International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 1 – JUNE 2016.

AN ANONYMOUS ACCESS CONTROL TO SUPPORT MULTI-KEYWORD RANKED SEARCH FOR MOBILE CLOUD

Keshiya V[1], Revathi A[2]

[1]*PG student, PERI Institute Of Technology-Chennai, Department of Computer science and engineering, Anna University, Chennai, India.*

**2Head Of The Department,PERI Institute Of Technology, Department of Computer science and engineering, Anna University, Chennai, India.*

***ABSTRACT*--The advancement in cloud computing has motivated the data owners to outsource their datamanagement systems from local sites to commercial public cloud for great flexibility and economic savings. For realprivacy, user identity should remain hidden from CSP (Cloud service provider) and to protect privacy of data, datawhich is sensitive is to be encrypted before outsourcing. Thus, enabling an encrypted cloud data search service is ofgreat importance. By considering the large number of data users, documents in the cloud, it is important for the searchservice to allow multi-keyword query and provide result similarity ranking to meet the effective need of data retrieval,search, and not often differentiate the search results. In this system first time, we define and solve the challengingproblem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set ofstrict privacy requirements for such a secure cloud data utilization system to be implemented in real. We first propose a basic idea for the Multi-keyword Ranked Search over Encrypted cloud data (MRSE) based on secure inner productcomputation and efficient similarity measure of coordinate matching, i.e., as many matches as possible, in order tocapture the relevance of data documents to the search query, then give two significantly improved MRSE schemes toachieve various stringent privacy requirements in two different threat models. Assignment of anonymous ID to the userto provide more security to the data on cloud server is done. To improve search experience of the data search service,**

further extension of these two schemes to support more search semantics is done.

Index Terms- Cloud Computing; Searchable Encryption Keyword Search; Ranked SearchAnonymization; MRSE

I. INTRODUCTION

Cloud computing has been a long dreamed vision of computing as a utility, where the cloud customers canremotely store their data into cloud so they can enjoy the on-demand high-quality applications and services from ashared pool of configurable computing resources. Great flexibility and economic savings in cloud computing are motivating the individuals and enterprises to outsource their local complex data management system into the cloud. In order to protect data privacy and combat unsolicited accesses in the cloud and beyond, sensitive data, for instance, emails, personal health records, photo albums, tax documents, financial transactions, etc. may have to be encrypted by data owners before outsourcing them to the commercial public cloud; this, however, obsoletes the traditional data utilization service based on plaintext keyword search. The trivial solution of downloading all the data and decrypting locally is clearly not practical, due to the huge amount of bandwidth cost in cloud scale systems. Moreover, besides from eliminating the local storage management, storing data into cloud serves no purpose unless and until they can be easily searched and utilized by users.

Thus, exploring privacy-preserving and effective search service overencrypted cloud data is of paramount importance. Considering the potentially large number of on-demand data users and huge amount of outsourced data documents in the cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements of performance, system usability and scalability. On the one hand, to meet the effective data retrieval need,the large amount of documents demand the cloud server toperform result relevance ranking, instead of returning undifferentiated results. Such ranked search system enables data users to find the most relevant information quickly, rather than burdensomely sorting through every match in the content collection [3]. 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. For privacy protection, such ranking operation, however, should not leak any keyword related information.

For protection of privacy, such ranking operation, however, should not leak any keyword related information. On the other hand, to improve the search result accuracy as well as to enhance the user searching experience, it is also essential for such ranking system to support multiple keywords search, as single keyword search often yields far too coarseresults. As a common practice indicated by today’s web search engines (like Google search), data users may tend toprovide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. Along with privacy of data and efficient searching schemes, real privacy is gained only if the user's identity remains hidden from the cloud service provider i.e. CSP as well as the third party user on the cloud server [1].

