|| Volume 5 || Issue 10 || October2020 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH

AND ENGINEERING TREND

A SECURE AND DYNAMIC MULTI-KEYWORD RANKED SEARCH SCHEME OVER ENCRYPTED CLOUD DATA

Mr. Vivek Kiran Kale

Student, CSMSS, Chh. Shahu College of Engineering Aurangabad, Maharashtra, India

Abstract: - Nowadays, the unique and safest way of stowing and conveying data is cloud computing. Automated computing and, on demand computing is another names of cloud computing. The method in which common podium or secluded server is used in the collection of data from several sources which can be easily accessible on their requirement. Due to recent advances in wireless communication technologies, there has been a rapid growth in wireless sensor networks research during the past few decades. Many novel architectures, protocols, algorithms, and applications have been proposed and implemented. The efficiency of these networks is highly dependent on routing protocols directly affecting the network life-time. In sparse wireless sensor networks, a mobile robot is usually exploited to collect the sensing data. Each sensor has a limited transmission range and the mobile robot must get into the coverage of each sensor node to obtain the sensing data. To minimize the energy consumption on the traveling of the mobile robot, it is significant to plan a data collection path with the minimum length to complete the data collection task. In this project, we observe that this problem can be formulated as traveling salesman problem with neighborhoods, which is known to be NP-hard. To address this problem, we apply the concept of artificial bee colony (ABC) and design an ABC-based routing algorithm.

Keywords- Artificial Bee Colony (ABC), Mobile Robot, Travelling Salesman Problem (TSP), Wireless Sensor Networks (WSN)

application.

I INTRODUCTION

Distributed computing has been considered as another model of big business IT foundation, which can sort out gigantic asset of registering, stockpiling and applications, and empower clients to appreciate omnipresent, advantageous and on demand organize access to a common pool of configurable figuring assets with extraordinary proficiency and negligible monetary overhead. Pulled in by these engaging highlights, the two people and endeavours are spurred to outsource their information to the cloud, rather than obtaining programming and equipment to deal with the information them. Regardless of the different focal points of cloud administrations, outsourcing delicate data, (for example, messages, individual well-being records, organization back information, government reports, and so on.) to remote servers brings security concerns. The cloud specialist co-ops (CSPs) that keep the information for clients may get to clients' delicate data without approval. A general way to deal with secure the information privacy is to scramble the information before outsourcing . Be that as it may, this will cause a tremendous cost as far as information ease of use. For instance, the current systems on catchphrase based data recovery, which are generally utilized on the plaintext information, can't be specifically connected on the scrambled information. Downloading every one of the information from the cloud and unscramble locally is clearly unfeasible.

Objectives

- To Study and Learn existing searchable encrypted keywords.
- To Implement Keyword Value Guessing Attacks on Cipher text and also Keyword Value Guessing Attacks on Trapdoors.
- To compare existing results.
- To ensure expressiveness of the keyword access structures expressed in any Boolean formula with AND / OR gates.
- The Efficiency should be adequately efficient in terms of computation, communication and storage for practical applications.
- Keyword privacy and provable security scheme should be formally proved under the standard model rather than the informal analysis.
- To design a dynamic Searchable encryption scheme whose updating operation can be completed by cloud server only while reserving the ability to support multi-keyword ranked search.

II LITERATURE REVIEW

The Searchable encryption scheme enabled the customer to stock there encrypted data on cloud & execute keyword search on the cipher text platform. We know that dissimilar cryptography primitives are available for searchable encryption structure, this scheme may be created on cryptography based on public key or the symmetric key cryptography.

In this project we use the symmetric searchable encryption (SSE) scheme, the search, time of the scheme is linear to the size of data collection this SSE scheme is based on bloom filter the search time of this scheme is O(n), where n is the cardinality of data collection. The symmetric searchable encryption scheme follows the user to input the multiple keywords to request suitable document. In this work the connective keyword search only return the documents which contain the whole keyword. The prediction search support both conjective and disjunctive search. All of this multikeyword search schemes retrieve the search result which is based on the existence of keyword. which cannot provide the acceptable ranking result functionality.

Enabling secure and efficient ranked keyword search over outsourced cloud data.

Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data has to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is inherently demanded by large number of users and huge amount of data files in cloud. In this paper, we define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. An efficient public key encryption with conjunctive-subset keywords search.

