Research Manuscript Title

A SURVEY ON IMPROVING ENERGY EFFICIENT KEYWORD SEARCH OVER ENCRYPTED MOBILE DATA

V.Subashini[1]
PG Scholar
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.

Subhacse1994@gmail.com

J.Gayathri[2]
Assistant Professor
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.

jgayathrivcew@gmail.com

Sep – 2017

www.istpublications.com

A SURVEY ON IMPROVING ENERGY EFFICIENT KEYWORD SEARCH OVER ENCRYPTED MOBILE DATA

V.Subashini[1]
PG Scholar
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.
Subhacse1994@gmail.com

J.Gayathri[2]
Assistant Professor
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.
jgayathrivcew@gmail.com

ABSTRACT

Cloud is used as a storage platform to store various types of data. Within low cost it provides large, convened and scalable storage. Major drawback is Data privacy we prevent user from storing file in the cloud secure manner. Privacy means from the data owner point of view to encrypt the file before saving the cloud and decrypt the file after downloading when we want. Data encryption in heavy overhead to mobile devices and it is more complicated to communication between data user and the cloud. The main problem is mobile provide limited battery life and limited capacity and so, it causes a computing and communication problem for mobile cloud (device) user. To prevent this problem we proposed one scheme Traffic and Energy saving Encrypted search (TEES), it will prevent more bandwidth and better energy efficient encrypted search over the cloud. Encrypted search architecture offloads the communication and computation from the mobile device to cloud. An encrypted search reduces the computation time and save the energy consumption.

KEYWORDS- Mobile Cloud Storage, Data Encryption, Energy Efficient, Traffic Efficient.

I.INTRODUCTION

Clouds are a large pool of easily usable; it provided the services and accessible virtualized resources. Cloud storage is a model of online data storage and access data in any time and anyway. Mobile Cloud Storage (MCS) provide services to users to save and retrieve data or files on the cloud through wireless communication. The data privacy issue in cloud storage system, so the data is encrypted by owner before outsourcing onto the cloud and data users retrieves the interested data by encrypted search scheme. MCS also imported many traditional data encryption methods but traditional data encryption methods cannot be imported directly because MCS have limited computing and battery capacities of mobile devices. The traditional encryption method incurs new challenges. TEES (Traffic and Energy Efficient Search) introduces architecture to achieve efficiencies of mobile cloud storage application. TEES reduces the energy consumption by offloading the computation of the relevance cloud search and also reduces the network traffic for the communication of the selected index and reduces the file retrieval time. It will TEES's employs and modifies ranked keyword search scheme over encrypted data on mobile cloud storage system. Two categories exist for encrypted keyword search: ranked keyword search and Boolean keyword search. The ranked keyword search sends top-k relevant files to client and the Boolean keyword search sends all the matching files to the client. So ranked keyword search is most suitable for the mobile cloud storage. The TEES architecture with ranked keyword search offloads the security calculation to the cloud to save energy consumption of mobile devices and simplify the encrypted search procedure to reduce the traffic for retrieving the data from encrypted cloud storage. Order Preserving Encryption (OPE) is used as an encryption algorithm.

II.LITERATURE REVIEW

In this section gives a detailed review about Data Encryption, Energy Efficiency, and Traffic Efficiency. Here we reviewed how the Data Encryption, Energy and traffic Efficiency problem is solved in each scheme. We List the algorithm and techniques used in that scheme and it merit and demerit of that scheme are specified. In the following paper are survived in this section.

In[1] Ruhui Ma, Jian Li, Haibing Guan, Mingyuan Xia and Xue Liu, in the paper, "**EnDAS: Efficient Encrypted Data Search as a Mobile Cloud Service**" a novel scheme for data encryption and the data is encrypted for security purpose. Encrypted data should be effectively search and retrieve the data without any privacy leaks for mobile client. They are many solution for security issues, but that architecture cannot applied directly apply to the mobile device because it under on the mobile cloud environment. For that problem we propose an efficient Encrypted Data Search (EnDAS) scheme as a mobile cloud service. That scheme uses a lightweight trapdoor (encrypted keyword) compression method and it process reducing the trapdoor size for traffic efficiency. For this problem we proposed two method search scheme Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) algorithm to speed up the search time. For the index encryption we provide Fast Accumulated Hash (FAH) algorithm by encrypting each index slices before send to the cloud. Ranked Serial Binary Search (RSBS) algorithm will encrypt the document index. Cryptography is an encryption method of store and transmits data in a particular form so that only those for whom it is intended can read and process it. Trapdoor Mapping Table (TMT) module will reduce the encryption process to online approach to offline. A Trapdoor accumulator introduces fast accumulated hashing for fast accumulates. Some merits of the scheme EnDAS over the mobile cloud, which improves network traffic and search time efficiency and RSBS algorithm to reduce the network traffic. But the demerit is long search time and extra network traffic costs.

