AN EFFICIENT SEARCH SCHEME OVER ENCRYPTED DATA ON MOBILE CLOUD

[1]Ms. Megha Desai **[2]Dr. Uttara Gogate**

[1]PG Scholar, Alamuri Ratnamala Institute of Engineering and Technology, Mumbai, India.
[2]Associate Professor, Shivajirao S. Jondhale College Of Engineering, Mumbai, India.

ABSTRACT

Cloud storage provides storage at a low cost. But users are concerned about issues like data privacy and security, which inhibit them from storing files on the cloud storage. We can secure data in the cloud by a simple and usual technique of encrypting the data and which later decrypted during file download. But encryption creates overhead on mobile devices. The mode of communication turns more complex while data retrieval from cloud storage to the user device. Mobile has limited bandwidth and battery which makes the encrypted search very challenging.

The proposed system with Traffic and Energy-saving Encrypted Search (TEES) algorithm is a bandwidth-efficient encrypted search in the mobile cloud. This proposed architecture offloads the computation, optimizes the communication between, and maintains the data privacy without degrading the performance of the mobile. TEES limits the computation time, saves energy consumption and network traffics while retrieving the files.

Keywords: Encrypted Search, Traffic and Energy-saving Encrypted Search (TEES), Mobile Cloud storage, Multi-Keyword Search, Query Processing.

I. INTRODUCTION

Cloud storage is a service model where data is managed, maintained, and backup remotely on a client-side. We have many cloud computing techniques for efficient accessing of data storage. A technique called cloud storage services is that we have to pay as we use. To reduce the cost of storage many providers use Dropbox and iCloud. This is a security breach as the cloud provider share data with outsiders and providers push under the high risk for privacy preservation. To address this problem of security, cryptography provides a primitive technique known as Searchable Symmetric Encryption (SSE).

The index storage is a centralized storage system that is built by the user and it constructs an index when data is lightweight or centrally stored. Most of the time, the users store their data in different data centers. In such cases, it becomes difficult to manage and users are unable to centralize the data and can have a searchable index. Personal data like chatting records are often stored in many devices like Laptops, Mobiles, and iPads and users cannot move all the data to one system. All the previous scenarios are not persistent with these data sharing schemes. So there is a need for SSE schemes that support multiple data sources which are referred to as multi-data source SSE. In this paper, we have proposed multi-keyword ranked searching techniques that are used while uploading and downloading the files. Query searching shows the final result using Cloud Computing Techniques based on multi keywords. The downloader can send the request to the service provider for downloading the file so the service provider checked the validity of the downloader, is it authentic users or not. If the downloader is valid users then the service provider provides the trapdoor keys which download the files.

Network traffic is nothing but the data traffic which occurs in the data packet in a network that is the amount of information that is transferred through the network. The proposed algorithm is based on sign in key fashion and trapdoor key generation which reduces the burden of network traffic. Therefore, we grow up with TEES as a component of mobile cloud storage applications. TEES fulfilling its privacy with high potential, by changing the keyword search written as an encrypted search platform, which has been requested in cloud storage systems. The trapdoor is a key generation and exchanging system which maintains the data privacy between multiple owners. We aim to improve data privacy preservation and reduce the burden of network traffic which can easily access the multiple files by our authorized users [1].

The energy consumption module is implemented for energy utilization over mobile data with encryption data. Every encrypted data have utilized more power while accessing the mobile data but the multiple keyword multi-data owners with trapdoor searching techniques reduce power consummation. So the proposed technique is more powerful as compared to the existing system which reduces the network overheads and bandwidth of the computing power, thus automatically reducing the energy consumption.

Thus the proposed encryption algorithm is more powerful as compared to the other algorithms. Also, Multi keyword searching techniques are explained in this paper for downloading the specified search result file by the requestor. The

Requestor searches the file using the multiple keywords on the cloud but the requestor cannot access this encrypted data without authentication of the user. The requestor can access the data without any disturbances only after getting permission from the user. Our paper mainly represents the concepts of privacy preservation while searching the data on the cloud. The algorithm proposed in this paper gives more accurate search results with multiple keywords which are explained in section VII.