We consider the advancement of conjunctive catchphrase accessible plan which empowers one to look encoded archives by utilizing more than one watchword. The thought of conjunctive watchword seeking was displayed by Golle et al. in 2004. Be that as it may, their security display was built in a symmetric-key setting which isn't material for the general applications in the truth. So Park et al. broadened Golle et al's. security display into a public key setting which calls the Public Key Encryption with Conjunctive Field Keyword Search (PECKS) plot. In this paper, we look at six security models by finishing up the mystery key setting and open key setting, and aggregate up six security prerequisites that must fulfill to develop a safe conjunctive catchphrase accessible plan Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud.

The appearance of distributed computing, information proprietors are roused to outsource their mind boggling information administration frameworks from neighbourhood locales to business open cloud for incredible adaptability and financial funds. In any case, for securing information protection, touchy information must be scrambled before outsourcing, which obsoletes conventional information usage in view of plaintext watchword seek. In this manner, empowering an encoded cloud information look benefit is of central significance.

Considering the vast number of information clients and reports in cloud, it is urgent for the hunt administration to permit multi-watchword inquiry and give result likeness positioning to meet the viable information recovery require.

Achieving usable and privacy-assured similarity search over outsourced cloud data.

Distributed computing is imagined as the cutting edge design of IT ventures, giving advantageous remote access to information stockpiling and application administrations. While this outsourced stockpiling model can possibly bring extraordinary practical reserve funds for information proprietors and clients, however because of wide worries of information proprietors that their private information might be automatically uncovered or dealt with by cloud suppliers.

III SYSTEM ARCHITECTURE

Propose the rest expressive SE scheme in the public-key setting from bilinear pairings in prime order groups. As such, our scheme is not only capable of expressive multi-keyword search, but also significantly more efficient than existing schemes built in composite-order groups. Using a randomness splitting technique, our scheme achieves security against offline keyword dictionary guessing attacks to the cipher texts. Moreover, to preserve the privacy of keywords against offline keyword dictionary guessing attacks to trapdoors, we divide each keyword into keyword name and keyword value and assign a designated cloud server to conduct search operations in our construction. Formalize the security definition of expressive SE, and formally prove that our proposed expressive SE scheme is selectively secure in the standard model. Implement our scheme using a rapidly prototyping tool called Charm, and conduct extensive experiments to evaluate its performance. Our results confirm that the proposed scheme is sufficiently efficient to be applied in practice. A trusted trapdoor generation center who publishes the system parameter and holds a master private key and is responsible for trapdoor generation for the system, data owners who outsource encrypted data to a public cloud, data users who are privileged to search and access encrypted data, and a designated cloud server who executes the keyword search operations for data users

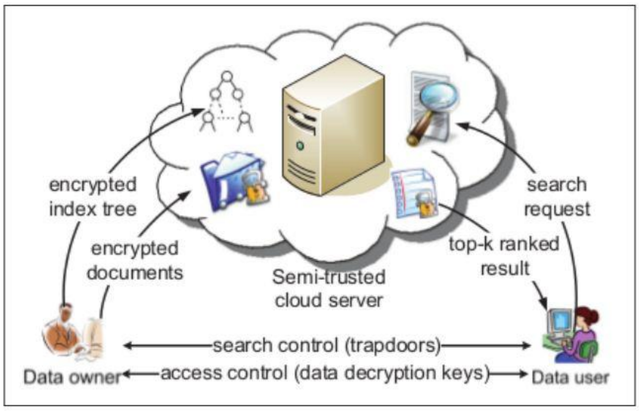


Figure 1: System File Structure

Attribute based encryption storage system supporting secure de-duplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file, encrypted under different access policies. A data provider intends to upload a file M to the cloud, and share M with users having certain credentials. In order to encrypt M under an access policy A over a set of attributes and uploads the corresponding cipher text to the cloud, such that only users whose sets of attributes satisfying the access policy can decrypt the cipher text. Later, another data provider uploads a cipher text for the same underlying le M but ascribed to a different access policy.

