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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

A Survey on Searchable Encryption Techniques for Efficient Data Searching Over CloudData

Ms. Priya A. Pande, Dr. Emmanuel M.

M.E. Scholar, Department of Information Technology, Pune Institute of Computer Technology, Pune, India.

Professor, Department of Information Technology, Pune Institute of Computer Technology, Pune, India.

ABSTRACT: Cloud computing is one of the preferred options in today's enterprise and it is widely accepted by end users and business consumers. Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers. Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. With the increasing number of documents stored in cloud, searching for the desired document can be a difficult and resource intensive task. Searching for string is a multi keyword search where the ordering of keywords is preserved. So in addition to the presence of all these keywords in a document, their ordering and adjacency are to be taken care off while searching.

KEYWORDS*:* Searchable Encryption, Multi-keyword search, Cloud Security, Cryptography, Cloud Storage

I. INTRODUCTION

Cloud Computing is the common buzzword in today's Information Technology. Cloud computing platforms are rapidly emerging as the preferred option for hosting applications in many business contexts. An important feature of the cloud that differentiates it from traditional services is its apparently infinite amount of resource capacity (e.g. CPU, storage, Network) offered at a competitive rate. It eliminates the need for setting up infrastructure which takes several months. With the rapid development of cloud computing, cloud storage has enabled the provision of high data availability, easy access to data, and reduced infrastructure costs from outsourcing of data to remote servers. Many users prefer cloud storage services to relieve the burden of maintenance costs as well as the overhead of storing data locally. Moreover, users are able to access their data from anywhere and at any time instead of having to use dedicated machines. Encryption protects data Amongst these, the service provider is unable to process the encrypted data as freely and efficiently as it can plaintext data, making access cumbersome for the data owner. To address the difficulty of retrieving encrypted text efficiently, increasingly practitioners turn to searchable encryption. An SE scheme encrypts a set of documents in a way that allows the data owner to delegate search capabilities to the provider without decrypting the documents. However many user believe that encryption of data before outsourcing provide a strong guarantee that the data privacy would be maintain against the cloud service providers. Encryption is an easiest route to keep the privacy of the data. On another side search operation on such data is very challenging task. Previously searching is suitable for only unencrypted data which does not offers security over cloud hence encryption of data came into existence and to search over such encrypted data is challenging task. Whenever cloud user store their data in third parties cloud system though it will cause security issues to confidentiality of their data. Data hiding techniques provide protection to data secret but it has some restriction to provide some functionality because some operations don't support over hidden information.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

There is a large amount of increase in cloud users because of the storage efficiency and availability of simple computational models in the cloud. It causes a huge amount of information is being added into cloud servers. So the finding required document file into this bulk of information is the most challenging and time consuming task. Searching and retrieving specific document over encrypted data is not much easier task. Data is in encrypted forms only so while retrieving such encrypted file user is forced to search in encrypted form only. It causes the data retrieval time efficiency problem. It is unreliable to access files without any relevance, although it affects the cost of computation. Overall there is need of advance efficient ranked search method to obtain the efficiency in ranked searching over encrypted data; the query can be formed using multiple keywords so that we can achieve required relevant data.

In a Cloud environment, cryptography is typically utilized for two purposes: security while data is at rest; and security while data is in transit. Unfortunately the Cloud cannot guarantee the security of data during processing as the current limitations of cryptography prevent data from being processed in encrypted form. Given the fact that data is processed in unencrypted form, it is quite common for attackers to target data in use, rather than targeting data which is encrypted during storage and transit. An entity wishing to store its data within the Cloud must choose to (1) Store Data in Encrypted Form or Store Data in Unencrypted Form. If storing data in encrypted form then 2 Options exist which are to 1. Disclose Decryption Key(s) to Cloud Service Provider (CSP) or 2. Keep Decryption Key(s) Private. SSE represents one of the few forms of Searchable Encryption that is achievable using established standardized encryption algorithms. Alternative forms of Searchable Encryption require the use of non-standardized, special purpose encryption algorithms. Solutions exist to eradicate and obfuscate all forms of Information Leakage in SSE; however existing solutions have a significant effect on the search efficiency of SSE.

