International Journal on Applications in Information and Communication Engineering
Volume 3: Issue3 : December 2017, pp 10 -16 www.aetsjournal.com *ISSN (Online) : 2394 - 6237*

An Analysis of Privacy Preserving Security Algorithms and Searchable Encryption Techniques in Cloud Computing

N.SathyaBalaji , Dr. Komarasamy.G

Abstract— Data storage and privacy becomes a major issue nowadays in the cloud storage service because valuable and private information has to be encrypted before uploading the data to the cloud server which makes file searching process very difficult for the cloud users. To selectively fetch the data or files of their own requirements, various searching options are available only on the plain text data which is supported by the major cloud servers. Enormous searching methods are available on the encrypted data but they support only exact keyword search. Exact keyword search is not suitable for cloud storage systems, because it doesn't allow the users to typing errors or format misrepresentations, which greatly affects the search efficiency and makes user irritated. In this paper, we explored the existing encryption algorithms, and searching techniques and their applications and features in the existing cloud infrastructure. This will help the cloud service provider to decide which algorithm to choose for encryption and decryption which will facilitate more cloud users to utilize the cloud platform by simplifying the data storage and retrieval process in the cloud environment while preserving their privacy in the cloud.

Keywords -- Cloud storage service; Exact Keyword search; Privacy .

I. INTRODUCTION

With the enormous reach of cloud computing, there is a well established trend of IT firms and public users ready to store their data in the cloud storage. In many cases, the storage services provided by the cloud companies cannot be fully trusted, so emails, personal health records, government documents and other sensitive information have to be encrypted before uploading to the cloud. Since the data uploaded by the data owners is encrypted, the searching of documents which contain specific keywords becomes rather difficult.

Intuitively, we may come up with a solution that the user downloads all the encrypted data and decrypts them with his/her secret key, and then he/she uses normal search methods to search documents containing specific keywords.

This approach is obviously not effective and requires the users to have strong storage capacity. The plaintext searching methods which are present cannot be applied directly to encrypted cloud data, thus data encryption makes data search a big problem. To solve the problem above, there have been many researches on efficient and secure keyword search on encrypted data [1]-[9].

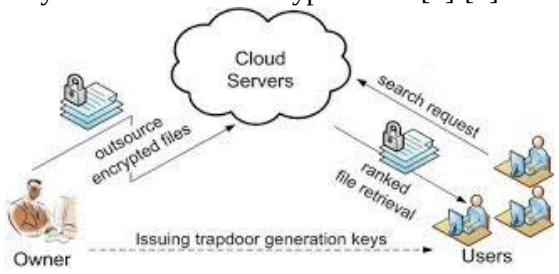

Fig 1.1 Cloud file storage and retrieval

II. ANALYSIS OF VARIOUS ENCRYPTION ALGORITHMS IN CLOUD

We will analyze the various encryption algorithms available for encrypting data in cloud searching techniques that can be applied to the encrypted data.

1) Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for both encryption and decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits. The entire plaintext is divided into blocks of 64bit size; last block is padded if necessary. Multiple permutations and substitutions are used throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. DES algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. Entire operation can divided into three phase. First phase is Initial permutation and last phase is the final permutations.

N.SathyaBalaji, Research scholar, Anna University, (Email Id: sathyabalajin@gmail.com)
Dr. Komarasamy.G , Assistant Professor (Senior Grade) , Department of CSE, Bannari Amman Institute of Technology, India. (Email Id: gkomarasamy@gmail.com)

2) Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). Most adopted symmetric encryption is AES. It operates computation on bytes rather than bits, treats 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. It operates on entire data block by using substitutions and permutations. The key size used for an AES cipher specifies the number of transformation rounds used in the encryption process [8][9].Possible keys and number of rounds are as following:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Major advantages of AES over DES are

1. Data block size is 128 bits.
2. Key size 128/192/256 bits depending on version.
3. Most CPUs now include hardware AES support making it very fast.
4. It uses substitution and permutations.
5. Possible keys are 2128 , 2192 and 2256 [10]
6. More secure than DES.
7. Most adopted symmetric encryption algorithm.

3) Rivest-Shamir-Adleman (RSA)

8.

RSA is a public key cipher developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular asymmetric key cryptographic algorithm. This algorithm uses various data block size and various size keys. It has asymmetric keys for both encryption and decryption. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose [11]. This algorithm can be broadly classified in to three stages; key generation by using two prime numbers, encryption and decryption.

RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data [12]. This algorithm is mainly used for secure communication and authentication upon an open communication channel.

While comparing the performance of RSA algorithm with DES and DES, When we use small values of p & q(prime numbers) are selected for the designing of key, then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES [12]. Operation speed of RSA Encryption algorithms is slow compare to symmetric algorithms; moreover it is not secured than DES.

4) Homomorphic EncryptionAlgorithm:

It is an encryption algorithm that provide remarkable computation facility over encrypted data(cipher text) and return encrypted result. This algorithm can solve many issues related to security and confidentiality issues. In this algorithm encryption and decryption taking place in client site and provider site operates upon encrypted data. This can solve threat while transferring data between client and service provider, it hide plaintext from service provider, provider operates upon ciphertext only.

Homomorphic encryption allows complex mathematical operations to be performed on encrypted data without using the original data. For plaintexts X1 and X2 and corresponding ciphertext Y1 and Y2, a Homomorphic encryption scheme permits the computation of X1 Θ X2 from Y1 and Y2 without using P1 Θ P2.The cryptosystem is multiplicative or additive Homomorphic depending upon the operation Θ which can be multiplication or addition[13].

III. SEARCHING TECHNIQUES

There are various searching techniques available, and to mention a few are as follows:

1) Searchable Encryption:

It allows users to securely search complete encrypted data through keywords. This method support only Boolean search, without capturing any relevant data. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. First one, users who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every file got, in order, to find ones most matching their interest; another drawback, regularly getting all files containing the queried keyword further incurs unnecessary network traffic, when retrieve more than one files.

2) Single Keyword Searchable Encryption:

A single keyword searchable encryption schemes usually builds an encrypted searchable index such that, it's content is hidden to the server, unless it is given appropriate trapdoors generated via secret key(s). Early work solves secure ranked keyword search which utilizes keyword frequency to rank results instead of returning undifferentiated results. However, it only supports single keyword search. Where anyone with public key can write to the data stored on server, but

only authorized users with private key can search. Traditional single keyword searchable encryption schemes are usually built in a way by creating an encrypted searchable index. Such indexes content will be hidden to the server. The information will be revealed only when the server gives the correct trapdoors that are generated via a secret key(s). The main drawback of single keyword-based search is that it is not comfortable enough to express complex information needs.

3) Ranked Keyword Search:

Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (eg. keyword frequency) thus, making one step closer toward practical deployment of privacy-preserving data hosting services in the context of cloud computing. To the best of knowledge it gives a legal status for the first time the problem of effective ranked keyword search over encrypted cloud data. Ranked keyword search strongly provides system usability by returning the matching files in ranked order concerning to certain relevance criteria, thus moving close towards the practical action of privacy preserving data presenting services in cloud

At first, the Blowfish key is exchanged with ECC for further encryption/decryption. In every Blowfish encryption, new random number of 64-bit is generated and checks whether least significant 16-bit of this number contains minimum five 1's or not. The procedure of random number generation is shown in Fig. 1. According to position of 1's in least significant 16-bit of random number, the F function is executed only in those corresponding rounds. It will be not executed in those rounds when there is 0's. The flowchart for Integrated Blowfish encryption is shown in Fig. 1. This will cause variation in execution of F function in every encryption/decryption. Kelsey developed an attack that could able to crack blowfish with 3 rounds but unable to attack whole 16 round algorithm19. Rijmen developed a second order differential attack that could attack able to crack blowfish with only 4 rounds20. Because of it, we have made constrain that the minimum five rounds must be executed in Blowfish.

4) Computing

To achieve design goals investigate the statistical measure approach from Information retrieval (IR) and text removal to insert relevance score of each file during the establishment of searchable index before outsourcing the encrypted file collection. An IR system allocates a relevance score to each and every document and ranks those documents by this score. Relevance score is used to build a secure searchable index to properly protect the sensitive information. This technique enables data users to find the most related information rapidly, rather than burdensome sorting through every match in the content collection. Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data. For privacy protection, such ranking function, however, should not leak any keyword relevant information. Another one, to improve search result accuracy as well as enhance user searching experience, it is also essential for such ranking system to support multiple keywords search.

5) Multi-keyword Searchable encryption:

Over the years, various searchable encryption approaches have been developed to provide the ability for selectively retrieving the encrypted documents through a keyword search. Typically, these systems build a secure index structure and outsource it along with the encrypted documents to the remote server. Authorized users submit their requests as secret trapdoors that are integrated properly with the stored indexing information. The server uses the received trapdoor to search over the stored index, and retrieves the matching encrypted documents. However, the previous searchable encryption schemes are impractical for real world cloud computing scenarios because these systems are designed to handle either a single keyword search or a Boolean search.