The information encryption, bethat as it may, would essentially bring down the ease of use of information because of the trouble

of lookingover the scrambled information [6]. Essentially encoding the information may even now bring about other security concerns. Case in point, Google Searchutilizes SSL (Secure Sockets Layer) to scramble the association between pursuit client and Google server when private information, for example, reports and messages show up in the indexed lists [7].In any case,if the inquiry client clicks into another site from the query items page, that site may have the capacity to recognize the hunt terms that the client has utilized. Ontending to above issues, the searchable encryption (e.g., [8], [9], [10]) has been as of late created as an essential way to deal with empower seeking over scrambled cloud information, which continues the accompanying operations. Firstly, the information proprietor needs to create a few watchwords as indicated by the outsourced information. These watchwords are then encoded and put away at the cloud server. At the point when a pursuit client needs to get to the outsourced information, it can choose some significant watchwords and send the ciphertext of the chose catchphrases to the cloud server. The cloud server then uses the ciphertext to coordinate the outsourced scrambled catchphrases, and in conclusion gives back the coordinating results to the inquiry client. To accomplish the comparative hunt effectiveness and accuracy over scrambled information as that of plaintext catchphrase seek, a broad group of exploration has been produced in writing. Wang et al. [11] propose a positioned catchphrase inquiry planwhich considers the importance scores of watchwords.

Sadly, because of utilizing request safe guarding encryption (OPE) [12] to accomplish the positioningproperty, the proposed plan can't accomplish unlink ability of trapdoor. Later, Sun et al. [13] propose a multi-watchword content hunt plan which considers the importance scores of catchphrases and uses a multidimensional tree method to accomplish effective inquiry question. Yu et al. [14] propose a multi watch word top-k recovery plan which utilizes completely Homomorphic encryption to encode the record/trapdoor and ensures high security. Cao et al. [6] propose a multi-watchword positioned look (MRSE), which applies direction machine as the catchphrase coordinating guideline, i.e., return information with the most coordinating catchphrases. Albeit numerous inquiry functionalities have been produced in past writing towards exact and proficient searchable encryption, it is still troublesome for searchable encryption to accomplish the same client experience as that of the plaintext pursuit, similar to Google look. This for the most part ascribes to taking after two issues. Firstly, inquiry with client inclinations is exceptionally main stream in the plaintext look [15], [16]. It empowers customized look and can all the more precisely speak to client's prerequisites, however has not been completely concentrated on and bolstered in the encoded information area. Furthermore, to further enhance the client's experience on looking, an imperative and major capacity is to empower the multiwatch word seek with the far reaching rationale

1.2 Contribution and plan of this paper

The contributions of this paper can be summarized as follows. Firstly, we provide formal definitions for the security and privacy requirements of keyword search on encrypted cloud data. Secondly, we propose an efficient ranked multi- keyword search scheme and formally prove that it is secure in accordance with the defined requirements. Thirdly, wepropose a ranking method that proves to be efficient to implement and effective in returning documents highly relevantto submitted search terms in the blind storage.

II. LITERATURE SURVEY

In [2], main focus is to find the solution of multi keyword ranked search over encrypted cloud data (MRSE) whilepreserving strict system-wise privacy in the cloud computing paradigm. A variety of multi- keyword semantics areavailable, an efficient similarity measure of “coordinate matching” i.e. as many matches as possible, to capture the datadocuments' relevancy tothe search query is used. Specifically “inner product similarity”, i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query is used in MRSE algorithm. The important drawback of this paper is that the user’s identity (ID) was not kepthidden. Hence, whoever puts the data on Cloud Service Provider (CSP) was known to the CSP. This might be risky insome situations. Hence, this limitation is overcome in proposed system. For instance, a user may want to store old emailmessages encrypted on a server managed by Yahoo or another large vendor, and later retrieves certain messageswhile travelling with a mobile device.

In [3], the schemes are efficient as no public-key cryptosystem is involved. Indeed, this approach is independent ofthe encryption method chosen for remote files. The main theme taken from the paper is of storing data remotely onother server and retrieving that data from anywhere through mobile, laptop etc.

In [4], an overall summary of thebenefits of a cryptographic storage service, for instance, reducing the legal exposure of both customers and cloudproviders, also achieving regulatory compliance is provided. Besides all this, cloud services that could be built on topof a cryptographic storage service such as secure back-ups, archival, health record systems, secure data exchange and discoveryis stated.

