Searching Techniques over Encrypted Cloud Data

Azza A. Abdo
Department of Computer Science, College of Science and Humanities - Jubail, Imam Abdulrahman Bin Faisal University, Saudi Arabia

Shereen Saleh
Math and Computer Science, Minufiya University, Egypt

Passent Elkafrawy
Math and Computer Science, Minufiya University, Egypt

ABSTRACT
Nowadays, large amount of data can be stored in the cloud. To preserve the secrecy of the data, the data must be encrypted. Encryption techniques play a major role when data are outsourced to the cloud, so that only the authenticated users can access. This study focuses on different searching techniques over the encrypted data in cloud. In this paper a comparison between different kinds searchable encryption techniques according to the features of multiple keyword, amount of scale data, search complexity, accuracy, and, amount of storage.

Keywords
Cloud, Ranked search, Fuzzy search, Conjunctive search, Multi-keyword search, Semantic search.

1. INTRODUCTION
A cloud is a set of connected servers and computers which are accessible through the internet [1]. It consider as "a pool of virtualized computer resources", this pool of virtualized resources provide abstraction of data. Service oriented , availability of resources (e.g. networks, servers, storage, applications and services), sharing resources, on-demand delivery of resources, virtualization, scalability of resources, pay-per-use, loose coupling, self-service, ease of use and high fault tolerance all these are the key characteristic of cloud computing [1,2].

A Large amount of data can store in the cloud. Encryption techniques play a major role when data outsourced to the cloud, since encryption techniques ensure the secrecy of data accessing. Many schemes have been proposed in keyword searching on encrypted data in cloud computing. Based on the related work, we can analyze searching techniques over encrypted data in five major groups, 1. Searchable Index Schemes, where the index file is built based on the actual keywords extracted. 2. Fuzzy key word search, which allowing matching between the query keyword and the stored keywords, and retrieving the approximate closest results. 3. Conjunctive keyword search, only returns documents with keywords specified by the search query. 4. Multi-keyword ranked search, which returns documents that contain one or more words specified by query. 5. Semantic search: where the search is built on sharing the original keywords different meanings with a different structure.

An overview of each searching technique type will be introduced at section.2. Also a comparison between them will be given at section.3. Finally conclusion of our paper will be given in section.4.

2. RELATED WORK

2.1 Searchable Index Schemes
The first construction of searching over encrypted data was proposed by Song et al. in 2000[3]. The scheme didn't contain an index, it only encrypt each word in the file independently, and thus, the search operation went through the entire file. This method is simple and fast, but it uses a sequential searching over data, and it isn't suitable of large amount of data size. The scheme is too slow in searching for a large number of documents.

In 2002, Goh [4] developed Per-file searchable index schemes. He used a bloom filter to construct the indexes for the data files, which reduce the cost of searching corresponding to number of files.

As a complementary approach, the first searchable encryption system using the public key system is proposed, by Boneh et al, 2004 [5], in which server contains encrypted files and keywords. User creates keyword trapdoor T_W using its private key to search w. The server checks T_W with existing encrypted keywords and sends encrypted file that match it. In Bonh scheme, the trapdoor may be memorized and then it well reveal knowledge about the keyword [5]. G.Duntao scheme [6] tried to solve the problem of memorized trapdoor. Based on Boneh's scheme, G.Duntao et al. proposed a temporary keyword search scheme over public key encryptio. G.Duntao scheme solves the problem of the memorized trapdoor. G.Duntao scheme divides the time into a few time slides, and generates a temporary trapdoor for corresponding time slides. The trapdoor of a keyword in some time t_1 doesn't reveal anything about the trapdoor at time t_2. To achieve more efficient search, Curtmola et al, 2006 [7] proposed an index searching technique. In Curtmola scheme, it builds an index file. In the index file, each entry consists of a trapdoor of each keyword and the corresponding files identifiers contain the keyword. Secure and privacy preserving keyword searching (SPKS) was proposed in 2011 by Q.Liu et al. [8]. In SPKS scheme cloud service provider (CSP) can determine files contain query keywords, and then make a partial decipherment of this files before returning the search results. Q.Liu scheme reduces the overhead in decryption for the user.