6) Fuzzy Keyword Searchable Encryption:

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, it uses edit distance to quantify keywords similarity and develop a novel technique that is a wildcard-based technique, for the construction of fuzzy keyword sets. This technique eliminates the need for enumerating all the fuzzy keywords and the resulted size of the fuzzy keyword sets is significantly reduced.

7) Plaintext Fuzzy Keyword Search:

The importance of fuzzy search has received attention in the context of plaintext searching in information retrieval community. The problem is addressed in the traditional information access paradigm by allowing user to search without using try-and-see approach for finding relevant information based on approximate string matching. At the first glance, it seems possible for one to directly apply these string matching algorithms to the context of

searchable encryption by computing the trapdoors on a character base within an alphabet. This trivial construction suffers from the dictionary and statistics attacks and fails to achieve the search privacy.

8) Boolean Keyword Search:

Boolean systems allowed customers to specify their information need using a combination of Boolean operators AND, OR and NOT. Boolean systems have several disadvantages, for example there are no any features of document ranking, and it is very difficult for a customer to make a good search request. Thus, the drawback of existing system specifies the important need for new techniques that support searching flexibility.

IV. OTHER SEARCHING TECHNIQUES:

Even though there are various systems existing, this literature survey mainly concentrates on the single keyword based encryption and multi-keyword based encryption and also included other searching techniques due to it known advantages.

1) Single keyword search:

- Deepali D. Rane et.al, [1] proposed implementation of the encryption and decryption, Secure index construction is successfully completed with desirable performance. After index construction it will get compressed and will be stored in .cfs file format. After firing single-keyword query, user will get all documents that contain the specified keyword. The advantages are protects data privacy by encrypting documents before out sourcing, rank based retrieval of the documents, To easily access the encrypted data by multi keyword rank search using keyword index. The Disadvantages of the proposed system are single-keyword search without ranking, Boolean keyword searching without ranking, single-keyword search with ranking, Rarely sorting of the results i.e. no index creation and ranking, Single User search.

C. Wang et al, [2] proposed a secure ranked keyword search technique that utilizes the keyword frequency to rank the results. The major drawbacks of single keyword search systems with or without ranking most probably won't retrieve the relevant data and it may also compromise the privacy.

- Y.-C. Chang et al, [3] proposed similar "index" approaches, in which a single encrypted hash table index was built for the entire file collection.
- D. Song, D. Wagner et al, [4] proposed a searchable encryption, in which each and every word in the considered document was encrypted autonomously under two-layered encryption construction.

2) Multi-keyword search:

- Zhihua Xia et.al,[5] proposed a secure, efficient and dynamic search scheme, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. They construct a special keyword balanced binary tree as the index, and proposed a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be carried out to further reduce the time cost. The security of the scheme is protected against two threat models by using the secure KNN algorithm. Experimental results demonstrate the efficiency of proposed scheme. The Advantages of the proposed system are searchable encryption schemes enable the client to store the encrypted data to the cloud and execute keyword search over cipher text domain and a secure tree-based search scheme over the encrypted cloud data, which supports multi-keyword ranked search and dynamic operation on the document collection. The disadvantages are the cloud service providers (CSPs) that keep the data for users may access users sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt the data before outsourcing. However, this will cause a huge cost in terms of data usability.
- Bing Wang et.al, [6] proposed a novel construction of a public key searchable encryption scheme based on inverted index. This scheme overcomes the one-time-only search limitation in the previous schemes. The disadvantages of the proposed system are first of all, the keyword privacy is compromised once a keyword is searched. As a result, the index must be rebuilt for the keyword once it has been searched. Such solution is counterproductive due to the high overhead suffered. Secondly, the existing inverted index based searchable schemes do not support conjunctive multi-keyword search, which is the most common form of queries now a days. The advantages are explore the problem of building a searchable encryption scheme based on the inverted index, Achieve secure and private matching between the query trapdoor and the secure index, Design a novel trapdoor generation algorithm so that the query related inverted lists are combined together secretly without letting the cloud server know which inverted lists are retrieved.

