ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

An Efficient Pursuit Plan over Scrambled Information on Portable Cloud

Dillibai. R, Sandra Johnson

Department of Computer Science & Engineering, R.M.K Engineering College, Kavaraipettai, India

Department of Computer Science & Engineering, R.M.K Engineering College, Kavaraipettai, India

ABSTRACT: More and more clients would like to store their data into cloud servers along with the rapid development of cloud computing. New accessing and traffic problems have to be resolved in order to help more clients process their data in cloud network. All the cloud have certain space maintenance problems, so that a new mechanism is required in proposed system, which provides Quality of Service based data services over cloud environment. The main objective of the proposed system is to reduce the network traffic by means of single round trip information exchange and the trapdoor compression method as well as the intention is to reducing the data retrieval time and improve the searching accuracy with proper speed. In this proposed system two new algorithms are introduced to resolve the issues found in network environment, called the Trapdoor Mapping Table (TMT) Scheme and Ranked Serial Binary Search (RSBS) Algorithm, which are used to improve the search time by increasing the speed. To improve the security overcloud environment several cryptographic approaches are used. When a cloud user uploads file, the file index is generated automatically and file is encrypted by using Advance Encryption Standard (AES) algorithm with automatically generated key. After that by Visual Cryptography Scheme (VCS), the key is converted into image and then generated as key image and source Images respectively. The encrypted file and the file indexes are stored in storage node, key and source image are stored in cloud server and key image is passed to file owner. Whenever file owner or file users want to download or access files, they perform search and put key image as an input. If valid, it matches the key with the source image and later it is downloaded.

KEYWORDS: Cloud Computing, Trapdoor Mapping Table, TMT, Ranked Serial Binary Search, RSBS, Advance Encryption Standard, Visual Cryptography.

I. INTRODUCTION

Cloud computing is a web/internet – based manipulation strategy, which can be mentioned as the putting away and getting to of information over the web/internet as opposed to your PC's hard disk. This implies the information from either the PC's hard disk or over a devoted hard disk. Cloud computing is put away at a remote place and is synchronized with other web/internet data. Cloud Storage framework is an administration in which information are kept, overseen and reinforced remotely on the cloud side, and in the meanwhile information keeps accessible to the clients over a system. Mobile Cloud Storage
(MCS) indicates a group of progressively well known on-line benefits,and even goes about as the essential record stockpiling for the cell phones. MCS empowers the cell phone clients to store and recover documents or information on the cloud through remote correspondence, which enhances the information accessibility and encourages the record sharing procedure without depleting the neighborhood cell phone assets. The information security issue is fundamental in Cloud storage framework, so the delicate information is encoded by the proprietor before outsourcing onto the cloud, and information clients recover the scheme information by keyword. In MCS, the cutting edge cell phones are gone up against with a considerable lot of indistinguishable security dangers from PCs, and different conventional information encryption strategies are foreign in MCS. In any case, Mobile Cloud storage framework causes new difficulties over the customary scrambled inquiry plans, with regards to the constrained figuring and battery limits of cell phone, and also information sharing and getting to approaches through remote correspondence. Thus, an

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

appropriate and productive encoded look scheme is important for MCS.

II. RELATED WORK

In the year of 2004, the authors Boneh, et. al [1] proposed "Public key encryption with keyword search", in which they described a problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. They refer to this mechanism as Public Key Encryption with keyword search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using this mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. They define the concept of public key encryption with keyword search and give several constructions.