II. EXISTING SYSTEM

Earlier cloud server has to perform different search techniques over the encrypted content such as - Boolean keyword search and Ranked keyword search. Rank keyword search sends all the matching retrieved files to the client based on the match of keywords whereas Boolean keyword search brings large network traffic. So, the Ranked keyword search is more efficient than a Boolean keyword search. Here in the above two approaches, all the data encrypted is downloaded, decrypted, and giving results to the client, which is not so efficient. Later on, conjunctive keyword searches have been proposed thus implement features like aggregation query computation and range query search but these methods all suffered from huge computation cost. No previous Boolean Keyword Search Encryption Scheme (BKSE) has supported multiple keywords ranked search, on the encrypted cloud content or data [2], [3]. Earlier cloud storage systems incurred challenges over traditional methods like limited computation and low battery and low data access.

1. There was huge leakage in the files which is nothing but a security problem.
2. A keyword is not isolated in encryption. The entire content is encrypted so that search is tough on the client-side. Earlier methods used costly calculated methods for calculation purposes; hardware at the server-side has a limited capacity for its storage and processing.

III. RELATED WORK

Many authors attempted to propose secure data and cloud storage services proposing various efficient algorithms. Some of the noticeable papers are discussed here.

The authors in [4] have suggested a secure cloud storage service that is designed to addresses the issue by showing optimal performance techniques. Here the third party is allowed to perform the public integrity verification. Data owners are unrestricted to do the work of checking data integrity periodically. The data owner is free from staying online as he was outsourcing the content. In this proposed paper an exact repair solution is addressed. There is no need for metadata to be generated for repaired data. Experimental results and performance analysis showed that designed service has less storage and communication cost. The advantage of this approach is faster data retrieval.

Some authors have introduced that Real-world data set was used and Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the “pay-as-you-use” cloud paradigm. Low communication overhead. In this stronger model, a cloud server is supposed to possess some background on the dataset, such as the subject and its related statistical information, in addition to what can be accessed in the known cipher text model. As an instance of possible attacks, in this case, the cloud server could utilize document frequency or keyword frequency to identify keywords in the query. The overall scheme is required by the trapdoor unlinkability requirement as well as the keyword privacy requirement. A static keyword searching scheme was used. No security of cloud data. [2]

The authors proposed a closer technique that is similar to our approach presented here, this method allows multi-keyword ranked search in the encrypted database. Here data owner distributes asymmetric key helped in trap door generation to authorized persons. This proposed work needs a keyword field in the index. Here, the user should list all the valid keywords and their corresponding positions surely for information to generate a query. The said approach may not apply to all cases. This may not be efficient as it has matrix multiplication operations for square matrices and the number of rows may be of several thousand and they also follow certain orders for every row [3].

The author has proposed an alternative for private key-word search using methods known as oblivious polynomial evaluation and Homomorphic encryption. The communication and computation cost of this proposed approach is as large as every search term. In this, a query uses several operations that depend on operations of Homomorphic encryption on server and the user side both. Wang et. al. recently proposed a work that allows ranked search in an encrypted database with the same or similar inner product. But this proposed work is limited to a single keyword only [1].

The authors have suggested Greedy Depth-first Search (GDFS) algorithm. Basic Dynamic Multi-Keyword Ranked Search (BDMRS) scheme by using the secure KNN algorithm also build the Index Tree algorithm was proposed. Here the authors stated that this method uses a single doc file with multiple keywords that were processed and a large number of keywords are processed [5].

Private Information Retrieval problem was introduced in [6]. Now in the recent past by Growth proposed a multi-query PIR method which followed a constant communication rate. PIR- based technique need to hide access patterns so, it uses costly cryptographic operations. This is an impossible task in a large scale cloud system. Privacy-preserving search is designed to hide the content of the retrieved data. Ogata and Kurosawa based on RSA blind signatures designed a privacy-preserving keyword search protocol. This PIR-based technique is used for every item in the database and every query, a public-key operation, and every operation is done on the user-side.

The authors in their paper [6] says that security is more from this technique when compared to previous searchable encryption approaches, It realizes the ranked keyword search. Cloud Computing is making sensitive information centralized to cloud-like emails, health records, financial data, etc. The data owners and cloud server may not be in a trustworthy domain and keep outsourced data that is not encrypted may be at risk. Cloud servers leak data to an unauthorized third party user. It needs to encrypt sensitive data before outsourcing enhancements made to ranked search schemes, with support of relevance score dynamics, the authentication is ranked and one-to-many order encryption preserving technique.