The [5], the paper has defined and found solution to the problem of effective yet secured ranked keyword searchover encrypted cloud data. For the first time, paper has defined and solved the most challenging problem of privacypreservingmulti-keyword ranked search over encrypted cloud data (MRSE), and established a set of strict privacyrequirements for such a secure cloud data utilization system to become a reality. The proposed ranking method provesto be efficient to return highly relevant documents which correspond to the submitted search terms. Idea of proposedranking method is used in the proposed system in order to enhance the security of data and the documents on CloudService Provider (CSP).

The [6] paper tells the significance of protecting individual’s privacy in cloud computing, it also provides someprivacy preserving technologies used in cloud computing services. Paper

tells that it is quite important to take privacyinto account while designing cloud services, if all this involves the collection, processing or sharing of personal data.From this paper, main idea taken is of privacy preserving of data. This paper importantly describes privacy of data butdoesn't allow indexed search as well as the user's identity is not kept hidden. Thus, these two main limitations areovercome in the proposed system.

In [7], the paper mainly focuses on existing and new algorithms for assigning anonymous IDs and their examination with respect to trade-offs between communication and computational requirements. These algorithms are built on topof a secure sum data mining operation using Newton's identities and Sturm's theorem. The main focus in this paper isof assigning anonymous ID to the user on the cloud.

In [8], paper's main idea is to formalize and provide solution to the problem of effective fuzzy keyword search overencrypted cloud data while maintaining keyword privacy. This basic theme is taken but it is mainly for multi-keywordranked search (MRSE scheme) in the proposed system.

In [9],design of secure cloud storage service which addressesthe reliability issue with near-optimal overall performance is mainly proposed.Achieving fine-graininess, scalability, and data confidentiality of access control simultaneously is a problem forwhich no solution is found yet.

The paper [10] addresses this challenging open issue on one hand, defining andenforcing access policies based on data attributes, and, on the other hand, allowing the data owner to refer most of thecomputation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing theunderlying data contents.

In [11], authors have proposed a privacy-preserving public auditing system for data storage security in Cloud
Computing scheme. It utilizes homomorphic linear authenticator and random masking to guarantee that the TPA wouldnot learn any knowledge about the data content stored on the cloud server during the efficient auditing process, whicheliminates the burden of cloud user from the difficult, tedious and possibly expensive auditing task, it also alleviatesuser's fear of his/her outsourced data leakage.

In [12], authors have defined and solved the problem of privacypreservingquery over encrypted graph-structured data in cloud computing (PPGQ), and established a set of strictprivacy requirements for such a secure cloud data utilization system to become a reality. The basic idea taken from thispaper is of privacy preserving over encrypted cloud data. The limitation in this is that the query is not indexed toprovide fast searching. This drawback is overcome in the proposed system.

III. EXISTING SYSTEM

In existing method data owner can be encrypted thedocuments and the cloud server, documents can bedecrypted in cloud. In order to meet the practical searchrequirements, search over encrypted data should support the following three roles. First, the searchable encryptionsystems should care multi-keyword search, and offer thesame user experience as searching in Google search withdiverse keywords; single keyword search is far fromappropriateness by only recurring very partial andimprecise search results. Although the existing schemesaim at providing integrity confirmation for different datastorage systems, the problem in supporting both publicauditability and data dynamics has not been fullyaddressed. How to achieve a protected and effective designto flawlessly integrate these two important components fordata storage service remains an open stimulating task inCloud Computing.

Issues in Existing System

1. Issue in mobile cloud computing.
2. Investigation of searchable encryption technique to achieve efficient searching over outsourced encrypted data
3. It fail to offer sufficient insights towards the construction of full functioned searchable encryption.

IV. PROPOSED SYSTEM

We define and solve the challenging problem ofauthentication and access control for multi-keyword rankedsearch over encrypted cloud data, andestablish a set of firm authentication and access controlrequirements for such a secure cloud data applicationsystem to become a truth. Among various multi-keywordsemantics, we had chosen the effective standard of"coordinate matching". Here we are providing foolproofsecurity in proprietors upload side as well as on thedownload side. For better security client splitting thatsingle file into nine different blocks and providing a uniqueidentification number for each chunk.

