Innovative Science and Technology Publications

International Journal of Future Innovative Science and Technology,
ISSN: 2454- 194X Volume-4, Issue-2, May - 2018

IMPROVING RESULT ACCURACY WITH MULTI-KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA

J.Gayathri[1],V.Subashini[2]

[1]Assistant Professor, Vivekanandha college of Engineering for Women, Namakkal

[2]PG Scholar, Vivekanandha college of Engineering for Women, Namakkal

Corresponding author E-Mail-ID:subhacse1994@gmail.com

May – 2018

www.istpublications.com

IMPROVING RESULT ACCURACY WITH MULTI-KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA

J.Gayathri [1],V.Subashini [2]

[1]Assistant Professor, Vivekanandha college of Engineering for Women, Namakkal

[2]PG Scholar, Vivekanandha college of Engineering for Women, Namakkal

Corresponding author E-Mail-ID:*subhacse1994@gmail.com*

ABSTRACT: **Data privacy is a growing challenge in cloud computing, as the users data are uploaded on a third party cloud. To preserve data privacy for user uploaded data, the information is encrypted and stored in cloud server. When the user calls for data, it can be downloaded and decrypt from user side. Data encryption incurs high overhead, which make it necessary to find an efficient search scheme. Existing technique uses, single keyword search on encrypted data, in which user may or may not get his relevant document, thus he has to do search again or download all relevant file, which incurs high communication cost. To overcome this problem, we propose multi-keyword energy efficient search scheme handles the user query effectively and gets most relevant results to user, reducing the communication cost between cloud and user. Using this technique, privacy for user uploaded data is not degraded.**

Keywords- *Mobile Cloud Storage, Data Encryption, Energy Efficient, Traffic Efficient*

1. INTRODUCTION

Data owner encrypts and uploads data to cloud server, these data, which is stored as cipher text can be request and download by users. User who wants to download data from cloud server pose a query to cloud server, the query dealt in existing system is single keyword query, for which k-results are arrived, the results may not be much relevant to user and poses high communication cost.

However, mobile cloud storage system faces challenges over the traditional encrypted search schemes. As mobile cloud devices have limited computing and battery capacities, there is a need for suitable and efficient encrypted search scheme is necessary for MCS. The mobile cloud storage requires high bandwidth and energy efficiency for data encrypted search scheme, due to the limited battery life and payable traffic fee.

To overcome, these problems, we focus on the design of a mobile cloud scheme that is efficient in terms of both energy consumption and communication overhead, while keep meeting the data security requirements through wireless communication channels. To reduce high overhead, we propose an algorithm multi-keyword energy efficient search on encrypted cloud data.

2. LITERATURE SURVEY

In [1] HIDE: AP-Assisted Broadcast Traffic Management to Save Smartphone Energy in this paper, we improve Smartphone energy efficiency by reducing energy wasted on useless WiFi broadcast traffic. WiFi is a major source of energy consumption on Smartphone. For that problem we design a system, namely HIDE, to reduce smartphone energy wasted on useless WiFi broadcast traffic. In this process we found two method receive-all method and client-side method. Receive-all method AP forwards all broadcast. Client-side method the smartphone receives all UDP broadcast frame and it solution reduces the time that the system spends in active state Buffered broadcast/multicast frames are sent out with a special type of TIM called DTIM (Delivery Traffic Indication Map) Calculating broadcast flags will Right before transmission. It process to reduce energy wasted on smartphones

due to useless broadcast frames. Our system saves 71%-82% energy and the system on network capacity is less than 0.2%.

In [2] the author proposed a distributed cryptographic system that preserved the security of the document retrieval process and the high availability of the system. A single round trip encrypted search scheme is not secure and associated document information from multiple keyword searches. Single-keyword encryption search design utilize ranked keyword search, which network communication between the user and the cloud by transferring the computing weight from the user to the cloud. The ranked keyword search will return documents to the relevance score. It proposed a novel technique that makes the server side carry out the search operation. However, it should send many unrelated documents back and let the user filter them. EnDAS over the mobile cloud, which improves network traffic and search time efficiency compared with the traditional system.