The authors suggested that the Web-based processing model which enables users to outsource their data to the cloud servers over the internet. A wild-card based technique with edit distance as the similarity metric to obtain fuzzy keyword sets. With symbol-based tries-traverse searching technique was used. [7].

IV PROBLEM DEFINITION

Mobile cloud has a large number of data users and the huge amount of documents in the cloud System, to access data through a network and Privacy Preservation is an important problem for mobile users. There is a need for multi-keyword search query and effective data retrieval methods. So, as to enrich the user searching, we need a ranking system with a trapdoor which is supporting multiple keywords search and encryption methods to give encrypted data.

Encrypt than sign key fashion is a data encryption technique which encrypts the key data in Sign key fashion.It was a difficult task for service providers to maintain data in sign fashion among the all data owners. The task of maintaining the validity of their secret keys for encryption and securing the data with different secret keys is challenging for data owners. If there are multiple data owners they should undergo enrolment and revocation techniques, so that our system revel in a multi-keyword, multi-owner search scheme over the mobile cloud system.

V. PROPOSED SYSTEM

In this multi-keyword trapdoor technology named traffic and energy-saving encrypted search scheme with Term Frequency-Inverse Document Frequency (TFIDF). Security calculation to cloud server has been offloaded for the energy consumption of mobile device this presented system is providing security to cloud storage from the information leak with good encryption a methods multi-keyword module used helps to get accurate results based on multiple keyword concept. Document vectors are first generated by combining the term frequency-inverse document frequency (TF-IDF) weight factor and the Trapdoor.

A. Traffic and Energy-saving Encrypted Search (TEES):

A novel approach MPS-SSE scheme is developed in the system. This model is efficient in the search time and also in terms of index term frequency size. This system is more secure and helps us to get rid of the chosen keyword attacks. Experimental results are checked with different types of data sets showing the efficiency of the scheme. In this research, the Traffic and Energy-saving Encrypted Search approach for cloud storage in mobile applications allow changing the ranked keyword search with the encrypted search platform in cloud storage systems. TEES is implemented with security features, but the security defects cannot be fully resolved. TEES block diagram shows encrypted search schemes. In this research TEES's architecture redesign was made over the traditional approach with encrypted search procedure. TEES uses the security calculation approach to the cloud which reduces the energy consumption of the complete process. TEES improves encrypted search procedure so, as to control the traffic when retrieving data from cloud storage that is encrypted. Along with traffic efficiencies and energy, security enhancement made with encrypted searches in TEES. The Architecture shows complete encryption and Decryption process which secure transfer the data from Data owner to User through the mobile cloud. Trapdoor key generation unit plays an important role which achieving data privacy preservation.

B. Architecture

In this multi-owner and multi-user cloud computing approach there are four entities- data owners, cloud server, the administration server, and lastly data users. The module Data owners have several files for efficient search operations and these

files are encrypted and on this TEES are built. The Proposed system has 3 modules were shown in Fig. 2.

1. Data Owner: Data owner data module is taking care of collecting documents, documenting the index and the last step is encrypting documents and outsourcing them.

2. Data User: New user's data get their authorization from the data owner before getting access to the data.

3. Cloud server: It allocates huge storage space and the resources for computation required by ciphertext search. After getting a request from the user, the server searches the encrypted index and sends documents matched the data user's query. This system protects data from leaking information also to the cloud server and also we improved the efficiency of ciphertext search. In our multi-user and multi-owner cloud model, the Data block is the data owner who has a collection of files. The Complete Operation is as shown in Fig. 1