A. PROPOSED SCHEME

In this section, we give a detailed description of ourscheme. We firstly propose to implement the semanticmulti-keyword ranked search.As an effort towards the issue, in this paper, we propose anefficient multi-keyword ranked search scheme overencrypted mobile cloud data through blindstorage. Our main contributions can be summarized asfollows:

• We introduce a relevance score in searchableencryption to achieve multi-keyword ranked searchover the encrypted mobile cloud data. In addition tothat, we construct an efficient index to improve thesearch efficiency.

• By modifying the blind storage system in theAMRSED, we solve the trapdoor disassociationproblem and mask access pattern of the search userfrom the cloud server.

• We give thorough security analysis to demonstrate thatthe EMRS can reach a high security level includingconfidentiality of documents and index, trapdoorconfidentiality, trapdoor disassociation, and coveringaccess pattern of the search user. Moreover, weimplement extensive experiments, which show that theAMRSED can achieve enhanced efficiency in theterms of functionality and search efficiency comparedwith existing proposals.

B. Security Requirements

Specifically, the AMRSED aims to provide the followingfour security requirements:

• Confidentiality of Documents and Index: Documents andindex should be encrypted before being subcontracted toa cloud server. The cloud server should be preventedfrom prying into the subcontracted documents andcannot infer any associations between the documents andkeywords using the index.

• Trapdoor Confidentiality: Since the search user wouldlike to keep her searches from being exposed to thecloud server, the cloud server should be prevented fromknowing the exact keywords contained in the trapdoor ofthe search user.

• Trapdoor disassociation: The trapdoors should not belinkable, which means the trapdoors should be totallydifferent even if they contain the same keywords. Inother words, the trapdoors should be randomized ratherthan determined. The cloud server cannot infer anyassociations between two trapdoors.

• Covering Access Pattern of the Search User: Accesspattern is the sequence of the searched results. In theEMRS, the access pattern should be totally masked fromthe cloud server. Specifically, the cloud server cannotlearn the total number of the documents stored on it orthe size of the searched document even when the searchuser retrieves this document from the cloud server.

C. Blind Storage System

A blind storage system is built on the cloud server to supportadding, updating and deleting documents and coveringthe access pattern of the search user from the cloud server.In the blind storage system, all documents are divided intofixed-size blocks. These blocks are indexed by a sequenceof random integers generated by a document-related seed.In the view of a cloud server, it can only see the blocks ofencrypted documents uploaded and downloaded. Thus, theblind storage system leaks little information to the cloudserver. Specifically, the cloud server does not know whichblocks are of the same document, even the total number ofthe documents and the size of each document. Moreover, all the documents and index can be stored in the blind storage system to achieve a searchable encryption scheme..

D. Advantages of proposed system

1. It addresses both spatial and temporal domains, which leads to detecting various malicious changes in spatial and time domains.
2. It is faster and lower complexity compared to existing algorithms, making it practical and suitable for real-time applications
3. Hiding Capacity of the secret data bits is high.
4. Hiding capacity was based on the pixel number corresponding to the two highest peaks of the image histogram

4.1 SYSTEM MODEL

The overview of the proposed system is illustrated in Figure 1. We assume that the parties are semi-honest and donot collude with each other to bypass the security measures.In Figure 1, steps and typical interactions between theparticipants of the system are illustrated. In an offline stage,the data owner creates a search index for each document.The search index file is created using a secret key basedtrapdoor generation function where the secret keys1 are onlyknown by the data owner. Then, the data owner uploads these search index files to the server together with the encrypted documents. We use symmetric-key encryption asthe encryption method since it can handle large document sizes efficiently. This process is referred as the index generation henceforth and the trapdoor generation is consideredas its one of the steps.