In 2012, B.Long et al [9] proposed an improved public encryption with keyword search scheme. The scheme builds an index as in Boneh scheme [5]. The scheme reduces the time cost of keywords search by dividing keywords into sets, so while a keyword searching, the server scan the particular keywords of the particular set. Similarity search over outsourced cloud encrypted data is still a major proplem, when user's search results might not match the input search. C.Wang et al [10] scheme suggested to build a storage with a set of similar keywords for each keyword in each document. The Wang scheme returns all most similar matched entries to the user. The similarity of keywords are built with a distance between them. Also C.Wang scheme proposes symbol-based trie-traverse searching mechanism for achieving the similarity search with constant search time complexity.

In 2013, Tseng et al [11] proposed IPEKS, where cloud storage provider maintains two lists, C-list and N-list. N-list contains files identifier, and C-list contains files identifiers for pervious searching. CSP searches C-list first to obtain file identifier. If the file identifier isn't in C-list, the CSP searches the N-list to obtain file identifier and then includes this information to C-list.

In 2016, S. Raghavendra et al. [12] proposed the concept of master key generation used to encrypt and store the contents in Cloud data. Raghavendra scheme designed an index-file for fast file retrieval from the cloud. Also, in Raghavendra scheme, only the master-key is updated with every revocation or membership modify without changing on the existing group members private and public keys.

In 2017, C.Liu et al. [13] proposed the idea of Multi-Data-Source Dynamic Symmetric Search Encryption (MDS-DSSE), which allows each data source to generate a local index individually and enables the storage provider to combine all local indexes into a global index afterwards.

In 2018, N. Rahim et al. [14] proposed a scheme to support secure search of images at mobile gallery phone. It encrypt images using a light-weight encryption algorithm on mobile device, and then it is uploaded to the cloud for features extraction to eliminate the computationally expensive process of features extraction on mobile. Images features extraction is holed by pre-trained convolution neural network (CNN) using a deep auto-encoder. A hash codes is computed and sent back to the mobile device to store in the hash table at mobile device. To retrieve a desired image the scheme uses approximate nearest neighbor (ANN) search approach.

2.2 Fuzzy Keyword Search

The fuzzy keyword search scheme depends on pre-set keywords, the server is expected to return the files containing the keyword. Fuzzy keyword schemes return the search results according to the user's searching input. If user search input exactly matches a keyword of the pre-set keywords, the system already returns the documents containing this keyword. Else if there exists errors and additionally design irregularities in the searching input, the server will retrieve the nearest conceivable outcomes dependent on pre-indicated comparability semantics. Pre-indicated comparability semantics for of the wrong searching keyword and correct intended keyword is measured as distance between two words. Distance between two words is measured as the number of operations required to transform one of them into the other. There are three primitive operations substitution, deletion, and insertion. Straight forward and wild-card based are two approaches used to edit the distance. Wild-Card based approach calculates edit distance by wild card fuzzy sets. To represent one or more character in Wild-Card search, the asterisk$'*'$ is used. All forms of keywords are needed to be listed to calculate the distance between two words, so it makes fuzzy search needs large storage to store data, and it is one of the most disadvantages of fuzzy search is the large storage that it need to store the data. The advantage of Wild-Card is reducing the size of the fuzzy keyword sets.

In 2010, Li et al [15] proposed a first technique using fuzzy keyword search scheme over encrypted cloud data. Li scheme used the metric of edit distance to construct a fuzzy keyword search scheme. In 2011, C.Lu et al [16] proposed a construction of dictionary-based fuzzy set. This dictionary contains each keyword and its corresponding fuzzy keywords by using edit distance. This scheme reduces each of index size, storage, and the overhead computation, where the dictionary contains all fuzzy keywords.

Fuzzy keyword search scheme with verifiable search result over cloud server was proposed by J. Wang et al [17](Wang) in 2012. In Wang scheme, an identifier is assigned to each document and a set of keywords, the symbol-tree is used in mapping. The server retrieves the search request and the proof for the result to the user. In Wang scheme, the user can verify the correctness of the result. In 2013, W.Zhou et al [18] proposed a k-gram based fuzzy keyword ranked search system over encrypted cloud data. The fuzzy set is constructed based on grams and Jaccard coefficient to calculate the keywords similarity. The gram of a string is a substring and can be used for effective approximate search. The order of the characters after the primitive operation is always kept the same before the operations. Then search results are ranked according to weighted ranking function.