In[2] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "**Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data**," a novel scheme for search over encrypted data, most of the data owners are motivated to outsource their complex data management systems from local sites, because public cloud for great flexibility and economic savings. The data will encrypt before storing the file in cloud for security purpose and the traditional data utilization based on plaintext keyword search. The large number of data user and document in cloud, it is important for the search service to allow multi-keyword query and provide result similarity from ranking efficient data retrieval need. Single keyword search or Boolean keyword search is a searchable encryption, and rarely differentiates the search results. To solve this problem we define Privacy-preserving multi-keyword search over encrypted data in the cloud (MRSE) for securing he cloud data utilization system. To establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of “coordinate matching”. It will base on encryption, client and multi-keyword module processer. It has some merits multi-keyword rank search over encrypted in the cloud data and the coordinate matching for the inner product summarily. It demerits is weakens keyword privacy.

In [3] C. O¨ rencik and E. Savas¸ “**Efficient and secure ranked multikeyword search on encrypted cloud data,”** 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. The multi-keyword rank search will insert and deleted of document flexibly and it will better efficient than linear algorithm and the tree-based search scheme will encrypted over the cloud data. It have some merits it will accepted the outsourcing sensitive information such as e-mails, personal health care record, company finance detail and government document etc…,

In[4] Baojiang Cui, Zheli Liu_ and Lingyu Wang, “**Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage**” processer will selectively sharing encrypted data with different user in cloud storage. The public cloud is more secure and it will avoid the data leakage in the cloud. In this process necessary distribution to user a large number of key for encryption and searching and the client will stored they received key submit an equally huge amount of keyword in the cloud. We proposed KASE scheme applied that supports the searchable group data sharing functionality. Key management is the main requirement of effective to support searchable group data sharing. First, a data owner only needs to distribute a single aggregate key and second user need to aggraded trapdoor to the cloud to performing keyword search. In the searchable encryption we used many algorithms that are all setup algorithm cloud server to provide set up the scheme, keygen algorithm data owner to generated random key, Encrypt data owner to encrypt the document, Extract algorithm to generate an aggregate searchable encryption key for delegating the keyword search, Trapdoor algorithm user has aggregate key to perform a search, Adjust algorithm is run by cloud server to adjust the aggregate trapdoor to generate the right trapdoor document, Test algorithm is run by the cloud server to perform keyword search over an encrypted document.

It advantage it will more secure and Decryption key should be sent in secure and kept secret. It has disadvantaged it not efficient and shared data will not secure.

In[5]W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, in the paper "**Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking**," a novel scheme for multi-keyword text search. Encryption helps to protecting user data confidentiality. In this paper, we present MTS scheme with ranking method to address the problem. To improve the search scheme we propose multi-dimensional (MD) algorithm. MD algorithm is used to find the k-best matches in database. MDB-tree will represent an attributes domain and it assigns an attributes values. Random traversal algorithm which makes the cloud server randomly traverse on index and returns different results for the same query, and in the meantime, it maintains the accuracy of queries unchanged for higher security. Random traversal algorithm supports the k-best matches. This scheme, the data owner can control the all level of query. We use this method experimental result will more efficient than the state-of-the-art and it will protect data privacy and good scalability performance. It has some advantage the query efficiency for better user experiences.

.

In [6] Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, and Yingjiu Li "**Efficient and Expressive Keyword Search Over Encrypted Data in Cloud"**, the searchable encryption allows a cloud server to organized keyword search over the encrypted data and the data user without leaning plaintext. Searchable encryption schemes only support single or conjunctive keyword search. To improve that process, we proposed an public-key searchable encryption scheme(PEKS) in prime order groups, and it will expressed in conjunctive, disjunctive or any monotonic Boolean formulas, it will formally define for security. A cipher text of keyword is called PEKS cipher text. Decisional Bilinear Diffie-Hellman, Decisional Linear Assumption problem for polynomial-time algorithm. Setup, sKeyGen, Trapdoor, encrypt, Test algorithm will take the public parameter parts. To retrieve all the encrypted PHRs containing a keyword and search a query on keywords. It has some advantages of the Rouselakis-Waters scheme.