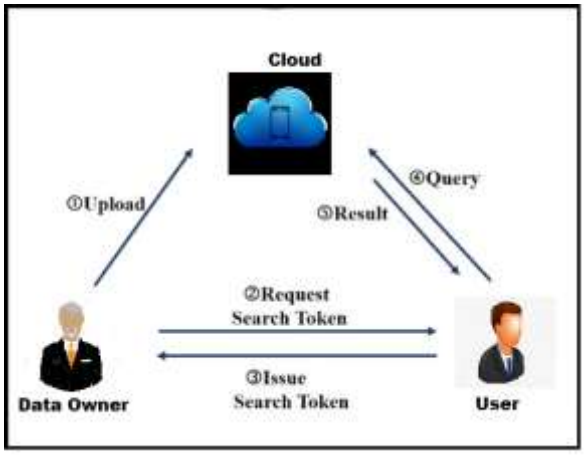

Fig.1 Operation between Owner and User

For efficient search operations, the files are encrypted and data owners build a searchable index on the keywords. The files are encrypted by the data owner sent to the administrator server where the administrator server re-encrypts files. Whenever the data owner wants to view files he is authorized by the administrator server. The cloud server encrypts the index files and makes some calculations and rank encrypted files. Whenever the data owner wants the encrypted data is retrieved from the cloud. The client is retrieving the encrypted file and is the data is decrypted at the client end. After all the operations are completed data is saved at the cloud end. So, in this way we are performing a multi-keyword ranked encryption search application is designed. This is a well-encrypted privacy-preserving multi-keyword search encryption approach.

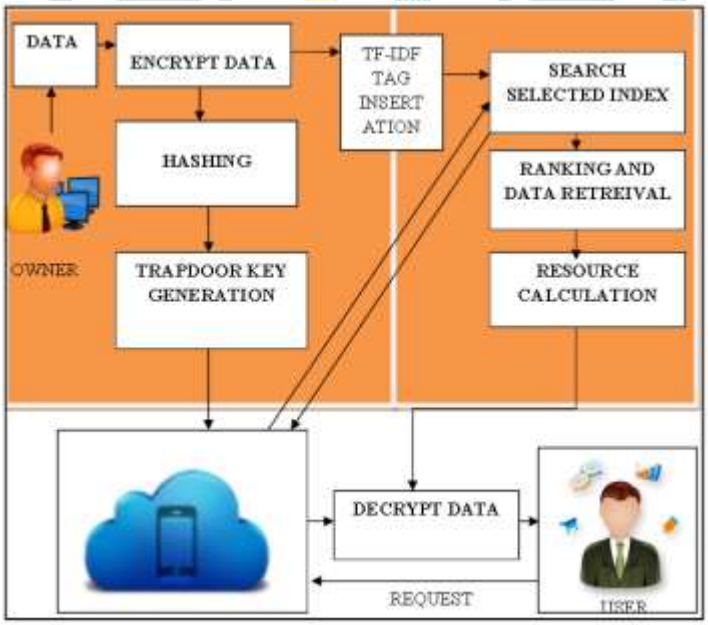

Fig. 2 Proposed Architecture

Key Generation: In this proposed module, the module Data Owner uses the Symmetric and Secret Key Based encryption algorithm on the AES algorithm. Initially, Data Owner types the Document name and enters the Keywords of Document. First data or documents are Encrypted based on Symmetric Key. Later Encrypt Keywords of the index based on Secret Key. Now Encrypted Documents with index are uploaded to Cloud Server. In the next module, the Search user selects a particular Data

Owner and send a Key Request. Then the user allotted with Symmetric and Secret Key by the Data Owner. When user Search Keywords, the search keywords are also Encrypted with Secret Key

Decrypt: Data user module can decrypt the documents. Decryption is done using a Symmetric Key.

D. ADVANTAGES OF PROPOSED SYSTEM

1. This proposed system's flexibilities are prompting both individuals and enterprises to convert complicated data to cloud administration.

2. Cloud Service provider is unaware of the original content and their data owner as data is encrypted it is more secure.

3. There is great purity in recommended or retrieved documents by the cloud.

VI. METHODOLOGY

The methodology used here is ranked search for proper use of outsourced cloud data as said in our model, this system design achieved both performance and security as given below.

1. **Multi-keyword Ranked Search:** Here the searching scheme is designed that allows multi-keyword query and provide effective data retrieval by giving results similarity ranking. Search Scheme on Mobile Cloud is encrypted and it returns undifferentiated results in this proposed research.

2. **Privacy-Preserving:** We restrict our cloud server from getting additional information from dataset or index we use encryption techniques and meet our security requirements or challenges.

3. **Efficiency:** all the above aims of the functionality of the system will follow or include all the privacy techniques with good encryption techniques and also reduce the overhead cost of our computation.

Here we have to use base64 decoder for file contents encryption that encrypted contents were uploaded on the cloud. This is one of the security processes which provide contents security of the cloud. It has a 64-bit decoder that shuffles the bit by bit correction. We have used most keywords

VII. ALGORITHM DESCRIPTION

Algorithms can perform automated reasoning, calculations, and processing data tasks. An algorithm is expressed within a finite amount of space and time and it defines a language to calculate a function. For encryption, we used Advanced Encryption Algorithm (AES) with a 256-bit encoder and decoder.