In the year of 2005, the authors Ballard et.al [2] proposed a "Achieving efficient conjunctive keyword searches over encrypted data", in that they described: two provably secure and efficient schemes for performing conjunctive keyword searches over symmetrically encrypted data. Their first scheme is based on Shamir Secret Sharing and provides the most efficient search technique in this context to date. Although the size of its trapdoors is linear in the number of documents being searched, they empirically show that this overhead remains reasonable in practice. Nonetheless, to address this limitation, they provide an alternative based on bilinear pairings that yields constant size trapdoors. This latter construction is not only asymptotically more efficient than previous secure conjunctive keyword search schemes in the symmetric setting, but incurs significantly less storage overhead. Additionally, unlike most previous work, our constructions are proven secure in the standard model.In the year of 2007, the authors "D. Boneh and B. Waters" proposed a paper titled "Conjunctive, Subset, and Range Queries on Encrypted Data", in that they constructed public-key systems that support comparison queries on encrypted data as well as more general queries such as subset queries . These systems support arbitrary conjunctive queries without leaking information on individual conjuncts. In addition, we present a general framework for constructing and analyzing public-key systems supporting queries on encrypted data.

III. PROBLEM STATEMENT

In the past cloud storage schemes, file owner stores the file into the cloud server. So here, lots of file owners access permission in the same cloud server and at that time other file owner will access the other files. Owner can missuse the other owner's file. And the keys generated here can be easily hacked.Tthe search delay mainly composes the trapdoor generation time and document search time and Trapdoor generation time faces challenges in mobile wireless networks: high communication latency, poor connectivity and low network transmission rate. It doesnot care for the authentication process as well as transmitting target documents from the cloud to the user. In past searching schemes,only one search request costs will be high in order to increase network traffic and that is two-round-trip network communication, which is inefficient for users in the mobile cloud environment.

IV. PROPOSED SYSTEM

In the proposed system, the main motto is to secure the user files in cloud storage. Firstly, user uploads the files with their respective login id. The main purpose of Cloud provider is to upload the files with secured image and generating OPE(Order Preserving Encryption)password .The purpose of secured image is, unauthorized user can't access the file in cloud. Here files are encrypted into two parts such as encrypted Index and encrypted files by using FSH (File Hash Splitting Accumulated Hash) Algorithm. As shown in fig1 now after splitting files, it automatically generates a secured image called as (OPE) password which is not known to the third party. The secured keys is converted into two images like source and keyimage by using BVCS (Binocular Visual Cryptography schemes) algorithm. The encrypted file, Source image and OPE have been stored in cloud with respective file. If the user needs to view or select the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

particular file, the request must first be sent to the cloud service provider. The provider

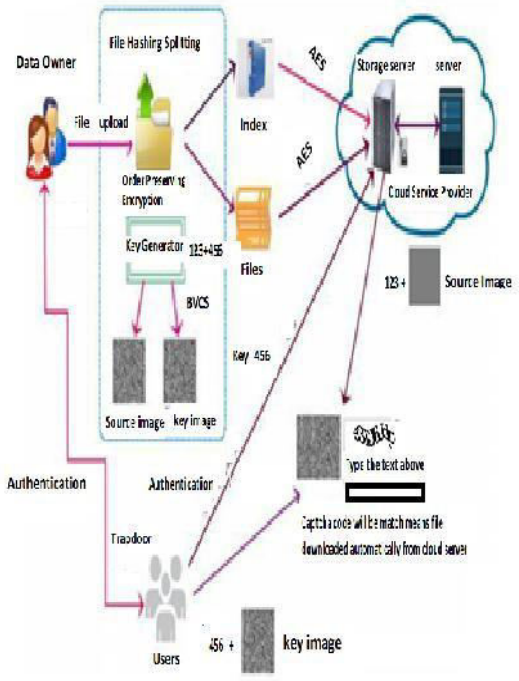

Fig.1 Proposed System Architecture

verifies the user id and file request, later it will send OPE password and key image to user. Now the user has to send the key image to the cloud for accessing the files. The cloud matches the key image with the source image it already has. When both matches, it will send the file in the form of a captcha and it can be downloaded. Hackers cannot hack the source image or key image and captcha will be produced only when it is a valid user.The proposed approach reduces the energy consumption by offloading the computation of the relevance scores to the cloud server as well as the proposed scheme reduces the network traffic for the communication of the selected index, and reduces the file retrieval time in our experiments. It redistributes the encrypted index to avoid statistics information leak, and wraps keywords adding noise in order to render them indistinguishable to the attackers. In the proposed scheme, the traditional encrypted search architecture is examined in terms of network traffic and search time, which shows that the conventional approach is not applicable in mobile-cloud environments.