- Yanzhi Ren et.al, [7] proposed a light-weight search approach that supports efficient multi-keyword ranked search in cloud computing system. The basic scheme employs the polynomial function to hide the encrypted keyword and search patterns for efficient multi-keyword ranked search. Then improve the basic scheme and propose a privacy-preserving scheme which utilizes the secure inner product method for protecting the privacy of the searched multi-keywords. The advantage of the proposed system is it analyzes the privacy guarantee of the proposed scheme and conduct extensive experiments based on the real-world dataset. The disadvantage is there is a chance of leakage of data in cloud.
- Hongwei Li et.al, [8] proposed a multi-keyword ranked search scheme to enable accurate, efficient and secure search over encrypted mobile cloud data. Security analysis have demonstrated that proposed scheme can effectively achieve confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user. The advantages Constructs an efficient index to improve the search efficiency. And it solves the trapdoor unlinkability problem. It also achieve enhanced efficiency in terms of functionality and search efficiency compared with existing proposals.
- Mikhail Strizhov et.al, [9] proposed a searchable encryption technique that enables secure searches over encrypted data stored on remote servers. They define and solve the problem of multi-keyword ranked search over encrypted cloud data. In particular, they present an efficient similarity searchable encryption scheme that supports multi-keyword se

  solution is based on two building blocks: Term Frequency Inverse Document Frequency (TF-IDF) measurement and ring-LWE-based variant of homomorphic cryptosystem. The Advantages of this system is it returns the matching data items in a ranked ordered manner. The Disadvantage is in traditional system it supports only single keyword search.

3) Other searching techniques:

- E.-J. Goh et al, [10] proposed a technique that uses Bloom filters in order to construct the indexes for the data files. Bloom filter containing trapdoors (for each file) of all distinct words is built up and stored on the server. For searching a particular word, the user must generate the search request by computing the trapdoor of the word and sends it to the server. The server upon receiving the request performs tests to check if any Bloom filter holds the trapdoor of the query word and if so, it returns the corresponding file identifiers.
- Jun Zhou et.al, [11] proposed a more efficient verifiable outsourced computation of encrypted data EVOC from any one-way trapdoor function is proposed by combining a newly devised privacy-preserving data aggregation supporting both addition and multiplication operations with Yao's Garbled Circuit. The advantage is it proves the security of the proposed efficient privacy-preserving data aggregation scheme.
- Fanyu Bu et.al, [12] proposed a privacy preserving back propagation algorithm based on the BGV encryption scheme on cloud. One property of the proposed algorithm is to apply the BGV encryption scheme to the back-propagation algorithm for preventing the disclose of private data with cloud computing. The advantages: The proposed algorithm improves the efficiency of back-propagation learning by offloading the expensive operations on the cloud. It also prevents the disclosure of private data, using full homomorphic encryption scheme to encrypt the source data. The disadvantage is sensitive data is easily disclosed during the process of the computation on the cloud.
- Joseph K et.al, [13] proposed an infrastructure for secure sharing and searching for real-time video data. It is particularly suitable for mobile users by deploying 5G technology and a cloud computing platform. The security is guaranteed even if the cloud server is hacked since data confidentiality is now protected by cryptographic encryption algorithms. The advantage of the proposed system is the infrastructure security is guaranteed even if the cloud server is hacked. The disadvantage is There are some existing platforms for sharing real time video, they may not be able to achieve secure fine-grained sharing and secure searching simultaneously.
- Zhangjie Fu et.al, [14] proposed an efficient verifiable keyword-based semantic search scheme. Comparing to most of the existing searchable encryption schemes, the proposed scheme is more practical and flexible, better suiting user's different search intentions. Moreover, the proposed scheme protects data privacy and supports verifiable search ability, in the presence of the semihonest server in the cloud computing environment. The Advantages: Improves the flexibility and support verification of search results. Also it provides verifiable searchability with data privacy preserving. The

disadvantage is The trivial solution of downloading the whole encrypted data first and then decrypting it locally is obviously impractical, due to the huge bandwidth and computation burden.

- Jin Li et al, [15] proposed a new searching technique that is fuzzy keyword search. They focused on enabling effective yet privacy preserving fuzzy keyword search in Cloud Computing. To the best of knowledge, they formalize for the first time the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy.
- D. Boneh, G. D. Crescenzo et.al, [16] proposed a searchable encryption, in which anyone who has the public key can write to the data stored in server but with a restriction that only authorized users with private key can search. The major demerits of using public key are that it's very expensive in terms of computation. Additionally, in the public key setting, the privacy of keyword may possibly not be protected as the server possesses the ability to encrypt any keyword with the public key. As a result of this it can be used to receive the trapdoor in order to evaluate the cipher text. For achieving more efficient search, Curtmolaet al. single keyword search.