II. RELATED WORK

Searching for string is a multi keyword search where the ordering of keywords is preserved. So in addition to the presence of all these keywords in a document, their ordering and adjacency are to be taken care off while searching. This scheme works in two phases, each taking one round of communication. In the first phase these documents are identified which contains all words occurring in the phrase. In the second round the candidate documents are checked to confirm the existence of the phrase. Yi Yangy, Hongwei Liy[5] proposed the secure k-nearest neighbor is leveraged for a secure dynamic searchable symmetric encryption scheme. With the development of cloud computing, data sharing has a new effective method, i.e., outsourced to cloud platform. Encrypting the data before outsourcing is a commonly used approach, where the data owners only need to send the corresponding encryption key to the authorized users. However, in such approach it is difficult to use the data since the encrypted data obsoletes comprehensive search functionalities of plaintext keyword search. The scheme can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in Dynamic Searchable Symmetric Encryption (DSSE) area. In addition, the performance of proposed scheme is evaluated compared with other DSSE schemes. The comparison results demonstrate the efficiency of our proposed scheme in terms of the storage, search and update complexity.

Authors[2] proposed the notion of Multi-Data-Source SSE (MDS-SSE), which allows each data source to build a local index individually and enables the storage provider to merge all local indexes into a global index afterwards. Cloud computing has greatly facilitated large-scale data outsourcing due to its cost efficiency, scalability and many other advantages. Searchable Symmetric Encryption (SSE) is an advanced cryptographic primitive addressing the above issue, which maintains efficient keyword search over encrypted data without disclosing much information to the storage provider.Also, a novel MDS-SSE scheme is proposed, in which an adversary only learns the number of data sources, the number of entire data files, the access pattern and the search pattern, but not any other distribution information such as how data files or search results are distributed over data sources.

An efficient and easy-to-implement symmetric searchable encryption scheme (SSE) is proposed by Indranil Ghosh Ray[1] for string search, which takes one round of communication, O(n) times of computations over n documents.The cloud is designed to hold a large number of encrypted documents. With the advent of cloud computing, growing number of clients and leading organizations have started adapting to the private storage outsourcing. This

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

allows resource constrained clients to privately store large amounts of encrypted data in cloud at low cost. However, this prevents one from searching. This gives rise to a newly emerging field of research, called searchable encryption (SE). SE can be classified into symmetric searchable encryptions (SSE) and asymmetric searchable encryptions (ASE). In the SSE, the client encrypts the data and stores it on the cloud.The hash-chaining technique instead of chain of encryption operations is proposed for index generation, which makes it suitable for lightweight applications.

A secure multi-keyword ranked search scheme over the encrypted cloud data is proposed in this paper[4]. Such scheme allows an authorized user to retrieve the most relevant documents in a descending order, while preserving the privacy of his search request and the contents of documents he retrieved. Advances in cloud computing and Internet technologies have pushed more and more data owners to outsource their data to remote cloud servers to enjoy with huge data management services in an efficient cost. To keep the confidentiality of their sensitive data, data owners usually outsource the encrypted format of their data to the untrusted cloud servers. Several approaches have been provided to enable searching the encrypted data. However, the majority of these approaches are limited to handle either a single keyword search or a Boolean search but not a multi keyword ranked search, a more efficient model to retrieve the top documents corresponding to the provided keywords. To do so, data owner builds his searchable index, and associates with each term document with a relevance score, which facilitates document ranking. The proposed scheme uses two distinct cloud servers, one for storing the secure index, while the other is used to store the encrypted document collection.

Shaun Mc Brearty [3] proposed SSE Inverted Index Technique for Storing Encrypted data on Cloud Server. In a Cloud environment, cryptography is typically utilized for two purposes: security while data is at rest; and security while data is in transit. Unfortunately the Cloud cannot guarantee the security of data during processing as the current limitations of cryptography prevent data from being processed in encrypted form. New techniques such as Searchable Encryption are being deployed to enable data to be encrypted online. Searchable Encryption is now at the point that it can be deployed and used within the Cloud. In the Cloud, Searchable Encryption has the ability to allow CSP customers to store their data in encrypted form, while retaining the ability to search that data without disclosing the associated decryption key(s) to CSPs that is, without compromising data security on the Server. In the case of constructing an IR Inverted Index, the results show that the time taken to generate an IR Inverted Index is directly proportional to the number of Terms contained in the underlying Document Collection. Converting the same IR Inverted Index to an SSE Inverted Index is directly proportional to the number of Postings contained within the IR Inverted Index, while the time taken to encrypt the underlying Document Collection is directly proportional to the number of Terms contained within the Document Collection. An SSE scheme is present and evaluate the efficiency of storing and retrieving data from the cloud. The results showed that carrying out a task using SSE is directly proportional to the amount of information involved.