V. LAYER SHIFT

Layer shift Limited is a global leader in high-quality managed hosting services with infrastructure in the UK, New York, and Singapore. Layer shift's team of virtualization and hosting industry professionals use more than a decade of experience to consistently deliver end- to-end excellence in all aspects of the company, backed by their renowned technical support team achieving exceptionally high customer satisfaction. The backup service performs regular filesystem backups – this takes backups of the Jelastic filesystem, including all files and directories inside each of the environments. Backups are made by taking a block-level copy of the filesystem without needing to understand the file content to be able to reliably restore its data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Benefits

1. It is very low overhead when taking filesystem backups which means no noticeable impact to application performance.
2. The highly sophisticated incremental backup mechanism reduces the amount of time necessary to create each individual recovery point.
3. It can restore individual files or directories (without needing to restore any unnecessary additional data, such as log files)and there is very low overhead, so we can restore backups very quickly.

4. Restores can be performed at any time, including while new backups are being taken.

Limitations

Databases: Reliable filesystem backups of databases can sometimes only be taken when the database server is either not running or is temporarily locked and connections flushed during the backup process. It cannot stop the database during every backup as availability is critical to most of customers so it is recommend to take your own periodic logical backups of any critical data to ensure it can be reliably restored.

Non-portability: These backups can only typically be restored onto the same platform and software stack versions. Layershift take filesystem backups 4 times per day and keep them for 14 days, offering 56 individual restore points. These backups are included free of charge, without any storage limits and are also covered by our robust Jelastic PaaS SLA. For your security, we store all filesystem backups on a secure, high- speed private backup network which is completely isolated from the rest of the platform.

STEP 5: The key and source images are securely stored in cloud server.

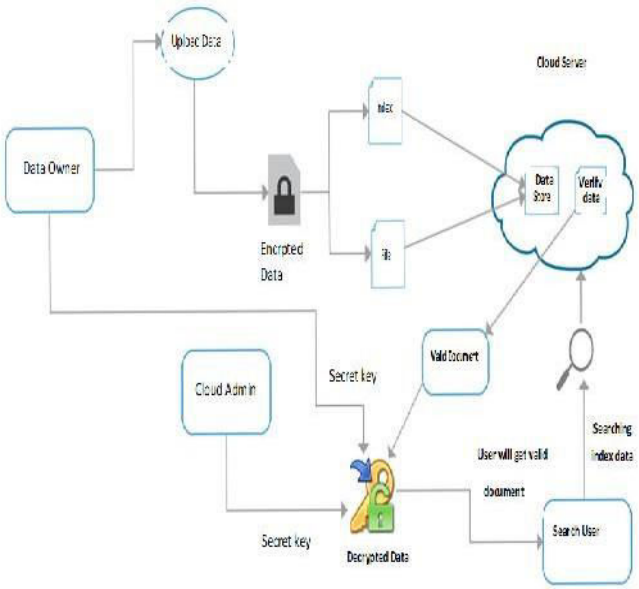

Fig.2 System Block Diagram

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

System Description Algorithm for File Upload:

The following algorithm gives the detailed Procedure for file upload as shown in fig 1

STEP 1: User can upload the file by hash splitting which means the file splits into two parts namely index and file.
STEP 2: The uploaded files are encrypted and secured by AES algorithm and stored in cloud storage.
STEP 3: The Cloud provider upload the files with secured image and OPE password and generates two key one key for index and another one for files.
STEP 4: The image should be splitting into two images like source and key image by using BVCS means (Binocular Visual Cryptography schemes) algorithm.