A. Searchable encryption schemes enable the clients to store the encrypted data to the cloud and execute keyword search over cipher text domain. Due to different cryptography primitives, searchable encryption schemes can be constructed using public key based cryptography or symmetric key based cryptography proposed the first symmetric searchable encryption (SSE) scheme, and the search time of their scheme is linear to the size of the data collection. Formal security definitions for SSE and designed a scheme based on Bloom filter. The search time where n is the cardinality of the document collection which achieve the optimal search time. Their SSE-1 scheme is secure against chosen keyword attacks (CKA1) and SSE-2 is secure against adaptive chosen-keyword attacks (CKA2). These early works are single keyword Boolean search schemes, which are very simple in terms of functionality. Afterward, abundant works have been proposed under different threat models to achieve various search functionality, such as single keyword search, similarity search, multi-keyword Boolean search, ranked search and multi-keyword ranked search. A trusted trapdoor generation center who publishes the system parameter and holds a master private key and is responsible for trapdoor generation for the system, data owners who outsource encrypted data to a public cloud, data users who are privileged to search and access encrypted data, and a designated cloud server who executes the keyword search operations for data users. Due to different cryptography primitives, searchable encryption schemes can be constructed using public key based cryptography or symmetric key based cryptography proposed the first symmetric searchable encryption (SSE) scheme, and the search time of their scheme is linear to the size of the data collection. Formal security definitions for SSE and designed a scheme based on Bloom filter.Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computers processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks. The cloud users upload the data into multi-cloud. Cloud computing environment is constructed based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud .A multi-cloud allows clients to easily access his/her resources remotely through interfaces. In our system the each cloud admin consist of data blocks.The cloud users upload the data into multi-cloud. Cloud computing environment is constructed based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability.

Algorithm-I: Build Index Tree (F)

Input: The document Collection F = {f1, f2, ..., fn} with the identifiers FID = {FID j FID = 1, 2, ..., n} Output : The index tree T

```
1. for each document fF ID in F do
2. Construct a leaf node u for fF ID with u. ID = GenID(), u.P1 = u.Pr = null, u.FID = FID, and D[i] = T FF ID for i = 1.....m
3. Insert u to Current Node Set;
4. end for
5. While the number of nodes in Current Node Set is larger than 1 do
6. if the number of nodes in Current Node Set is even i.e. 2h then
7. for each pair of nodes u' and u" in Current Node Set do
8. Generate a parent node u for u", with u.ID = GenID(), u.P1 = u', u.Pr = u", u.FID = 0 and D[i] = max f u'.D[i], u".D[i] g for each i = 1....m;
9. Insert u to Temp Node Set
10. end for
11. else
12. for each pair of nodes u' and u" of the former (2h-2) nodes in Current Node Set do
13.. Generate a parent node u for u' and u";
14. Insert u to Temp Node Set
15. end for
16. Create a parent node u1 for (2h1)
th and 2h
th node and then create a parent
nodeu for u1 and the (2h+1)
th node;
17. Insert u to Temp Node Set
18. end if
19. Replace Current Node Set with Temp Node Set and then clear Temp Node Set
20. end While
21. Return the only node left Current Node Set namely the root of index tree T.
```

Algorithm-II: GDFS

```
1. If the node u is not a leaf node then
2. if RScore(Du, Q) > k
th Score then
3. GDFS (u.hchild);
4. GDFS (u.lchild);
5. else
6. return
7. end if
8. if RScore(Du, Q) > k
th Score then
9. Delete the element with the smallest relevance score from RList.
10. Insert a element RScore(Du, Q), u.FID > and sort all the element of list.
11. end if
12. return
13. end if
```

Algorithm-III: Atom Cluster List Generation Algorithm

Considering the document set D as the input raw cluster, we use the bisecting kmeans algorithms to perform top-down bisecting clustering until all the generated subclusters contain less than documents in Algorithms 1 and 2, and thus a binary clustering tree is built as shown in Algorithm 2. Here, is the given threshold for clustering. Then, we traverse the leaf clusters in the generated binary clustering tree, and the atom Security and Communication Networks cluster list L is constructed in Algorithm 3, which is used for building the -filtering index tree.

Definition 1. Atom Cluster. The leaf clusters in the binary tree generated by Algorithm 1 are the atom clusters, where the number of documents in each atom cluster is no more than.