Authors [9] proposed a tree based ranked multi-keyword search scheme for multiple data owners (TBMSM). With the development of cloud storage, more data owners are inclined to outsource their data to cloud services. For privacy concerns, sensitive data should be encrypted before outsourcing. There are various searchable encryption schemes to ensure data availability. Specifically, by considering a large amount of data in the cloud, the TF_IDF model is utilized to develop a multi-keyword search and return the top-k ranked search results. To enable the cloud servers to perform a secure search without knowing any sensitive data (e.g. keywords and trapdoors), we construct a novel privacy-preserving search protocol based on the bilinear mapping. To achieve an efficient search, for each data owner, a tree-based index encrypted with an additive order and privacy-preserving function family is constructed. The cloud server can then merge these indexes effectively, using the “Depth first Search” algorithm to find the corresponding files.

The challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE) is solved in this paper[10]. For the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. A set of strict privacy requirements for such a secure cloud data utilization system is established. Among various multi-keyword semantics, the efficient similarity measure of “coordinate matching,” i.e., as many matches as

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

possible is chosen, to capture the relevance of data documents to the search query. Further "inner product similarity" to quantitatively evaluate such similarity measure is used. A basic idea for the MRSE based on secure inner product computationis proposed, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given.

III. ALGORITHMS

The problem of searching over encrypted data has become an important issue in security and cryptography. To achieve the confidentiality, data is stored in encrypted form on cloud storage. But, it is difficult to perform any operation on encrypted data. User need to download the encrypted data, and then decrypt it and performs operation on it. The resulting data need to be encrypted and uploaded on the cloud. Searching on encrypted data is a major issue in cloud. There are several solutions for searching over encrypted data are listed below.

1. Practical technique for search over encrypted data

In this technique, pseudo random function, pseudo random generator and sequential scan is used. It supports controlled searching, query isolation and hidden searches. The main objective of their work is: 1. Un-trusted server cannot able to search for arbitrary keywords without the user authorization. 2. Un-trusted server cannot learn anything more about the plaintext than the search result. 3. It supports hidden queries so that user may ask the un-trusted server to search for a secret word without revealing the word to the server. The scheme is efficient, secure and practical and has no communication overhead. However, the sequential scan is not efficient if data size is large and also too slow in searching for a large number of documents. If we search frequently, server may be learned some information.

2. Searchable Symmetric Encryption:

Searchable symmetric encryption scheme use symmetric encryption which provides searching capabilities over encrypted data. An approach to provisioning symmetric encryption with search capabilities is called as secured index. An index is a data structure that stores document collections. User indexes and encrypts its document collection and sends the secure index together combine with encrypted data to the server. To search for a keyword, user generates and sends a trapdoor for that keyword to the server. The server uses the trapdoor to perform the search operation and recover pointers to appropriate document. The main objective of their work is: 1. Symmetric searchable encryption can be achieved in its full generality. 2. Any types of queries can be performing over encrypted data. This technique is more efficient and guarantees more security than previous schemes. But, this scheme not suitable for large scale data and support only single user. Searchable encryption scheme with cryptographic cloud storage can accomplish the essential security requisite of the cloud storage.

3. Public Key Encryption with a Keyword Search

In this scheme, document is encrypted using public key by the people who wants to store it in the un-trusted server. But the valid user can generate keyword trapdoor with the help of his private key can search over those encrypted data.For example, there are three entities which are data owner, user and server.A server is a cloud system who stores data and conducts searches, while data owner can be anyone who wants to share encrypted data under an authorized user's public key. Authorized user can query the server with keywords to perform search over the data owner documents. Anytime the server wants to conduct a keyword search, it needs the authorized user sends a trapdoor which includes his/her private key and keywords information. With the help of trapdoor, the server can test whether the keyword is present in the document or not. If the keyword matches, then returns desire document to user.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

4. Multi-user Searchable Encryption

In MUSE, schemes are constructed by sharing the document's searchable encryption key with all users who can access it, and broadcast encryption is used to achieve coarse-grained access control. In Broadcast encryption scheme, a broadcaster encrypts a message for some subsets S of users who are listening on a broadcast channel. Any user in S can use his/her private key to decrypt the message. This scheme allows multiple users can search over encrypted data. The main problem in MUSE is, how to control which users can access which documents and how to reduce the number of shared keys and trapdoors is not considered.

5. Multi-key Searchable Encryption

A multi-user searchable encryption scheme allows data owner to share encrypted data to users with access right to search over those encrypted data. In a multi user application, the number of trapdoors is proportional to number of documents. That is, user requires submitting a multiple trapdoor in order to perform search on shared encrypted data. To overcome this problem, A Multi-key searchable encryption scheme allows a user to search over shared data using a single keyword trapdoor instead of a multiple keyword trapdoor in the server.