In [3] this system we described and explain the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching". A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Data we assemble a special tree-based index structure. Propose a "Greedy Depth-first Search" algorithm to provide efficient multi keyword search, it deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme. Dynamic schemes have been planned to support inserting and deleting operations on document collection. This paper we suggest a secure tree-based search scheme over the encrypted cloud data, which supports MRSE and dynamic operation on the document collection. Advantage is Multi-keyword Ranked Search over Encrypted Cloud Data (MRSE).

In [4] this document the novel concept of Key-Aggregate Searchable Encryption (KASE) this scheme applies to any cloud storage that supports the searchable group data sharing functionality. First, a data owner only needs to distribute a single aggregate key to a user for sharing any number of files. The consumer needs to present a single aggregate trapdoor to the cloud. We first define a general framework of key aggregate searchable encryption (KASE) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. After provided that detailed constructions for the seven algorithms, we analyze the efficiency of the scheme, and establish its security through detailed analysis. And its advantage is describe both functional and security requirements for designing a valid KASE scheme.

In [5] this An Analysis of Power Consumption in a Smartphone paper Mobile consumer-electronics devices, particularly phones, are powered from batteries which are limited in size. Good energy management requires an excellent understanding of where and how the energy is used. We present this power breakdown for micro-benchmarks as well as for a number of reasonable usage scenarios. These results are validated by overall power measurements of two other procedures: the HTC Dream and Google Nexus One. Method Our advance to profiling energy consumption is to take physical power capacity at the component level on a piece of real hardware.

The power consumption of CPU and memory, rather than making comparisons between special platforms' algorithms, hence unity of the suite was not a relevant consideration. We have fundamentals to the experimental setup: the device-under-test (DuT), a hardware data acquisition (DAQ) system, and a host computer.

In [6] the Practical Techniques for Searches on Encrypted Datait is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. The method provides provable secrecy for encryption, in the sense that the entrusted server cannot study anything about the plaintext given only the cipher text. Our techniques have a number of crucial advantages. A pseudorandom permutation a block cipher. The algorithms we present are easy and fast (for a document , the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and

communication overhead, and hence are practical to use today. Our scheme is also very flexible, and it can easily be extended to support more advanced search queries. We end that this provides a powerful new building block for the construction of secure services in the untrusted infrastructure.

In[7] Efficient and secure ranked multi keyword search on encrypted cloud data in this paper Modern mobile device continue to approach the capabilities and extensibility of standard desktop PCs. Due to increasing then probability of cloud computing more and more data are stored in the cloud, data owner are approach to stored their data in cloud server for great convent and it will reduced management cost. Our data will be encrypted before stored in cloud for privacy purpose and it will retrieval based on keyword-based document. Search scheme to support dynamic operation like delete and insert the document. For the process we used two algorithm kNN algorithm and Greedy Depth-first Search algorithm. This algorithm is used to encrypt the index and query vector and also calculate the accurate relevance score. Another algorithm constructs the special tree-based index structure and to provide efficient search. .This approach is complex and resource intensive in both computation and power. The new model for mobile functionality is moved to an off-device network service. The file identifier algorithms and communications protocol with the network service are important, as the agent spends most of its cycles on those activities.

In [8] Secure and Energy Efficient Prefetching Design for Smartphones this method for greatly reduce energy consumption and data transmission. But the traditional prefetching systems cannot solve the security problem, in this problem we proposed SEEP to meet the security requirement of HTTPs connections and to save smartphone's energy consumption and data transmission. Informed Mobile Prefetching (IMP) is systems where developers the system can optimize for data, power, and performance based on a hint of the network object and the later action for this object. Security Design in Local Proxy have to achieve these goals, the local proxy includes four major components, i.e. connection redirector, context interpreter, request generator, and message forwarding. The SEEP system should not reveal the plaintext of the requests and responses to the remote proxy. Security Analysis will propose two security requirements: Confidentiality and Robustness. The SEEP can successfully reduce the energy and data cost of establishing connections and receiving responses.