In 2016, X-Jin Shi et al. [19] proposed cloud data search strategy based on fuzzy multiple keywords by supporting Chinese and English keyword search. The scheme used an English and Chinese comparison table to convert Chinese keyword to English keyword to retrieve of fuzzy multi-keyword from the hybrid data.

In 2017, M A-Manazir.Ahsan et al. [20] proposed a scheme for fuzzy keyword search on encrypted data focusing on fuzzy word matching among dictionary words. Based on the letter position in the word, the scheme constructed a monogram set by transforming keyword. This enables to find out original word from its typo with maximum similarity matric.

In 2018, X.Ge et al. [21] proposed a verifiable exact keyword search scheme and then extend to fuzzy keyword search scheme. In X.Ge et al. scheme built a linked list with three nodes for the same keyword and produce a fuzzy keyword set for it. One index vector for each fuzzy keyword set was generated to decrease the storage space and computation cost.

2.3 Conjunctive Keyword Search

The goal of a conjunctive keyword search (CKS) is to enable the user to ask a conjunctive keyword query to the server, so that the server can test which encrypted data contains the conjunctive keyword. In CKS system, data and keywords are firstly encrypted and then uploaded into the storage system, hence the server cannot see the data and keywords. In 2004, P.Golle et al. [22] assumed structured documents where keywords are organized with vector $D_i = (w_{i1}, w_{i2}, \dots, w_{in})$ where w_{ij} is the keyword of document D_i in the j'th keyword field. To search keywords $w_1, w_2, \dots, w_j$, server verify that a document contains a specific keyword in field j. As in 2012, N.M et al [23] in this technique, proposed a conjunction of keywords is implemented for searching and retrieves most efficient and relevant data files in a ranked order. An advanced Tire-Tree is used for storing this conjunction of keywords and searching each separately. This technique uses Gram-Based method and Wild-Card method for fuzzy keyword construction. In both these methods the conjunction of keyword is implemented, which will produce a highly efficient ranked result. In 2014, J.Yu et al [24] proposed an efficient conjunctive fuzzy keyword search scheme. Conjunctive fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. More specifically, use edit distance to quantify keywords similarity for the construction of fuzzy keyword sets. Where scheme J.Wang et al [18] only

supports single fuzzy keyword search. If the users want to retrieve the files that contain a set of keywords, he has to repeatedly implement the protocol for several times, which is rather inefficient. The definition of conjunctive fuzzy keyword search can be formulated as follows: given a collection of m encrypted data files $D = \{D1, D2, \dots, Dm\}$ stored in the cloud server, associated a list of keywords $W = \{Swi1, \dots, Swil\}$ with each document $Di(Sw, d)$denote the set of words w' satisfying $ed(w, w') \leq d$ for a certain integer d) and a searching input $W = (w1, \dots, wd)$, the execution of conjunctive fuzzy keyword search returns a set of file Ids whose corresponding data files possibly contain the word $W = (w1, \dots, wd)$.

In 2018, MB.Smithamol et al. [25] proposed a privacy enhanced conjunctive search (PECS) over encrypted data in the cloud. Also a parallel search is used at MB.Smithamol et al. scheme by constructing a tree-based partitioned index structure (TPIS) in cloud data server by multiple threads, and this reduces search time cost. Also, the scheme provides query privacy and keyword privacy.

2.4 Multi-keyword Ranked Search

Ranked search, over outsourced cloud data, facilitates searching settings of single keyword and multi-keyword search. Ranked search scheme was proposed in 2010, by Wang et al [26]. This scheme supports only single keyword search. It uses the order preserving symmetric encryption, and gives each keyword a weight by. Cloud server rank relevant data files doesn't have knowledge about the specific keyword weight.