Algorithm-1: AES

Algorithm: Advanced Encryption Standard (AES)
Step-1: Initialize the Block of data And Initial Key Value.
Step-2: the initial key is added to the block using an XOR ("exclusive or") cipher, which is an operation built into the processor.
Step-3: Each byte of data is substituted with another; we have used 256-bit length and used 4*4 array for Shifting.

a) The rows of the 4x4 array are shifted, bytes in the second row are moved one space to the left, bytes in the third row are moved two spaces, and bytes in the fourth are moved three.
b) The columns are then mixed a mathematical operation combines the four bytes in each column

Step-4: The Secret key is added to the block (much like the initial key was), and Repeat Step-2 until the data block is empty.
Step-5: For AES decryption, the same process is carried out in reverse.

AES consist of block ciphers like AES-128,192 and 256. To encrypt/decrypt a block of messages; AES-128 will use a 128-bit key length. The key length depends on block cipher AES-192 uses a key bit length of 192 and AES-256 is using a key bit length of 256. Symmetric ciphers use a similar key for both encrypting and decrypting data, the sender and the receiver both use the same secret key. 128-bit keys have 10 rounds, 192-bit keys have 12 rounds, and 256-bit have14 rounds for keys. Every round has several processing steps like substitution, transposition, etc. Lastly plaintext converted to Cipher text. AES encryption algorithm has several transformations that need to be done on stored data in an array. The first and initial step of the cipher is to keep data in an array and later cipher transformations are performed in rounds. The total number of rounds is decided by key length like 128-bit keys have 10 rounds, 192-bit keys have 12 rounds and 256-bit keys have 14 rounds. The first step in

transformation is the substitution of data and the second step in transformation is to shift the data rows and the third is to mix columns. The final transformation is exclusive or operation done on every column using an encryption key.

VIII. PERFORMANCE ANALYSIS

The Performance Analysis of given keywords based on Time required in seconds (X-axis) against the number of given keywords on (Y-axis) is shown in Fig. 3. Time analysis varies with variation in the total number of keywords.

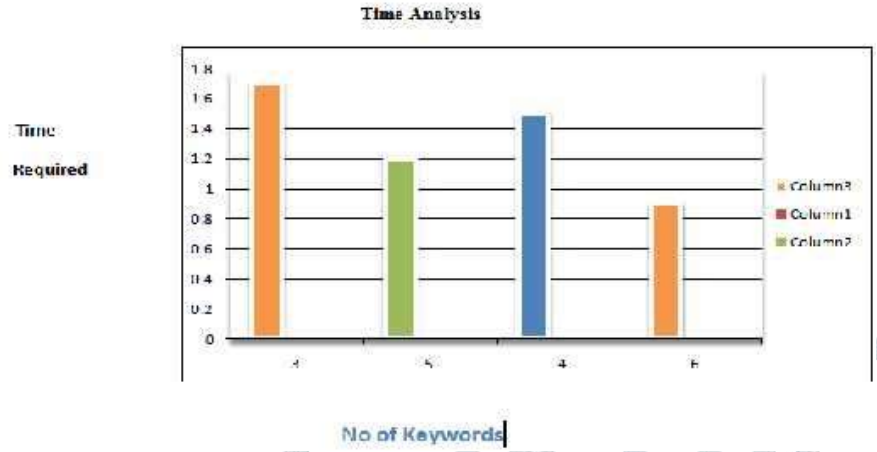

Fig. 3: Time Analysis With Given Keywords

Performance analysis based on the time required and the total number of documents are shown in Fig. 4. Time analysis varies with varying document sizes when compared with the existing systems. It gives better results in less time when compared with a single keyword search model.