In [9] Virtualized In-Cloud Security Services for Mobile Devices Modern mobile devices are face many of the same security threats as desktops. Belong the problem we introduce new model whereby mobile antivirus functionality is moved to an off-device network service employing multiple virtualized malware detection engines. The core of this approach is expending bandwidth to reduce on-device CPU and memory resources and thereby save power. Resource-intensive method of detecting malicious activity is through behavioral analysis. Scale of detect Algorithms the power overhead of the mobile manager in the worst case was greater the antivirus software, if only scanned for 284 threats, Cloud AV network service. Mobile threats increase, on-device engines and their signature databases will require more processing, storage, and power. Reduced on-device software complexity.

Modern threats have become particularly complicated, requiring complex antivirus software to detect and mitigate. The architecture that consists of two primary components: a lightweight host agent that runs on mobile devices, acquires files, and sends them into the network for analysis; and a network service that receives files from the agent and identifies malicious or unwanted content.

In [10] Mobile Cloud storage provides a large and scalable storage at low cost, but data privacy is a major concern that prevents users files. Because mobile device have limited bandwidth capacity and limited battery life so it will heavy overhead. It will offload the computation from mobile devices to the cloud to communication between the mobile clients and the cloud. We use traditional encrypted search schemes, in consideration of the limited computing and battery

capacities of mobile device we dedicate in the single-keyword search algorithm to provide secured and lightweight searchable encryption solution for mobile cloud storage and file sharing system design. TEES is slightly more time and energy consuming than keyword search over plain-text, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. And also it have some advantage it provides security for mobile cloud computing and it saves the energy levels and increases the performance.

3. PROBLEM STATEMENTS

Two categories of encrypted search methods exit

- Ranked keyword search and
- Boolean keyword search

The Ranked Keyword search adopts the relevance scores to represent the relevance of a file to the searched keyword and sends the top-k relevant files to the client. It is more suitable for cloud storage than the Boolean Keyword search approaches

Boolean Keyword search approaches need to send all the matching files to the clients, and therefore incur a larger amount of network traffic and a heavier post-processing overhead for the mobile devices. Single keyword search on encrypted data, the results may not be much relevant to user and poses high communication cost.

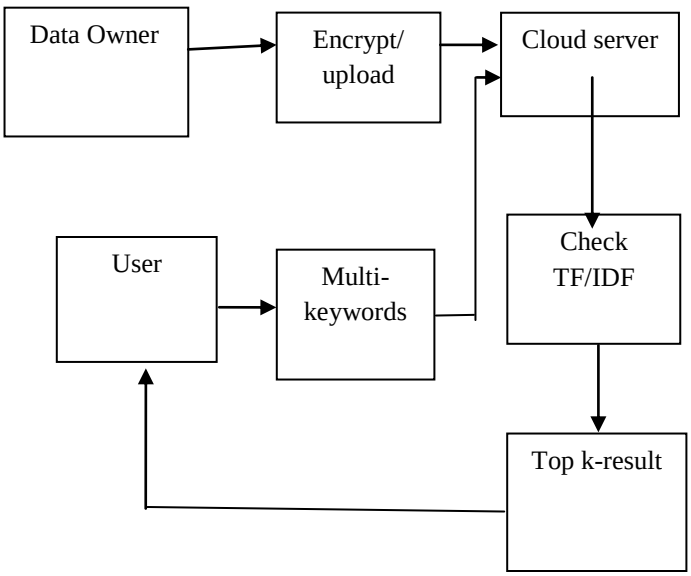
3.1 Disadvantages

- Boolean keyword search is not recommended for cloud data retrieval
- Single keyword search is implemented for data retrieval
- Query result may not be much efficient