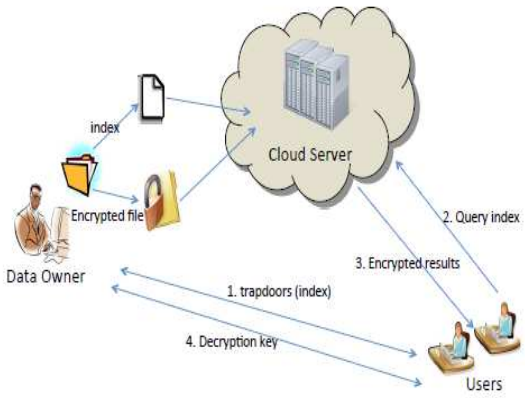

Fig .1 System Architecture

When a user wants to perform a keyword search, it firstconnects to the data owner. He learns the trapdoors (cf.Step 1 in Figure 1) for the keywords he wants to searchfor, without revealing the keyword information to the dataowner. Since the user can use the same trapdoor for manyqueries containing the corresponding search term, this operation does not need to be performed every time the userperforms a query. After learning the trapdoor information,the user generates the query (referred as query generationhenceforth) and submits it to the server (cf. step 2 in Figure 1). In return, he receives metadata2 for the

matcheddocuments in a rank ordered manner as will be explained insubsequent sections. Then the user retrieves the encrypteddocuments (cf. Step 3 in Figure 1) he chooses after analyzingthe metadata that basically conveys a relevancy level of theeach matched document, where the number of documentsreturned is specified by the user. Finally, the user interactswith the data owner in order to decrypt the documents andget the corresponding plaintext (cf. Step 4 in Figure 1); andin the process the data owner does not learn the documentsthat it is assisting to decrypt.

The multi-keyword search method explained in this section, it checks whether queried keywords exist in a document or not.If the user searches for a single or more keywords, there willpossibly be many correct matches where some of them maynot be useful for the user at all. Therefore, it is difficultto decide as to which documents are the most relevant. Weadd ranking capability to the system by adding extra indexinformation for frequently occurring keywords in a file. Withranking, the user can retrieve only the top matches where is chosen by the user.In order to rank the documents, a ranking function isrequired, which assigns relevancy scores to each documentmatching to a given search query. One of the most widelyused metrics in information retrieval is the term frequency [15]. Term frequency is defined as the number of times akeyword appears in a document. Instead of using term frequency itself, we assign relevancy levels based on the termfrequencies of keywords.

We assume that there are η levels of ranking in our proposed method for some integer $\eta \geq 1$. For each document,each level stores an index for frequent keywords of that document in a cumulative way in descending order. This basically means that i^{th} level index includes all keywords in the(i + 1)th level and the keywords that have term frequencyfor the i^{th} level. The higher the level, the higher the termfrequency of the keywords is. For instance, if η = 3, level1 index includes keywords that occur at least once in thedocument while levels 2 and 3 include keywords that occurat least, say 5 times and 10 times4, respectively. There areseveral variations for relevancy score calculations [15] andwe use a very basic method. The relevancy score of a document is calculated as the number representing the highestlevel search index that the query index matches.

All the keywords that exist in a document are included
in the first level search index of that document. The other higher level indices include thefrequent keywords that also occur in its previous level, butthis time they have to occur the number of times, whichare at least the term frequency of the corresponding level.The highest level includes only the keywords that have thehighest term frequency. In the oblivious search phase, theserver starts comparing the user query against the first levelindices of each document. The matching documents found asa result of the comparison in the first level are then comparedwith the search indices in the other levels according to theAlgorithm 1.

In this method, some information may be lost due to theranking method employed here. Rank of two documentswill be the same if one involves all the queried keywords infrequently and the other involves all the queried keywordsfrequently except one infrequent one. The rank of the document is identified with the least frequent keyword of thequery. We tested the correctness of our ranking method bycomparing with a commonly used formula for relevance scorecalculation [13], which is given in the following section.