Multi-keyword search over encrypted cloud data (MRSE) is firstly defined in 2011, when N.cao et al. made the first attempt to define and solve multi-keyword ranked query problem (kNN) [27]. In N.cao et al, data owner first defines a set of keywords and builds a dictionary containing them. The dictionary contains an index vector p built for each keyword. If the file in dataset contains a keyword, the element $p[i]$ is set to 1, otherwise, $p[i]$ is set to 0. To execute multi keyword ranked query q, firstly a trapdoor to equerry keywords set is sent to cloud server provider (CSP). CSP uses inner product between the trapdoors and $p[i]$ to determine the similarity between them. Finally, the first k results with the highest scores are returned to user. But in this scheme, position of each keyword in the dictionary is fixed, so it must rebuilt it when the number of keywords increased. So, Z.Xu et al. proposed scheme for multi-keyword query (MKQE) [28] with the same steps of MRSE N.cao et al. scheme [27]. Only minor changes in the dictionary structure have to be done at MKQE scheme.

In 2012, P.Lu et al [29] proposed a searchable encryption multi-keyword with two rounds (TRSE). P.lu algorithm uses a vector space model to measure inner product similarity between document index vector and query vector in which giving each keyword weight by TF-IDF and hence support more accurate ranked search result. Also in 2012, based on inner product similarity,

C.Yang et al [30] proposed a combination of kNN-based MRSE scheme and bloom filter. C.Yang scheme propose a new multi-keyword search scheme based on inner product similarity. The scheme is proposed for supporting multi-keyword semantic with privacy. Also, it combines bloom filter to support dynamic update.

In 2013, K.Sengoden et al. [31] proposed searching scheme based on combination between concepts and keyword searching techniques. K.Sengoden used keyword search method to get relevance results when the user search keyword hasn't any spelling errors. But if the user keyword hasn't any meaning, then the concept based searching is added. Concept based searching returns words are conceptually related to user keyword search.

In 2013, C.Orencik et al. [32] proposed multi-keyword search scheme that returns search results in a ranked order manner. C.Orencik scheme uses minhash functions to compare between documents signatures and queries signatures, then sort this matching results according to the query relevancy to.

In 2014, B.Wang et al. [33] proposed a scheme supports fuzzy and multiple keyword search. B.Wang scheme was based on building index on per file. The index containing all the keywords in the file is an m-bit bloom filter. LSH functions is the key for implementing fuzzy search in B.Wang scheme, where the scheme converts each keyword into a bigram vector and then use locality sensitive hashing (LSH) functions to insert keywords into the bloom. Also, in 2015, H.Poon et al. proposed a phrase search scheme [34]. H.Poon scheme takes bloom filters space efficiency to obtain low storage cost.

In 2016, X.Jiang et al. [35] developed a multi-keyword ranked search scheme over encrypted cloud data. A special data structure QSet based on an inverted index structure is used for accomplish an efficient multi-keyword search. The X.Jiang scheme strategy was to search the estimated least frequent keyword in the query to significantly narrow down the number of searching documents. Ranked search is supported in X.Jiang scheme by using the common TF IDF×rule to compute the relevance scores of documents matching a given search request. X.Jiang et al. scheme also supports search results verification.

In 2018, Y. Miao et al. [36] presented a secure cryptographic primitive, Verifiable Multiple Keywords Search (VMKS) over ciphertexts, which leverages the Identity-Based Encryption (IBE) and certificate less signature techniques. The VMKS scheme allows the user to verify the correctness of search results and avoids both certificate management and key escrow limitations.

2.5 Semantic Search

Semantic search means retrieving of synonyms of query keywords, where this keywords are a predefined. In semantic search the keywords extracted from outsourced text documents are extended by its common synonyms, for examples, the synonym of the keyword “journey” is “travel” or “trip”, these keywords are totally different in spelling. Semantic search is used into knowing search engine Wikipedia, where there are three schemes was developed to improved search over it such as, Synonym-keyword search (SBKS): Wikipedia-based keyword search, and Wikipedia-based synonym keyword search.