4. PROPOSED SYSTEM

To propose Multi-Keyword Energy Efficient search (MKEE) architecture for mobile cloud storage applications. MKEE achieves the efficiencies through employing and modifying the ranked keyword search as the encrypted search platform basis, which has been widely employed in cloud storage systems. Ranked keyword search procedure is modified to save the energy consumption of mobile devices, and proposed scheme simplifies the encrypted search procedure to reduce the traffic amount for retrieving data from encrypted cloud storage. MKEE is implemented with security enhancement based on popular TF-IDF.

SYSTEM ARCHITECTURE



TF – Term Frequency

IDF – Inverse Document Frequency

4.1 MODULES DESCRIPTION

4.1.1 Data Owner

Data owner upload data to cloud server. Data owner encrypts the data using popular encryption algorithm such as AES (Advance encryption standard) converts to cipher text and upload to cloud server. Consider a file set F= (F1, F2 … FN) containing the number of F files, the keywords index is also get a input from data owner. A table is created to store the file id and its corresponding keywords. TF table as our index and the cloud server calculates the relevance scores using the encrypted TF values. The ranking function of the relevance scores will be introduced in the subsection dedicated to the cloud server.

4.1.2 Key Generation

When a user wants to access the file, he first sends his information to be authenticated by the data owner. The data owner sends the keys along with the hash table back if the user belongs to the legal set. This hash table will be used in the hash process. With use of key received from data owner, user can able to decrypt and view the data from cloud.

4.1.3 Multi Keyword Search

When an authorized data user wants to retrieve files, he needs to encrypt the corresponding query keyword w, and get the hash value h from the hash table. The query keyword is sent as multiple keywords from data user. This hash value is then sent to the cloud server and used to compute the relevance scores. The function decrypting the files corresponds to the encryption done by the data owner. The authentication function is used for authentication.

4.1.4 Mobile Cloud Storage

Note that the cloud server is Semitrusted, and the unwrap function can be processed by the server. Upon receiving the tuple Wrap(w) = (h1; h2), the server calls Unwrapto get user keywords, searches into the TF table, and then sends back the corresponding files. Cloud server calculates the relevance scores and return top-k relevant files according to the searching query from data user.

$$Score(Ws, Fc) = \sum_{w \in Ws} \frac{1}{|F_c|} \times (1 + \ln f_{c,w}) | \times \ln(1 + \frac{D}{f_w})$$

Ws is the keyword set to be searched; Fc is a certain file in the file set; fc,w denotes the TF of the keyword w in the file Fc; Fc is the total length of Fc; fw is the number of files containing the keyword w and D is the total number of files. Mobile Cloud Storage (MCS) provides storage solutions to mobile device users by enabling storage and retrieval of data on cloud through wireless communication. But, MCS incurs new challenges due to limitations of mobile devices in terms of computational capacity, battery life, bandwidth and payable traffic fee. Due to these limitations, encrypted search over mobile cloud results in huge processing overhead. TEES architecture is an initial attempt to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. TEES uses single keyword search scheme. Single keyword search produces a broad result set. Our methodology narrow down the result set by using multiple keyword search scheme. This improves the search result accuracy and enhances user searching experience. The methodology and implementation details are supported by the graphical results. The time complexity and battery consumption of mobile device is minimized for multiple keyword searches as compared to single keyword search.

4.2 Advantages

- Energy consumption is reduced by employing MKEE using relevance scores to the cloud server.
- Proposed system redistributes the encrypted index to avoid statistics information leak, and wraps keywords adding noise.
- Much relevant results using multi-keyword search.

5. Output

This section contains the screenshots of Owner register with all information, Owner login to the application, Data upload, encryption and decryption process, User login and checks the results from cloud admin. The Owner registers all information Fig 1.