Theorem 1. Assuming that the list of the atom clusters generated by Algorithm 1 is L C 1 , C 2 , . . ., C t , we have the following properties

(1) 1 —C i —

(2) C 1 ł C 2 ł . . . ł C t D

We illustrate the generation process of the atomic cluster list L in Algorithms 13 by an example. We assume that the document set is D d 1 , d 2 , . . ., d 15 and 3. The first round of bisecting clustering is performed on D, and two subclusters are generated as shown in Figure 2. With the same process, the second layers and the third layers subclusters are all sequentially divided into two clusters, and the subcluster stops clustering when the number of documents contained in the subcluster is less than or equal to 3. Finally, a binary clustering tree is formed, where the leaf nodes are C 1 d 1 , d 2 , d 3 , C 2 d 4 , d 5 , d 6 , C 3 d 9 , d 10 , C 4 d 11 , d 12 , C 5 d 7 , d 8 , and C 6 d 13 , d 14 , d 15 , as shown in Figure 2. Then, the algorithm traverses the leaf nodes of the binary clustering tree in the middle order and then the atom cluster list L C 1 , C 2 , C 3 , C 4 , C 5 , C 6 is generated.

IV.RESULT

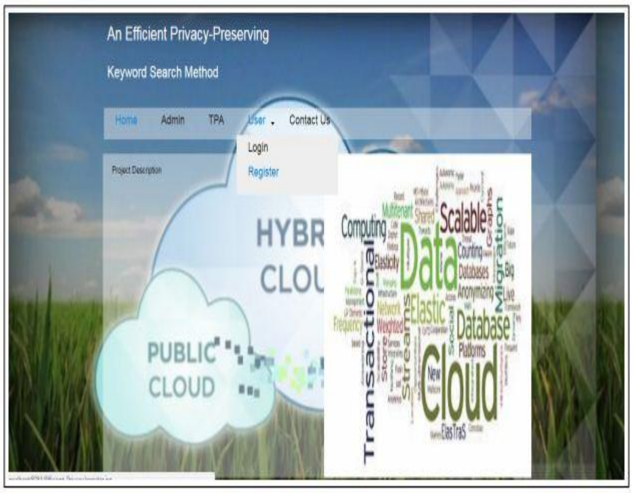


Figure 2: Home Page

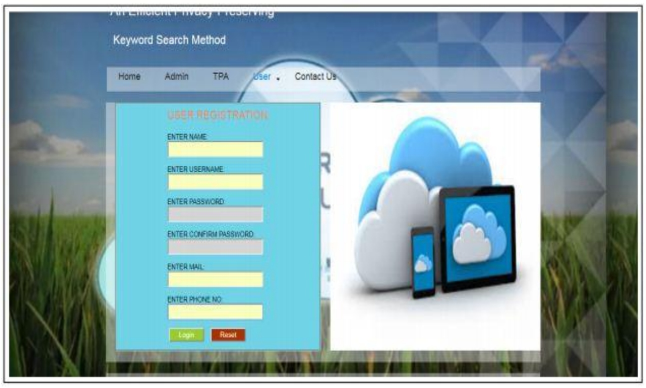
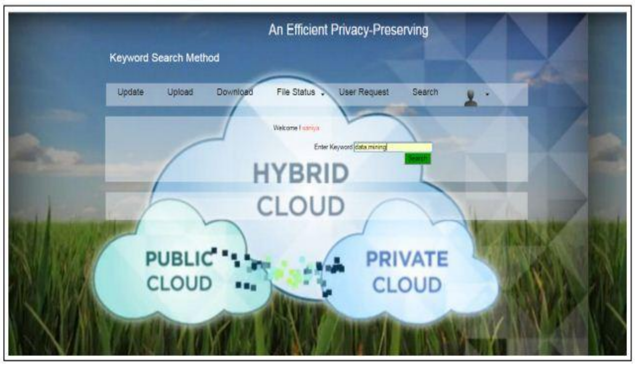