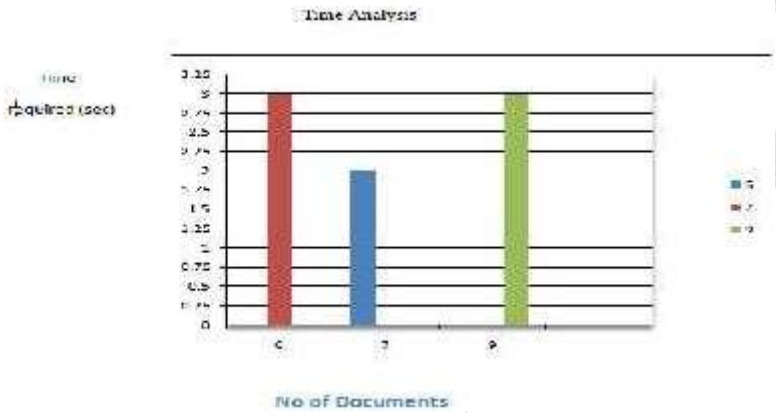

Fig. 4 Time Analysis With Given Number of Documents

IX. CONCLUSION

In an efficient search scheme over encrypted data on the mobile cloud, we have tried to give a solution to the problem of a secure ranked multi-keyword search performed on the remote encrypted database where all users are getting protection against security violations. Initially, the security requirements for the given problem are well defined. Secondly, secure usage of the total number of keywords searched is relatively limited and there are by trapdoor system which is generated by the data owner. The efficiency of the scheme increased with the usage of the symmetric-key encryption technique. This proposed method solves all the security requirements in the Cloud. Thus this proposed ranking method very well retrieves relevant documents related to our submitted search terms.

All the mentioned schemes have experimented and their results have demonstrated compared with the effectiveness of our proposed system. TEES was implemented for the energy-efficient encrypted keyword search on cloud storage. TEES approach is time and energy-consuming when compared with keyword searches within the plain- text. Our work can be further expanded to more new implementations. In our model, we proposed a multi-keyword search scheme for making the encrypted

search of data. We have possible extensions to our current work which are still to be implemented. But, there are certain problems such as time and cost for index tree building and so on, which are not yet implemented. We are planning to explore multi-keyword semantics over encrypted data.

REFERENCES

[1] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y.T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ACM, 2013.

[2]Ning Cao, Cong Wang**,** Ming Li, Kui Ren " Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, Volume: 25, Issue: 1, Jan. 2014.

[3] N. Cao, C. Wang, and M. Li, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distribute. Syst., vol. 25, no. 1, pp.222-233, 2014.

[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," Proc. of the IEEE Symposium on Security and Privacy. Oakland, USA, pp.44-55, May. 2000.

[5] Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data" IEEE Transactions on Parallel and Distributed Systems, Volume: 27, Issue: 2, Feb. 1, 2016.

[6] J. Li, Q. Wang, and C. Wang, "Enabling efficient fuzzy keyword search over encrypted data in cloud computing," Cryptology ePrint Archive, 2009.

[7] Jin Li, Qian Wang, Cong Wang, Ning Cao, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing" 2010 Proceedings IEEE INFOCOM, 06 May 2011 1291450, **DOI:** 10.1109/ INFCOM.2010.5462196.

[8] Y. -C. Chang, and M. Mitzenmacher, "Privacy-preserving keyword searches on remote encrypted data," Proc. of ACNS, pp.391-421, 2005.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," J. Comput. Secure., vol.19, no.5, pp.895-934, 2011.

[10] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling Secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467-1479, Aug. 2012.

[11] K. Li, W. Zhang, C. Yang, and N. Yu, "Security analysis on one-to-many order-preserving encryption-based cloud data search," IEEE Trans. Inf. Forensics Secure., vol. 10, no. 9, pp. 1918-1926, 2015.

[12] S. Tahir, S. Ruj, Y. Rahulamathavan, M. Rajarajan, and C. Glackin, "A new secure and lightweight searchable encryption scheme over encrypted cloud data," IEEE Trans. Emerg. Top. Comput., vol. 99, no. 99, pp.1-1, 2017.

[13] D. Boneh, and B. Waters, "Conjunctive, subset, and range queries on encrypted data," Theory Cryptogr., pp.535-554, 2007.

[14] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multi-keyword top-k retrieval over encrypted cloud data," IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 239-250, 2013.

[15] Z. Fu, X. Sun, and Q. Liu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Trans. Commun., vol. 98, no. 1, pp.190-200, 2015.

[16] W. K. Wong, D. W. Cheung, and B. Kao, "Secure kNN computation on encrypted databases," In ACM Sigmoid International Conference on Management of Data New York, USA, pp. 139-152, 2009.