Fig. 1 Owner registration page

In Fig 2 owner can login their application with their respected user id and password. Register owner will be login and upload there data.

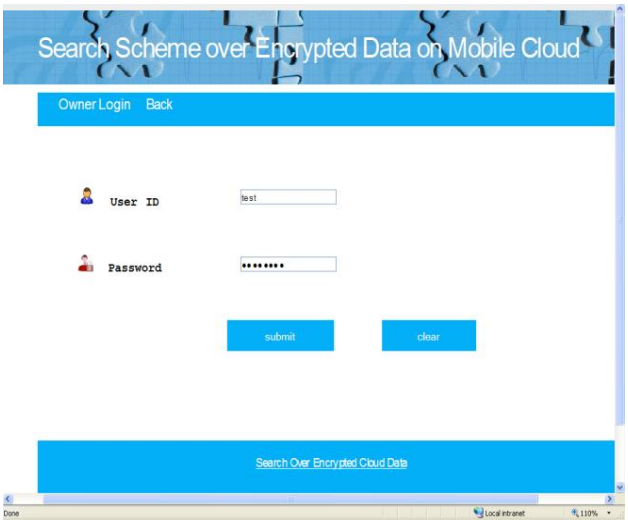


Fig 2 Owner login to the application

Owner uploads data to cloud server with public key and master key generated as random integer in Fig 3. In that owner can Browse there Document and upload there data in mobile code and data will encrypted.

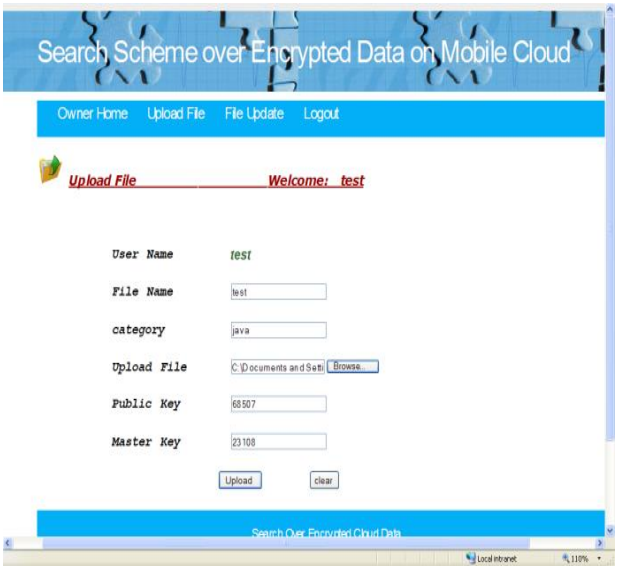


Fig 3 Owner uploads data to cloud server with public key and master key

Owner can update the outsourced data, data owner decrypt the data and update and uploaded the file in Mobile Cloud in Fig 4.

Fig 4 Owner can Update Uploaded there file

Next User register to cloud server, User provides all information to register in Fig 5. Without registration we cannot access.

Fig 5 User Register the detail

Fig 6 User login and access the application without username and password cannot access this application.

Fig 6 User login to access the application

User will search document with multiple keywords, uses of this multiple key words search process will easy, user can get most particular data and also energy efficient will be reduced Fig 7. At that time we will improve our result accuracy in cloud devices. We can reduce traffic and also improving energy band with.

Fig 7 User enter multi keyword search to cloud server

User login and check the results from cloud admin about the searching. User getting result with TF and IDF value from cloud admin in Fig 8.