In 2014, Z.Fu et al [37] proposed a searchable encrypted scheme which supports both multi-keyword ranked search and synonym-based search. Z.Fu scheme uses a vector space model (VSM) to build document index. Searchable index tree is constructed with the document index vectors. So the related documents can be found by traversing the tree. Also, in 2014, T.Moh et al [38] proposed semantic search scheme extends the search to keywords with similar meaning and reduce

Table.1. A comparison between searching techniques types

	Single keyword search	Ranked keyword search	Fuzzy keyword search	Multiple-keyword search	Semantic search
Multiple keyword.	Not support	support	support	support	support
Amount of Scale data.	Suitable	Suitable	Not suitable	Not suitable	Not suitable
Search complexity	O(N)	O(log N) where M is domain score of keyword W	O(1) search on each document	O(mn) Where m documents and n unique terms.	O(rn) Where r number of files and n number of distinct keywords.
Accuracy	Not accurate	High accuracy	Acceptable	Acceptable	Less accuracy
Storage	Less	Not large	Large	Less	Large

unrelated keywords.

In 2016, C. Rama Krishna et al. [39] proposed Privacy Preserving Synonym Based Fuzzy Multi-Keyword Ranked Search over Encrypted Cloud Data(BBSBFMRS). BBSBFMRS-scheme provides fuzzy and synonym based multi-keyword ranked search schemes to enhance the user search experience. The scheme utilized a binary tree based dynamic index of encrypted keywords in alphabetic post-order sequence. The binary tree minimize the overhead of updating index in the case of new files uploaded.

In 2018, B.Lang et al. [40] proposed semantic-based compound keyword search (SCKS) scheme. SCKS-scheme combines the Locality-Sensitive Hashing function and the secure k-Nearest Neighbor scheme. SCKS achieves both of semantic-based search, multi-keyword search, and ranked keyword search.

3. COMPARISON

In this section we make a comparison between searchable encryption techniques according to this features:

1. Multiple keyword: It means which kind of the search algorithms allow searching over data for more than one keyword which narrow down the number of search result?.
2. Amount of Scale data: It means which of kind of the search algorithms is suitable to be used in the case for searching over large amount of data. It's not a standard term but can be associated with data that grows to a huge size over time.
3. Search complexity: Algorithmic complexity is concerned about how fast or slow particular algorithm performs, time complexity is the computational complexity that describes the amount of time it takes to run an algorithm. Complexity of the fastest algorithms takes $O(N)$.
4. Accuracy: It means the retrieved results approximation ratio from the desirable search. Some of searching algorithms gets high accuracy for the desired searing, and some are not, and some has an acceptable accuracy. Accuracy refers to the closeness of the results to the known or true results.
5. Large storage requirements (Storage): Storage offers a simple way in which data is maintained, managed, backed up and made available to users. It is a main point of the desired requirement of each search techniques. Some algorithms depends on the number of files stored on the server, some needs large amount of storage, and some algorithms needs less amount.

Table.1 summarized the comparison between the previous schemes according above metrics. We can see that the above studied searching techniques had been proposed to conduct the search over the encrypted data that are been stored on the cloud side. Each of this methods has some advantages and also disadvantages, for example the single keyword search technique facilitates search result relevance, but it does not support multiple keyword search. On the other hand, ranked keyword search techniques have a high accuracy of search for wide range of applications. But, a large amount of post-processing of encrypted files is the most disadvantage of it. Also, the fuzzy keyword search techniques increase searching effectiveness hence the distance can be implemented, but not support ranked search problem, and need a large storage requirements.

On the other hand, the multiple-keyword search techniques improve search accuracy. But it is not suitable for large scale data. Also for the semantic search techniques, it is more efficient and more practical and performed better in the search quality. But the time of index construction is high.

4. CONCLUSION

In this study rigorous analysis was made on encryption techniques which relate to search based retrieval of files from the outsourced encrypted data. Many searchable techniques have been analyzed based on single keyword, multiple keyword search, and ranking, fuzzy tolerance. The ultimate goal is to enable search semantics in a privacy preserving manner. Rank based retrieval of data has been discussed which provides fast search access and consider most efficient for searching on encrypted data and only similar files are retrieved.

5. REFERENCES

[1] S. Zhang, X.Chen, and S.Wu: Analysis and Research of Cloud Computing instance, second International Conference on Future Network, China, IEEE, pp. 88-92, (2010).