Figure 3: User Registration

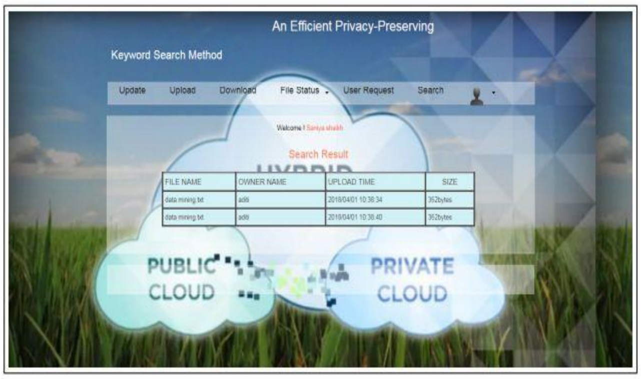


Welcome ! saniya

Enter Keyword: data mining

Search

Figure 4: Search Keyword



Welcome ! Saniya shaikh

Search Result

FILE NAME	OWNER NAME	UPLOAD TIME	SIZE
data mining.txt	aditi	2018/04/01 10:38:34	352bytes
data mining.txt	aditi	2018/04/01 10:38:40	352bytes

Figure 5: Show Result

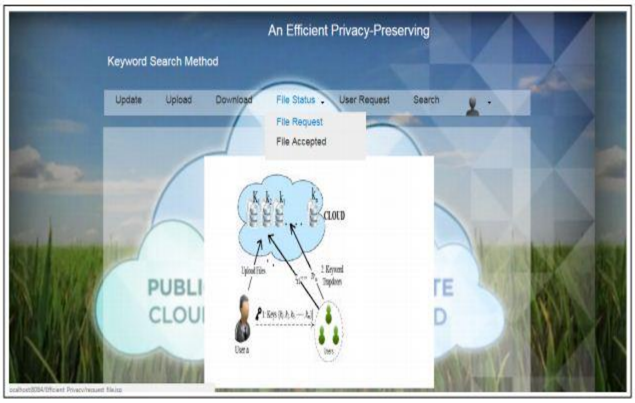
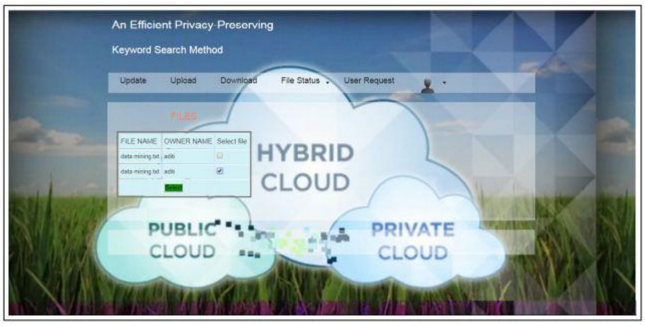
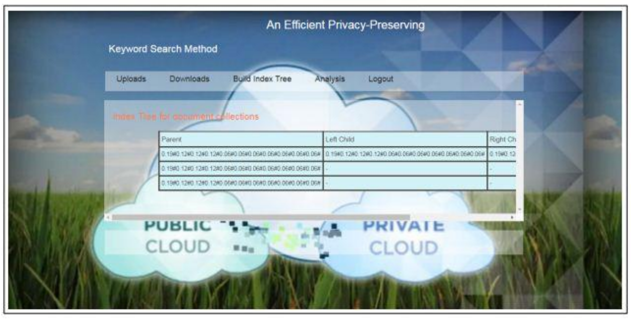


Figure 6: File Request



FILE NAME	OWNER NAME	Select file
data mining.txt	adib	□
data mining.txt	adib	☑

Figure 7: File Select



Parent	Left Child	Right Ch
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	0.19#0.12
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	-	-
0.19#0.12#0.12#0.12#0.06#0.06#0.06#0.06#0.06#0.06#0.06#	-	-

Figure 8: Index Tree For Document Collection

V CONCLUSION

In this System, a safe, effective and dynamic pursuit conspire is proposed, which underpins not just the precise multi-keyword positioned look yet in addition the dynamic cancellation and inclusion of archives. We develop a unique watchword adjusted paired tree as the record, and propose a "Ravenous Profundity initially Search" calculation to acquire better proficiency than direct hunt. Also, the parallel pursuit process can be done to additionally lessen the time cost. The security of the plan is ensured against two risk models by utilizing the protected KNN calculation. Trial comes about illustrate the effectiveness of our proposed conspire. There are as yet many test issues in symmetric SE plans. In the proposed plot, the information proprietor is dependable for producing refreshing data and sending them to the cloud server. Along these lines, the information proprietor needs to store the decoded list tree and the data that are important to recalculate the IDF esteems. Such a dynamic information proprietor may not be extremely reasonable for the distributed computing model. It could be an important however trouble some future work to outline a dynamic accessible encryption plot whose refreshing operation can be finished by cloud server just, in the interim saving the capacity to help multi-watchword positioned look. Furthermore, as the a large portion of works about accessible encryption, our plan for the most part considers the test from the cloud server. In reality, there are many secure difficulties in a multi-client conspire. To start with, every one of the clients for the most part keep the same secure key for trapdoor age in a symmetric SE plot.