In [7] Ge Peng, Gang Zhou, David T. Nguyen, Xin Qi, Shan Lin**, "HIDE: AP-assisted Broadcast Traffic Management to Save Smartphone Energy"** in the present year Smartphone Will used for many purpose, particular for Wi-Fi. But Wi-Fi is major drawback for energy consumption. Smartphone energy is wasted to receive Wi-Fi broadcast frames because it wants high power consumed for broadcasting. So, in this paper, we improve Smartphone energy efficiency by reducing energy wasted on useless Wi-Fi broadcast traffic. That's why we design a system is HIDE to reduce Smartphone energy wasted on useless Wi-Fi broadcast traffic. So we propose to filter out useless UDP-padded broadcast frames (MAC layer Wi-Fi broadcast data frames with UDP payload) at APs before they are received by smart phones. So no energy will be wasted on Smartphone to receive or process on broadcast frames. We used one algorithm calculating broadcast flags it will reduce the client UDP port. So the energy will saved in Smartphone up to 35%-75% during broadcast. Our overhead analysis demonstrates to impact on network capacity and packet round-trip time. Demerits are high power combustion and its merits to save energy and energy consumption on Smartphone.

In[8] GAO Shang, PENG Zhe, XIAO Bin, SONG Yubo, "**Secure and Energy Efficient Prefetching Design for Smartphone**", energy efficient perfecting for Smartphone, it will use for reduce the energy computation and data transmission and also maintain the information in secure manner. Proxy system will cause security problem and end to end encryption cannot solve the security problem. For this problem we propose Secure and Energy Efficient Prefetching (SEEP) to reduce the security problem of HTTPS. The SEEP will include two parts. One is local proxy on the Smartphone to verify the validity of prefetched responses, and the remote proxy to store encrypted prefetched responses. Prefetching techniques will used reduce energy and data usage in Smartphone. We analyze the confidentiality and robustness requirements of the SEEP and it build for energy consumption and data transmission. SEES for both Smartphone and wed server and it cannot change the Brower/server. For the propose system consumes 25% less energy and 95% less data when prefetching the webpage.

Merits are to reduce energy computation and data transmission. But demerits is Proxy system will cause security problem and during data transmission.

In[9] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "**Toward privacy-assured and searchable cloud data storage services**", Cloud Computing provide convent and massive cloud storage and some application services. Cloud will provide great economical savings for data owners and users. In this paper we proposed end-to-end encryption techniques, it have been proposed as promising solutions for secure cloud data storage and a challenge are towards a primary full-fledged cloud data service. It will effectively support flexible data utilization services search over the data in a privacy-preserving manner. Symmetric Searchable Encryption methodology will proposed deterministic symmetric key encryption scheme. Scalar-Product-Preserving Encryption (SPE) scheme preserves the dot product between two *d*-dimensional vectors. Order-Preserving Symmetric Encryption OPSE the numerical ordering of plaintext is preserved after encryption. This search scheme will related some techniques Secure Multiparty Computation (SMC) it possess some private input, and Searchable Encryption (SE) involves a client and a server for stores an encrypted database. It advances in this field are surveyed, so it functionally rich, usable, and efficient search on encrypted data and it is possible without sacrificing privacy guarantee too much.

In [10] 2015, Jian Li, Ruhui Ma, Haibing Guan proposed "**TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud** ", Cloud will provide scalable storage at low cost. We perform encryption process for data privacy. But the data encryption is a heavy overhead for the mobile devices, and data retrieval process is complicated to communication between the data user and cloud. For this problem we propose TEES bandwidth and energy efficient encrypted search architecture over mobile cloud. TEES architecture creates a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. It offloads the computation from mobile devices to the cloud. However, TEES architecture uses Single keyword search and the single keyword search using OPE algorithm and TF-IDF table. To improve the search result accuracy as well as to enhance the user searching experience, it is necessary to support multiple keyword searches to narrow down the results. Multi-keyword is potentially the future main stream encrypted search scheme with higher searching accuracy.

Advantage is TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55% per file retrieval and it reduce network traffic. Disadvantage is Data encryption is a heavy overhead for the mobile devices and also heavy overhead to computing and communication as well as higher power consumption for mobile device users.

III.ANALYSIS

This section presents the study on data encryption and energy saving schemes which we reviewed in previous section. Based on this study results we can find the finest scheme used for data encryption and energy saving.