[2] C.Gong , J.Liu , Q.Zhang , H.Chen , and Z.Gong :The Characteristics of Cloud Computing, 39th International Conference on Parallel Processing Workshops,pp. 275-279,(2010).

[3] S. Zhang, X.Chen, and S.Wu: Analysis and Research of Cloud Computing instance, second International Conference on Future Network, China, IEEE, pp. 88-92, (2010).

[4] C.Gong , J.Liu , Q.Zhang , H.Chen , and Z.Gong :The Characteristics of Cloud Computing, 39th International Conference on Parallel Processing Workshops,pp. 275-279,(2010).

[5] D.Song, D.Wagner, and A.Perrig :Practical Techniques for Searches on Encrypted Data, In Proc. Of IEEE Symposium on Security and Privacy ,pp. 44-55,(2000).

[6] E-J.Goh :Secure indexes, In Cryptology ePrint Archive on October 7th, pp. 1-18,(2003).

[7] D.Boneh, G.Di Crescenzo, R.Ostrovsky, and G.Persiano :Public Key Encryption with Keyword Search, In Proc. Of Euro Crypto'04, pp. 506-522,(2004).

[8] G.Duntao, H.Dawei, C.Haibin, and Y.Xiaoyuan :A new Public Key Encryption with Temporary Keyword Search, In International Conference on computer, Mechatronics, Control and Electronic Engineering(CMCE), (volume:4), pp.80-83,(2010).

[9] R.Curtmola, J.A.Garay, S.Kamara, and R.Ostrovsky :Searchable Symmetric Encryption: improved definitions and efficient constructions, In Proc. Of ACM CCS, pp. 79-88,(2006).

[10] Q.Liu, G.Wang, J.Wu :Secure and Privacy Preserving Keyword Searching for Cloud Storage Services , Journal of Network and Computer Applications, (volume:35),pp 927-933,(2011).

[11] B.Long, D.Gu,N.Ding, and H.Lu :On Improving the Performance of Public Key Encryption with Keyword Search , International Conference on Cloud and Service Computing(CSC), pp. 143-147,(2012).

[12] C.Wang, K.Ren, S.Yu, K.Mahendra, and R.Urs, :Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data , In Proc. IEEE INFOCOM , pp. 451-459,(2012).

[13] F.Tseng , R.Chen ,and B.lin: iPEKS : Fast and Secure Cloud Data Retrieval from the Public-Key Encryption with Keyword Search, In 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom) , pp. 452-458 ,(2013).

[14] S. Raghavendra, K. Meghana, P. A. Doddabasappa, C. M. Geeta, Rajkumar Buyya , K. R. Venugopal ,S.S.Iyengar and L.M.Patnaik: Index Generation and Secure Multi-User Access Control over an Encrypted Cloud Data. Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016).

[15] C.Liu, L.Zhu and J.Chen: Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud, Journal of Network and Computer Applications, Volume 86, 15 May 2017, Pages 3-14.

[16] N.Rahim, J.Ahmad, K.Muhammad, A-Kumar.Sangaiah and S-Wook.Baik: Privacy-preserving image retrieval for mobile devices with deep features on the cloud, Computer Communications, Volume 127, September 2018, Pages 75-85.

[17] J.Li , Q.Wang , N.Cao , K.Ren , and W.Lou :Fuzzy Keyword Search over Encrypted Data in Cloud Computing , In Proc. IEEE INFOCOM , pp. 1-5,(2010).

[18] C.Liu,L.Zhu,L.Li,and Y.Tan: Fuzzy Keyword Search on Encrypted Cloud Storage Data with Small Index, In IEEE International Conference on Cloud Computing and Intelligence Systems(CCIS) ,pp. 269-273,(2011).

[19] J.Wang, X.Chen, H.Ma, Q.Tang, and J.Li: A Verifiable Fuzzy Keyword Search Scheme over Encrypted Data, Journal of Internet Services and Information Security(JISIS) ,pp.49-58,(2013).

[20] W.Zhou , L.Liu , H.Jing , C.Zhang , S.Yao , and S.Wan :K-Gram Based Fuzzy Keyword Search over Encrypted Cloud Computing , Journal of Software Engineering and Applications, pp. 29-32,(2013).