6. Key Aggregate Encryption for Data sharing

In this scheme, data owner generates an aggregate key for the user to decrypt all the documents. To allow a set of documents encrypted by different keys to be decrypted with a single aggregate key, user could encrypt a message not only under a public-key, but also under the identifier of each document. The data owner holds a master-secret key, which can be used to extract secret keys for different classes. The extracted key can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys.

7. Boolean Keyword Searchable Encryption Scheme

It provides a solution to efficient ranked keyword search problem. As a result by using this technique Encrypted data which is stored remotely utilized effectively in cloud computing. It focuses on effective searching and secures ranked keyword searching over encrypted data. keyword searching is done using SSE technique. TF x IDF rules are used for ranking function. OPSE cryptosystem is proposed for security purpose.

8. Fuzzy Keyword Searchable Encryption Scheme

A technique which solves problem of maintaining keyword privacy and fuzzy keyword search over encrypted cloud data is done effectively. In this, the wildcardbased scheme is used for fuzzy keywords search. system utilization improved by using Fuzzy keyword search. Here keywords are predefined .these predefined keywords matched with returned files. as a result, efficiency is obtained while retrieving the file.

9. Plaintext Fuzzy Keyword Searchable Encryption Scheme

Multiple users conveniently search ciphertexts using this technique by Probabilistic public key system. This system provides the multi-keyword search with the fuzzy search. A hash function is used to provide an index of keywords which has been searched. This hash function provides protective fuzzy search.

10. Conjunctive Keyword Searchable Encryption Scheme

Scheme which supports queries with conjunctive keyword over encrypted data. Boolean keyword search problem is solved by this scheme. It proposed secure cloud model for Conjunctive keyword encrypted data search. In this paper it defines two techniques first technique defines communication cost over no. of documents whose security is

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

provided by using the Decisional Diffie-Hellman (DDH) assumption. Second technique defines communication cost on no. of keywords whose security dependable on hardness assumption.

11. Ranked Keyword Searchable Encryption Scheme

It provides the solution to the problem of supporting efficient ranked keyword search, to achieve effective utilization of encrypted data which is stored remotely in cloud computing.it denotes that using existing searchable encryption scheme there is difficulty in achieving efficiency in ranked search. This causes the security issue, to provide the solution to this problem it derives an efficient one-to-many order-preserving mapping function which provides effectively searchable encryption scheme.it gives direction to work on ranked keyword search over encrypted data basically on multiple keywords.

IV. COMPARISION OF DIFFERENT SEARCHABLE ENCRYPTION TECHNIQUES

Sr No.	Technique	Process used	User	Advantage	Disadvantage
1	Practical Techniques	Pseudo, Random, function, Sequential scan, Cryptographic scheme	Single user	Controlled and hidden search. Query isolation is supported. Easy and fast.	Sequential scan is not efficient to the large data size. Overhead occurs in Storing and updating the index.
2	Searchable Encryption Scheme	Symmetric Public Key Encryption	Single user	Secure Search employed over encrypted data on cloud	Costly in terms of Computation
3	Public Key Encryption Scheme	Public key & Private key Encryption	Single user	Provides better security	Increases the number of keys which makes a system complex
4	Multi-user Searchable Encryption	Broadcast Encryption Scheme	Multi user	Multiple users can search over encrypted data using single key	Control over users to access documents and reduce the number of shared keys and trapdoors is not considered
5	Multi-key Searchable Encryption	Provides Secure Index structure, generates Secret Trapdoors	Multi user	Documents confidentiality and privacy of Index, Trapdoor, Trapdoor unlinkability.	CSPs that keep the data for users may access users sensitive information without authorization.
6	Key Aggregate encryption for data Sharing	Single Aggregate key	Multi user	Reduce the number of distributed data encryption keys	Does not support search over encrypted data
7	Boolean Keyword Searchable Encryption Scheme	Boolean keyword Search using Boolean operators AND, OR and NOT.	Multi user	Comfortable enough to express small, Easy information needs	Excess network traffic. efficient document ranking is not supported.
8	Fuzzy Keyword Searchable Encryption	Wildcard-based Technique	Multi user	Eliminates the requirement for enumerating all the	Supports only Boolean keyword search. Huge storage complexity