V. CONCLUSION

Thus the various encryption algorithms which are used for encrypting the data before uploading to the cloud server is discussed and the advantages and disadvantages in terms of security and cryptanalysis is listed out.

The various searching techniques available for selecting the required file from the cloud server through appropriate keyword search based on the user interest is analyzed and the pros and cons and the effectiveness of each method is listed.

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'00, Pages 44-55, 2000

[2] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, Report 2003/216, 2003, http://eprint.iacr.org/.

[3] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, and P. Paillier, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions," Journal of Cryptology, Volume 21, Number 3, Pages 350-391, 2008.

[4] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and Efficiently Searchable Encryption," in Proc. of Crypto 2007, Volume 4622 of LNCS. Springer-Verlag, 2007.

[5] J. W. Byun, D. H. Lee, and J. Lim, "Efficient Conjunctive Keyword Search on Encrypted Data Storage System," Lecture Notes in Computer Science, Volume 4043, Public Key Infrastructure, Pages 184-196, 2006.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption With Keyword Search," in Proc. of EUROCRYP'04, 2004.

[7] R. Zhang, and H. Imai, "Generic Combination of Public Key Encryption with Keyword Search and Public Key Encryption," Lecture Notes in Computer Science, Volume 4856, Cryptology and Network Security, Pages 159-174, 2007.

[8] N. Borisov, and S. Mitra, "Restricted Queries over an Encrypted Index with Applications to Regulatory Compliance," Lecture Notes in Computer Science, Volume 5037, Applied Cryptography and Network Security, Pages 373-391, 2008.

[9] H.-A. Park, J. W. Byum, and D. H. Lee, "Secure Index Search for Groups," Lecture Notes in Computer Science, Volume 3592, Trust, Privacy, and Security in Digital Business, Pages 128-140, 2005.

[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 of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, 2010

[11] R. Brinkman. "Different Search Strategies on Encrypted Data Compared. Data-Centric Systems and Applications," Security, Privacy, and Trust in Modern Data Management, Part 3, Pages 183-196, 2007.

[12] E. S. Ristad, and Peter N. Yianilos, "Learning String-Edit Distance," IEEE transaction on pattern analysis and machine intelligence, volume 20, number 5, 1998.

[13] Link-Assistant.com, "Stop Words: Words Ignored By Search Engines," Referenced online at http://www.link-assistant.com/seo-stop-words.html

[14] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving Keyword searches on remote encrypted data," in *Proc. of ACNS'05*, 2005.

[15] Keywords density analyzer referred from the URL http://www. keyworddensity.com/stop_words/

[16] Deepali D. Rane and Dr.V.R.Ghorpade " Multi-User Multi-Keyword Privacy Preserving Ranked Based Search Over Encrypted Cloud Data" International Conference on Pervasive Computing (ICPC), 2015.

[17] 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.

[18] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.

[19] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.

[20] Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL., NO.1,2015.

[21] Yanzhi Ren, Yingying Chen, Jie Yang, Bin Xie " Privacy-preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing" Globecom Communication and Information System Security Symposium 2014.

[22] Hongwei Li, Dongxiao Liu,Yuanshun Dai, Tom H. Luan, And Xuemin (Sherman) Shen "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", December 2014.

[23] Mikhail Strizhov and Indrajit Ray "Multi-keyword Similarity Search Over Encrypted Cloud Data" International Conference on Pervasive Computing (ICPC), 2012.

[24] E.-J. Goh, **"** Bloom filters in order to construct the indexes for the data files" IEEE Conference on Computer Communications 2016.

[25] Jun Zhou, Zhenfu Cao, Xiaolei Dong and Xiaodong Lin "More Efficient Verifiable Outsourced Computation from Any One-way Trapdoor Function" IEEE ICC - Communication and Information Systems Security Symposium, 2015.

[26] Fanyu Bu, Yu Ma, Zhikui Chen and Han Xu "Privacy Preserving Back-Propagation Based on BGV on Cloud" 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on

Embedded Software and Systems (ICESS).

[27] Joseph K, "Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud" 2015.

[28] Zhangjie Fu, *Member*, IEEE, Jiangang Shu, Xingming Sun, and Nigel Linge "Verifiable Keyword-based Semantic Search over Encrypted Cloud Data" IEEE Transactions on Consumer Electronics, Vol. 60, No. 4, November 2014.

[29] 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, San Diego, CA, USA, March 2010.

[30] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, IEEE Conference on Computer Communications 2004.