D., Wagner D., and Perrig A., "Practical Techniques for Searches on Encrypted Data", in Proc. of the 2000 IEEE Symposium on Security and Privacy (S&P 2000).

37. Sun W., Wang B., Cao N., Li M., Lou W., Hou Y. T. and Li H., "Verifiable privacy-preserving multi keyword text search in the cloud supporting similarity-based ranking", IEEE Transactions on Parallel and Distributed Systems 2014, Vol. 25, Issue 11, pp. 3025-3035.

38. Wang C., Cao N., Li J., Ren K. and Lou, W., "Secure ranked keyword search over encrypted cloud data", 30th International Conference on Distributed Computing Systems (ICDCS), 2010 IEEE, pp. 253-262.

39. Wang J., Ma H., Tang Q., Li J., Zhu H., Ma S., Chen X., "Efficient verifiable fuzzy keyword search over encrypted data in cloud computing", Computer Science and Information Systems 2013, Vol. 10, Issue 2, pp. 667-684

40. Wan. C., Ren K., Yu S. and Urs, K. M. R., "Achieving usable and privacy-assured similarity search over outsourced cloud data", INFOCOM, 2012 Proceedings IEEE , pp. 451-459.

41. Waters B., Balfanz D., Durfee G., Smetters D., "Building an encrypted and searchable audit log", to appear in NDSS '04.

42. Xu J., Zhang W., Yang C., Xu J.and Yu N., "Two-step-ranking secure multi-keyword search over encrypted cloud data", International Conference on Cloud and Service Computing (CSC), 2012, pp. 124-130.

43. Zhang W., Wu J. and Lin Y., "Secure and privacy preserving keyword search over the large scale cloud data", accepted to appear in Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, 2015.

44. Zhang W., Lin Y., Xiao S., Wu J. and Zhou S., "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing", IEEE Transactions on Computers, Jun. 2015, Volume:PP , Issue: 99 , pp. 1.

45. Zhang W., Lin Y. and Gu Q., "Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing 2015", IEEE Transactions on Cloud Computing.

46. Zhang W., Xiao S., Lin Y., Zhou T. and Zhou S., "Secure ranked multi-keyword search for multiple data owners in cloud computing", 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2014, pp. 276-286.

47. Zheng M. and Zhou H., "An Efficient Attack on A Fuzzy Keyword Search Scheme over Encrypted Data", IEEE International Conference on Embedded and Ubiquitous Computing, 2013, 13-15 Nov. 2013, pp- 1647-1651.