REFERENCES

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

[2] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keywordsearch for multiple data owners in cloud computing", in Dependable Syst. Networks (DSN), IEEE 44th Annu. IEEE/IFIP Int. Conf., 2014.

[3] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacypreserving multi-keyword text search in the cloud supporting similarity-based ranking", in Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. secur.,

2013.

[4] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multikeyword search method over encrypted cloud data", in Proc. IEEE 6th Int. Conf. Cloud Comput., 2013.

[5] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption", in Proc. Financ. Cryptography Data Secur., 2013.

[6] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for Boolean queries", in Proc. Adv. Cryptol, 2013.

[7] 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. 14671479, Aug. 2012.

[8] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacyassured similarity search over outsourced cloud data", in Proc. IEEE INFOCOM, 2012.

[9] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data", in Proc. IEEE 28th Int. Conf. Data Eng., 2012.

[10] S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption”, in Proc. ACM Conf. Comput. Commun. Secur., 2012.

[11] B. Zhang and F. Zhang, “An efficient public key encryption with conjunctivesubset keywords search”, J. Netw. Comput. Appl., vol. 34, no. 1, pp. 262267,

2011.

[12] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multikeyword ranked search over encrypted cloud data”, in Proc. IEEE INFOCOM, Apr. 2011.

[13] J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunctions, polynomial equations, and inner products”, in Proc.Adv. Cryptol., 2008, pp. 146162.

[14] E. Shen, E. Shi, and B. Waters, “Predicate privacy in encryption systems”, in Proc. 6th Theory of Cryptography Conf. Theory Cryptography., 2009, pp.

457473.

[15] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption”, in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Tech., 2010, pp. 6291.

[16] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, “Confidentiality-preserving rank-ordered search”, in Proc. ACM Workshop Storage Security Survivability, 2007, pp. 712.

[17] S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption”, in Proc. ACM Conf. Comput. Commun. Secur., 2012, pp. 965976. X. Wen, L. Shao, W. Fang, and Y. Xue, “Efficient feature selection and classification for vehicle detection”, IEEE Trans. Circuits Syst. Video Technol, DOI: 10.1109/TCSVT.2014.2358031.

[18] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications. New York, NY, USA: Springer, 2007.

[19] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, “Secure KNN computation on encrypted databases”, in Proc.ACM SIGMOD Int. Conf. Manag.

Data, 2009, pp. 139152. (2014). Request for comments.

[20] Y. H. Hwang and P. J. Lee, “Public key encryption with conjunctive keyword search and its extension to a multi-user system”, in Proc. 1st Int. Conf. PairingBased Cryptography, 2007, pp. 222

[21] L. Ballard, S. Kamara, and F. Monrose, “Achieving efficient conjunctive keyword searches over encrypted data”, in Proc. 7th Int. Conf. Inf. Commun. Secur., 2005, pp. 414426.

[22] K. Ren, C.Wang, Q.Wang et al.,Security challenges for the public cloud, IEEE Internet Computing, Vol. 16, No. 1, pp. 6973, 2012.

[23] S. Kamara, K. Lauter,Cryptographic cloud storage, In Financial Cryptography and Data Security. Springer, 2010, pp. 136 149.

[24] C. Gentry,A fully homomorphic encryption scheme, Ph.D. dissertation, Stanford University, 2009.

[25] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, In Advances in Cryptology- Eurocrypt 2004. Springer,2004, pp. 506522.

[26] D. Boneh, E. Kushilevitz, R. Ostrovsky, W. E. Skeith III,Public key encryption that allows pir queries, In Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 5067.

[27] D. X. Song, D. Wagner, A. Perrig,Practical techniques for searches on encrypted data, In Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 4455.