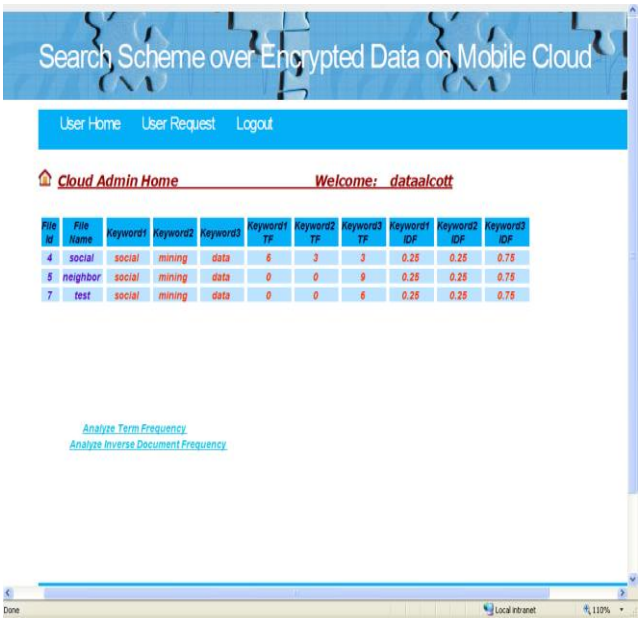


Fig 8 User getting result with TF and IDF value from cloud admin

5. PERFORMANCE ANALYSIS

This section illustrates the comparison between efficiency of keyword process and storage space required by existing system and Ranked keyword search & Boolean keyword search System. In Fig. 9 we have compared three different algorithms for keyword process.

The ranked keyword search adopts the relevance scores to represent the relevance of a file to the searched keyword and sends the top-k relevant files to the client. It is more suitable for cloud storage than the Boolean Keyword search approaches.

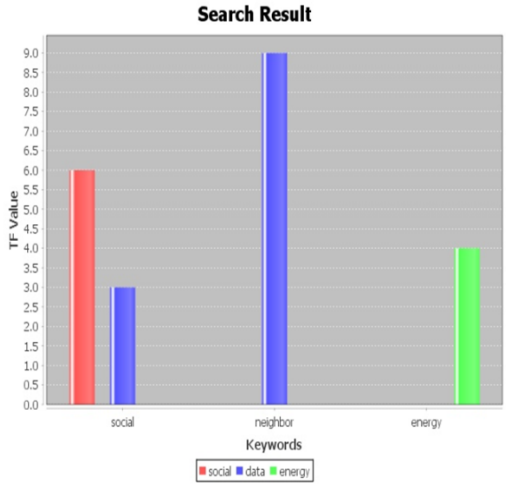


Fig. 9 we have compared three different algorithms for keyword process

In efficient multi keyword search requirement, the space required by MKEE achieves the efficiencies through employing and modifying the ranked keyword search as the encrypted search platform basis, which has been widely employed in cloud storage systems.