ALGORITHM FOR RANK SEARCH

for all documents R_i do
Compare(level1 index of R_i, query index)
j = 1
while match do
increment j
Compare (levelj indices of R_i, query index)
end while
rank of R_i = highest level that match with query index
end for

While this new method necessitates an additional r-bitstorage per level for a document, it reduces the communication overhead of the user since matches with low rankdocuments will not be retrieved unless the user requests.Considering η search indices are stored instead of a singlesearch index per document, storage overhead for indexingmechanism increases η times due to ranking. This additionalcost is not a burden for the server since the index sizes areusually negligibly small compared to actual document sizes.

V. IMPLEMENTATION

The proposed system of this project is divided into three major modules and described as below.

1. **DATA OWNER**
2. **SERVER**
3. **USER**

5.1 MODULES DESCRIPTION

5.1.1 USER

After receiving trapdoor keys from the dataowner, query index is generated, which is essentially equivalent to per-forming hash operations. Subsequent to the retrieval of encrypted documents, the user shouldperform one blinding operation over an RSA encryption, one signing for authentication purposesand symmetric-key decryption operations. These operations are equivalent to 3 modular exponentiations, 2 modular multiplications and one symmetric-key decryptionoperation per document retrieved.

5.1.2 SERVER

The server only does the search operation, which is binary comparison of r-bit queryindex with database indices, each of which isagain r-bit binary sequence. If the ranking isused, the query index should also be comparedwith indices of the matching documents. So theserver performs additional binary comparison of
r-bit indices for each matching document, where η is the number of levels.

5.1.3 DATA OWNER

The data owner creates the indicesand symmetric-key encryptions of all documents;but these operations are performed only once inthe initialization phase. Other than this, dataowner is active while the user learns the trapdoorsand decryption keys, which requires 2 modularexponentiations for each.

Fig .2User register page

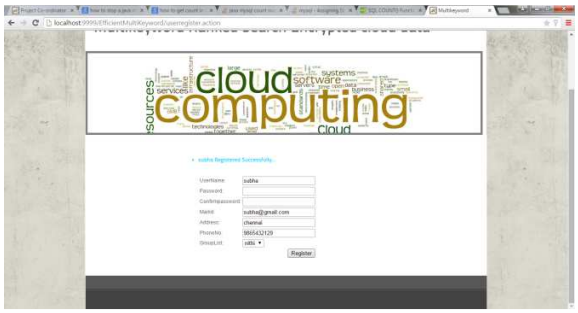

Fig.3 User registered successfully

Fig .4 file upload

Fig .5 Key Generation

Fig .6 SearchingModule

Fig.7 Results

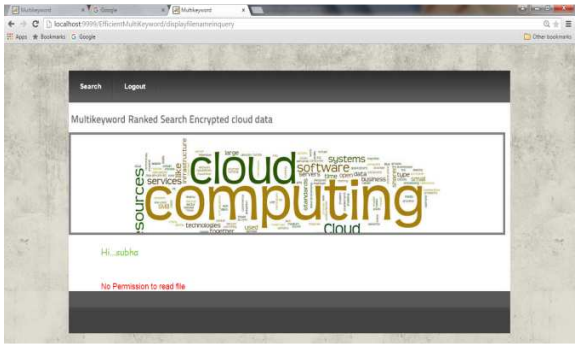

Fig. 8 For Unauthorized User

VI. CONCLUSION

In this paper, we have proposed a multi-keyword rankedsearch scheme to enable accurate, efficient and securesearch over encrypted mobile cloud data. Security analysishave confirmed that proposed scheme can effectivelyachieve confidentiality of documents and index, trapdoorconfidentiality, trapdoor disassociation, and coveringaccess pattern of the search user. Wide performanceappraisals have shown that the proposed scheme canachieve better efficacy in terms of the functionality andcomputation overhead compared with existing ones. Forthe future work, will investigate on the authentication andaccess control issues in searchable encryption method andprovide an block insertion method to divide the files andprovide unique identification method and using decryptionkey download the files in the users side. This method can
achieve the search effectiveness.

REFERENCE

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Confidentiality-preserving multi- keyword ranked searchover encrypted cloud data,"" IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.
[2] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases", inProc. ACM SIGMOD Int. Conf. Manage. Data, 2009, pp.139–152.