[21] X-jin SHI and S-ping HU, Fuzzy Multi-Keyword Query on Encrypted Data in the Cloud. 2016 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics/1st Intl Conf on Big Data, Cloud Computing, Data Science & Engineering.

[22] M A-Manazir Ahsan, F-Z.Chowdhury, M.Sabilah, A- W-Bin Abdul Wahab, and M –Y- Idna Bin Idris: An efficient fuzzy keyword matching technique for searching through encrypted cloud data, 2017 International Conference on Research and Innovation in Information Systems (ICRIIS).

[23] X. Ge , J.Yu , C.Hu , H.Zhang and R.Hao: Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing, IEEE Access (Volume: 6) August 2018, Pages 45725 – 45739.

[24] P.Golle, J.Staddon, and B.R.Waters :Secure Conjunctive Keyword Search over Encrypted Data, In Proc. Of ACNS, pp. 31-45,(2004).

[25] N.M, and L.P :Improving the Efficiency of Data Retrieval in Secure Cloud , Advances in communication,network, and computing lecture notes of the institute for computer sciences, social informatics and telecommunications engineering ,pp. 238-241,(2012).

[26] J.Yu, J.Li, X.Wang, and W.Gao :Conjunctive Fuzzy Keyword Search over Encrypted Data in Cloud Computing ,TELKOMNIKA Indonesian Journal of Electrical Engineering , pp. 2104-2109,(2014).

[27] MB.Smithamol and R.Sridhar: PECS: Privacy Enhanced Conjunctive Search over Encrypted Data in the Cloud Supporting Parallel Search, Computer Communications, Volume 126, August 2018, Pages 50-63.

[28] C.Wang , N.Cao , J.Li , K.Ren , and W.Lou :Secure Ranked Keyword Search over Encrypted Cloud Data , In

IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 253-262 , (2010).

[29] 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 , pp. 829-837 (2011).

[30] Z.Xu , W.Kang , R.Li , K.Yow , and CH-Zhong.Xu :Efficient Multi-Keyword Ranked Query on Encrypted Data in the Cloud , IEEE 18th International Conference on Parallel and Distributed Systems (ICPADS), pp. 244-251,(2012).

[31] P.Lu, J.Yu, X.Dong, G.Xue, and M.Li :Privacy- a ware Multi-keyword Top-k search over Untrust Data Cloud, In IEEE 18th international conference on Parallel and distributed systems(ICPADS), pp. 252-259,(2012).

[32] C.Yang, W.Zhang, J.Xu, and N.Yu : A fast privacy-preserving multi-keyword search scheme on cloud data, International Conference on Cloud and Service Computing (CSC), pp. 104-110,(2012) .

[33] K.Sengoden, and S.Paul : Improving the Efficiency of Ranked Keyword Search over Cloud Data, International Journal of Advanced Research in Computer Engineering &Technology(IJARCET) , pp. 881-883,(2013) .

[34] C.Orencik , M.Kantarcioglu , and E.Savas :A practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data, IEEE sixth International Conference on Cloud Computing(CLOUD) , pp. 390-397,(2013) .

[35] B.Wang,S.Yu,W.Lou,and Y.Hou :Privacy Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud , IEEE INFOCOM ,IEEE Conference on Computer Communications , pp. 2112-2120,(2014).

[36] H.Poon, and A.Miri: Alow Storage Phase Search Scheme based on Bloom Filters for Encrypted Cloud Services, IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 253-259,(2015).

[37] X. Jiang J. Yu J. Yan, and R. Hao: Enabling Efficient and Verifiable Multi-keyword Ranked Search over Encrypted Cloud Data, Information Sciences,Volumes 403–404, September 2017, Pages 22-41.

[38] Y.Miao, J.Weng, X.Liu, K-Raymond.Choo, Z.Liu and H.Li: enabling verifiable multiple keywords search over encrypted cloud data, Information SciencesVolume 465, October 2018, Pages 21-37.

[39] Z.Fu , X.Sun , L.N , and L.Zhou :Achieving Effective Cloud Search Services: Multi-Keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query, In IEEE Transactions on Consumer Electronic , pp. 164-172,(2014) .