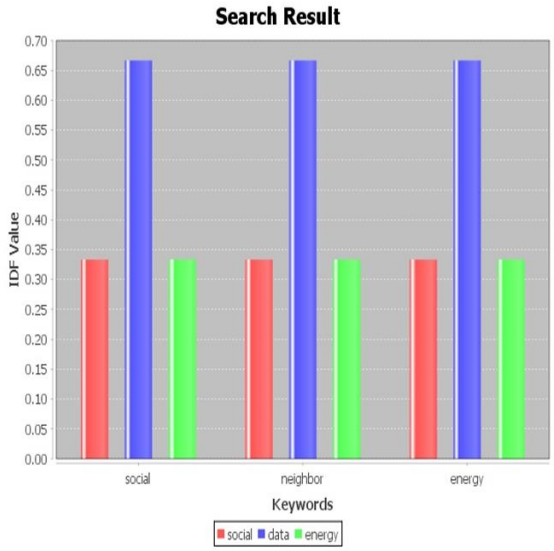


Fig. 10 MKEE is implemented with security enhancement based on popular TF-IDF

Ranked keyword search procedure is modified to save the energy consumption of mobile devices, and proposed scheme simplifies the encrypted search procedure to reduce the traffic amount for retrieving data from encrypted cloud storage. MKEE is implemented with security enhancement based on popular TF-IDF. Ranked keyword search is 15.6% improve the keyword search and Boolean keyword search System and 23.6% improve the keyword search. MKEE is implemented with security enhancement based on popular TF-IDF. Which is shown in the Fig. 10? It is because we search the file in location and compared the MKEE is implemented with security with database. And then the file is search keyword is unique. But in existing Systems the encrypted file is directly uploaded into Storage when its keyword value is unique. When a file is encrypted by different algorithms then it is possible to obtain two different key values for a single file. As a result, the policy based MKEE system eliminates nearly 32.8% of accuracy data.

6. CONCLUSION

Multi-keyword Energy Efficient search scheme (MKEE) is implemented as an initial attempt to create a traffic and energy efficient encrypted keyword search tool over encrypted cloud data. Developed an efficient implementation to achieve an encrypted search in a cloud data. The security study of proposed system shows that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency. MKEE is slightly more time and energy consuming than keyword search over plain-text, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level.

REFERENCES

[1] Ge Peng, Gang Zhou, David T. Nguyen, Xin Qi, Shan Lin, “HIDE: AP-assisted Broadcast Traffic Management to Save Smartphone Energy” 2016 IEEE 36th International Conference on Distributed Computing Systems 1063-6927/16 $31.00 © 2016 IEEE DOI 10.1109/ICDCS.2016.14.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[3] Baojiang Cui, Zheli Liu_ and Lingyu Wang,” Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage” IEEE TRANSACTIONS ON COMPUTERS, VOL. 6, NO. 1, JANUARY 2014.

[4] Dawn Xiaodong Song David Wagner Adrian Perrig "Practical Techniques for Searches on Encrypted Data", dawnsong, daw, perrig @cs.berkeley.edu University of California, Berkeley.

[5] A. Carroll and G. Heiser, "An analysis of power consumption in a Smartphone," in Proceedings of the 2010 USENIX conference on USENIX annual technical conference. USENIX Association, 2010, pp. 271–284.

[6] GAO Shang, PENG Zhe, XIAO Bin, SONG Yubo, "Secure and Energy Efficient Prefetching Design for Smartphone", IEEE ICC 2016 Communication and Information Systems Security Symposium 978-1-4799-6664-6/16/$31.00 ©2016 IEEE.

[7] C. O¨ rencik and E. Savas¸, "Efficient and secure ranked multikeyword search on encrypted cloud data," in Proceedings of the 2012 Joint EDBT/ICDT Workshops. ACM, 2012, pp. 186–195.

[8] "Virtualized In-Cloud Security Services for Mobile Devices" , Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, Farnam Jahanian Electrical Engineering and Computer Science Department University of Michigan, Ann Arbor, MI 48109 fjonojono, kaushikv, emcooke, jflinn, farnamg@umich.edu

[9] "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 71–82.

[10] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "Toward privacy assured and searchable cloud data storage services," Network, IEEE, vol. 27, no. 4, pp. 56–62, 2013.

[11] Ruhui Ma, Jian Li, Haibing Guan, Mingyuan Xia and Xue Liu, in the paper, "EnDAS: Efficient Encrypted Data Search as a Mobile Cloud Service" IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING.

[12] A.Miettinen and J. Nurminen, "Energy efficiency of mobile clients in cloud computing," in Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, 2010, pp. 21–28.

[13] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology- Eurocrypt 2004. Springer, 2004, pp. 506–522.

[14] A. Boldyreva, N. Chenette, Y. Lee, and A. O´ neill, "Order preserving symmetric encryption," Advances in Cryptology- EUROCRYPT 2009, pp. 224–241, 2009.

[15] K. Kumar and Y. Lu, "Cloud computing for mobile users: Can offloading computation save energy?" Computer, vol. 43, no. 4, pp. 51–56, 2010.

[16] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.