[3] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamicsearchable encryption via blind storage", in Proc. IEEESymp. Secur. Confidentiality, May 2014, pp. 639–654.

[4] H. Pang, J. Shen, and R. Krishnan, " Confidentialitypreservingsimilarity-based text retrieval ", ACM Trans.Internet Technol., vol. 10, no. 1, p. 4, 2010.

[5] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, ''AnSMDP-based service model for interdomain resourceallocation in mobile cloud networks,'' IEEE Trans. Veh.Technol., vol. 61, no. 5, pp. 2222–2232, Jun. 2012.

[6] M. M. E. A. Mahmoud and X. Shen, ''A cloud-basedscheme for protecting source-location privacy againsthotspot-locating attack in wireless sensor networks,'' IEEETrans. Parallel Distrib. Syst., vol. 23, no. 10, pp. 1805–1818,Oct. 2012.

[7] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo,
''Exploiting geodistributed clouds for a e-health monitoringsystem with minimum service delay and privacypreservation,'' IEEE J. Biomed. Health Inform., vol. 18, no.2, pp. 430–439, Mar. 2014.

[8] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, ''A survey ofmobile cloud computing: Architecture, applications, andapproaches,'' Wireless Commun. Mobile Comput., vol. 13,no. 18, pp. 1587–1611, Dec. 2013.

[9] H. Li, Y. Dai, L. Tian, and H. Yang, ''Identity-based
authentication for cloud computing,'' in Cloud Computing.Berlin, Germany: Springer-Verlag, 2009, pp. 157–166.

[10] W. Sun, et al., ''Confidentiality-preserving multi-keywordtext search in the cloud supporting similarity-basedranking,'' in Proc. 8th ACM SIGSAC Symp. Inf., Comput.Commun.Secur., 2013, pp. 71–82.

[11]B.Wang,S.Yu,W.Lou,andY.T.Hou,''Confidentialitypreservingmulti-keywordfuzzy search over encrypted data
in the cloud,'' in Proc. IEEE INFOCOM, Apr./May 2014,pp. 2112–2120.

[12] E. Stefanov, C. Papamanthou, and E. Shi, ''Practical
dynamic searchable encryption with small leakage,'' in Proc.NDSS, Feb. 2014.

[13] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, ''Securedynamic searchable symmetric encryption with constantdocument update cost,'' in Proc. GLOBECOM, Anaheim,CA, USA, 2014.

[14] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, andM. Steiner, ''Highly-scalable searchable symmetricencryption with support for Boolean queries,'' in Proc.CRYPTO, 2013, pp. 353–373.

[15] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou,''Confidentiality-preserving multikeyword ranked searchover encrypted cloud data,'' IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[16] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis,''Secure kNN computation on encrypted databases,'' inProc. ACM SIGMOD Int. Conf. Manage. Data, 2009, pp.139–152.
[17] M. Naveed, M. Prabhakaran, and C. A. Gunter, ''Dynamicsearchable encryption via blind storage,'' in Proc. IEEESymp.Secur. Confidentiality, May 2014, pp. 639–654.

[18] H. Pang, J. Shen, and R. Krishnan, ''Confidentialitypreservingsimilarity-based text retrieval,'' ACM Trans. Internet Technol., vol. 10, no. 1, p. 4, 2010.

[19] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, ''Toward securemultikeyword top-k retrieval over encrypted cloud data,''IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp.239–250, Jul./Aug. 2013.

[20] A. Lewko and B. Waters, ''Decentralizing attribute-basedencryption,'' in Proc. EUROCRYPT. Berlin, Germany:Springer-Verlag, 2011, pp. 568–588.

[22] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano,''Public key encryption with keyword search,'' in Proc.EUROCRYPT, 2004, pp. 506–522.

[23] D. Boneh and B. Waters, ''Conjunctive, subset, and rangequeries on encrypted data,'' in Proc. TCC, 2007, pp. 535–554.

[24] B. Zhang and F. Zhang, ''An efficient public key encryptionwith conjunctive-subset keywords search,'' J. Netw.Comput. Appl., vol. 34, no. 1, pp. 262–267, Jan. 2011.