Table 1: COMPARATIVE STUDY ON DATA ENCRYPTION AND ENERGY SAVING SCHEMES

SI. NO	TITLE	Algorithms Used	Merits	Demerits
1.	EnDAS Efficient Encrypted Data Search as a Mobile Cloud Service	Trapdoor Generation Process algorithm : Encryption process and fast accumulator hashing	EnDAS over the mobile cloud, which improves network traffic and search time efficiency and RSBS algorithm to cope with the inefficient search time issue	Mobile device cause high search time and more network traffic
		Ranked Serial Binary Search (RSBS) algorithm: to find document and search keyword, Last significant bit(LSB) and Centre Bit Signification(CBS)		

2.	Efficient and secure ranked multikeyword search on encrypted cloud data	kNN algorithm: to encrypt the index and query vectors. Greedy Depth-first Search: algorithm to provide efficient multi-keyword ranked search LSH algorithm: provide exact ranking	Provides blinded encryption techniques for accessing the contents of the retrieved documents.	Computation & Communication costs of this method are little high as every searched word and Huge cost in terms of data usability.
3.	Privacy-preserving multi-keyword search over encrypted data in the cloud	Setup :symmetric key Build index :encrypted the symmetric key Trapdoor and query :ranked search on index	Result should be solved by cloud server And it will reduce the communication cost	Encrypted cloud data search is very challenging and weakens keyword privacy
4.	Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage	Broadcast encryption: setup, encrypt, decrypt Searchable Encryption : setup, encrypt, trpdr, test KASE Framework: setup, keygen, encrypt, extract,	More secure and Efficient public-key encryption scheme which supports flexible description.	Shared data will not be secure and license escalation will expose all.

		trapdoor, adjust, test algorithm		
5.	Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking	MD algorithm: improve the search efficiency represent attribute domain am and values Two secured index schemes: BMTS for known cipher text model and EMTS for known background mode	Efficiency better than linear search in cloud environment	It doesn't supports Dynamic data operation in cloud environment
6.	Efficient and Expressive Keyword Search Over Encrypted Data in Cloud	Keywords to be searched: KP-ABE and SE Encryption algorithm: Setup, sKeyGen, Trapdoor, Encrypt and Test	SE scheme it immutable with the number of keywords. prime order groups have parameter sizes over composite order groups	Data security
7.	HIDE: AP-assisted Broadcast Traffic Management to Save Smartphone Energy	Calculating broadcast flags: To start a DTIM period	Energy saving up to 34%-75%	Energy is wasted on Smartphone while broadcast frames.

8.	Secure and Energy Efficient Prefetching Design for Smartphone	Secure and Energy Efficient Prefetching (SEEP):to save energy consumption and data transmission	to reduce the energy and data cost on a Smartphone,	End-to-End encryption (SSL) in traditional prefetching systems cannot solve the security problem
9.	Toward privacy-assured and searchable cloud data storage services	encryption algorithm: MRSE scheme secure in the KC model polynomial-time algorithms: KeyGen, Index Enc, Query Enc, BuildIndex, Search	usable, and efficient search on encrypted data	Offline brute force attack, dictionary attack, week passwords and. Block level deduplication will cause additional overhead.
10.	TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud	single-keyword search algorithm :to provide secured and Lightweight searchable encryption. encryption algorithm : GenKey	It reduces the energy consumption By 35~55 % and time consumption by 23% to 46%.	Data encryption is heavy overhead for mobile device. Limited bandwidth capacity and limited battery life.

IV.POSSIBLE SOLUTION

To propose Multi-Keyword Energy Efficient (MKEE) search 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. Proposed system redistributes the encrypted index to avoid statistics information leak, and wraps keywords adding noise. Energy consumption is reduced by employing MKEE using relevance scores to the cloud server.

V.CONCLUSION

Mobile Cloud Storage (MCS) provides storage solutions to mobile device users by storage and retrieval of data on cloud. But, MCS have 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 outcome processing overhead**.** In this paper, we have survived various encryption schemes. Based on the analysis, many demerits were found which reduce the energy and traffic efficient for encryption process. To overcome these limitations we have proposed a method to enhance the efficient search scheme over encrypted data and also it provide security, reduce computation time etc. In future, the proposed method will be implemented in a encryption scheme which will increase the traffic & energy efficiency of encryption process higher than the existing schemes.

REFERENCES

[1] 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.

[2] 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.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in INFOCOM, 2011 Proceedings IEEE. IEEE, 2011, pp. 829–837.

[4] "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.

[5] 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.

[6] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[13] 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.

[14] Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, and Yingjiu Li “Efficient and Expressive Keyword Search Over Encrypted Data in Cloud”, JOURNAL OF, VOL., NO. , 2016 .[15] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 253–262.

[16] 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.

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

[18] A. Swaminathan, Y. Mao, G. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, “Confidentiality-preserving rank-ordered search,” in Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007, pp. 7–12.

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

[20] 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.