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

	Scheme			fuzzy keywords	
9	Plaintext Fuzzy Keyword Searchable Encryption Scheme	Plaintext Searching, String matching algorithm	Multi user	To find relevant information asit allows user to search using Try and-See approach	Statistics and dictionary attacks and fails to attain the search privacy.
10	Conjunctive keyword Searchable Encryption Scheme	Decisional Diffie Hellman (DDH) and Hardness assumption	Multi user	Solution to Boolean Keyword Search problem	Privacy overhead
11	Ranked Keyword Searchable Encryption Scheme	Secure Searchable Index, Order-Preserving Mapping function	Multi user	Enhances system usability by returning the matching files in a ranked order concerning to certain relevance criteria. eliminate excess network traffic	Compromise the privacy

Table 1 :Comparison of different searchable techniques

V. CONCLUSION

In this paper, the brief survey on various strategies for searching encrypted information over a cloud is done. Nowadays, everyone uses cloud services to outsource their private data via public cloud storage because of many advantages over traditional method. To ensure privacy of outsourced data, user encrypts their private data before uploading to cloud so that server doesn't know anything about the data. But, how to efficiently share selectively encrypted data with valid users and how the server can perform search operation without knowing the user data. Several searchable encryption techniques are analyzed based on single keyword, Boolean keyword, fuzzy keyword, conjunctive keyword, multi-keyword, search based on similarity measures, attribute-based search etc. The majority of strategies has drawback with them that is they are taking longer time to search the information also they are facing some privacy issues, while multi keyword search techniques supports more privacy and efficient retrieval of data. Therefore, a major analysis is important which will provide privacy and minimize the searching time over encrypted information in the cloud.

REFERENCES

[1] Indranil Ghosh Ray, YogachandranRahulamathavan ,MuttukrishnanRajarajan, "A New Lightweight Symmetric Searchable Encryption Scheme for String Identification", IEEE Transactions on Cloud Computing, Vol. 66, No 2, 2018
[2] Chang Liu, LiehuangZhu, Jinjun Chen, "Efficient Searchable Symmetric Encryption for Storing Multiple Source Data on Cloud" , IEEE Transactions on Cloud Computing, Vol. 32, No 3, 2015.
[3] Shaun Mc Brearty, William Farrelly, Kevin Curran, "Preserving Data Privacy with Searchable Symmetric Encryption", IEEE Transactions on Industrial Informatics, Vol. 54, No 2, 2016.
[4] Ayad Ibrahim, Hai Jin, Ali A. Yassin, Deqing Zou, "Secure Rank-ordered Search of Multi-keyword Trapdoor over Encrypted Cloud Data", IEEE Transactions on Services Computing, Vol. 45, No 3, 2012.
[5] Yi Yangy, Hongwei Liy, WenchaoLiuy, HaomiaoYaoy, Mi Wen, "Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost", IEEE Transactions on Information Forensics and Security, Vol. 23, No 2, 2014.
[6] Muhammad Naveed, Seny Kamara,Charles V. Wright, "Inference Attacks on Property-Preserving Encrypted Databases", Advances in Cryptology, ACM, Vol. 49, No. 655–670, October 12 - 16, 2015.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

[7] Mihir Bellare, Alexandra Boldyreva, Adam O'Neill, "Deterministic and Efficiently Searchable Encryption", Advances in Cryptology, Springer, Vol. 4622, No. 535–552, 2007

[8] David Cash, Joseph Jaeger, Stanislaw Jarecki, CharanjitJutla, Hugo Krawczyk, Marcel-CatalinRosu,"Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation", IEEE Transactions on Services Computing , Vol. 30, No. 2, February 2014

[9] Tianyue Peng, Yaping Lin, Xin Yao, Wei Zhang, "An Efficient Ranked Multi-Keyword Search for Multiple Data Owners over Encrypted Cloud Data", IEEE Transactions on Cloud Computing, Vol. 18, No. 2, March 2018

[10] Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou, "Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, January 2014

[11] David Cash, Jason Perry, Thomas Ristenpart, paul Grubbs, "Leakage-Abuse Attacks Against Searchable Encryption", Advances in Cryptology, ACM, October 12–16, 2015

[12] Arijit Karati, Ruhul Amin, SK Hafizul Islam, Kim-Kwang Raymond, "Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment Cho", IEEE Transactions on Cloud Computing, Vol.27, No 2, 8 May,2018

[13] Yinqi Tang, Dawu Gu, Ning Ding, Haining Lu, "Phrase Search over Encrypted Data with Symmetric Encryption Scheme", IEEE International Conference on Distributed Computing Systems Workshops, Vol. 18, No 2, 2012.

[14] C.Chu, S.Chow, W.Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014

[15] X. Song, D. Wagner, A. Perrig. "Practical techniques for searches on Encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55,2000

[16] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", Eurocrypt2004, pp.506C522, 2004