Algorithm for File Download:

The following algorithm gives the detailed Procedure for file download as shown in fig 1
STEP 1: The user needs to send request to the cloud the cloud data owner will check for the authentication of particular user.
STEP 2: Verification is done on the user side after that the owner will send the key and the key image to the user.
STEP 3: The user has to send the key and the key image to the cloud.
STEP 4: The verification is done in the cloud has verify the key source and the key image.
STEP 5: After verification or the given data is matched with valid data the cloud will send the captcha to the user.
STEP 6: Finally the verification is done after that the user have to type the captcha sent by the cloud so that the file can be automatically download and saved.

Algorithm for key splitting

The two encryption methods used in this work for encryption use different keys. Key splitting module generates two random keys from the main key. It divides the key bits into half i.e. if key is of length n then the generated random two keys will be of length n/2. The pseudo code for key splitting is given below:

STEP1: Input is n bit key
STEP2: Set Key1 and Key2 as n/2 bit value and initialize it to 0
STEP3: Initialize the random function with given seed value. 323
STEP4: Initialize length as n, i=0, j=0, flag=0. STEP5: While (length != 0)
5.1: If Flag==0 then
Find a bit position randomly that has not been used. Find out the value at that bit position in main key.

If value at that bit position is 1 then Set the i'th bit
of key1 as 1 and Increment i value else
Set the i'th bit of key1 as 0 and Increment i value Set Flag=1, Set the above found bit position is used.
Go to Step 5.3 5.2: Else
Find a bit position randomly that has not been used.
Find out the value at that bit position in main key. If value at that bit position is 1 then
Set the i'th bit of key2 as 1 and Increment j value else
Set the i'th bit of key2 as 0 and Increment j value Set Flag=0, Set the above found bit position is used.
Go to Step 5.3
5.3: Decrement the Length; 5.4: Go to step 5
Step6: Return the keys key1 and key2 of size n/2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

VI. EXPERIMENTAL RESULTS

The fig 3 illustrates the Owner Login page of the proposed system. Here the Owner will login

Fig.3 Owner Login

The fig 4 illustrates the User Login Page of the proposed system.

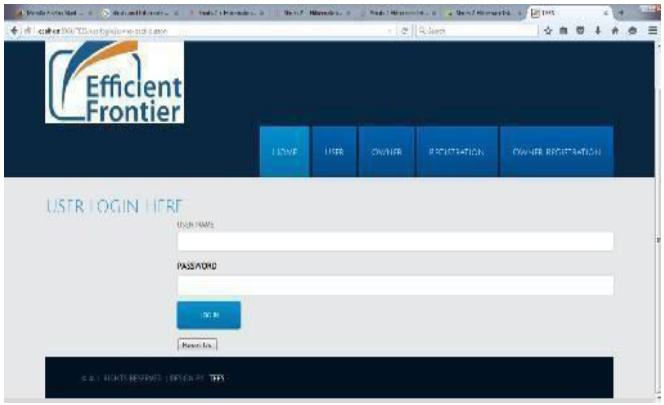

Fig.4 User Login

The fig 5 illustrates the file Permission

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Fig.5 Permission

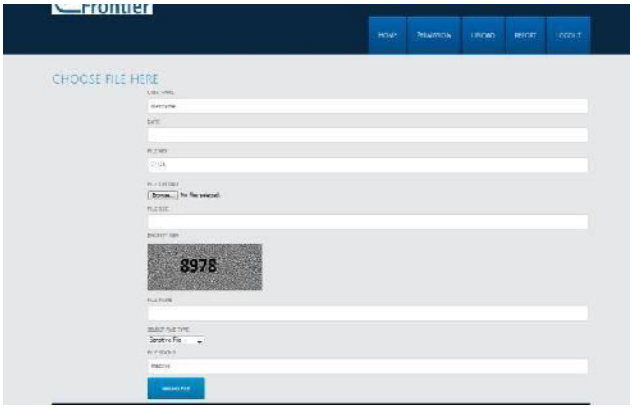

Fig.6 File upload

The fig 6 illustrates the file upload the process.

The fig 7 illustrates the uploading logic of data owner.

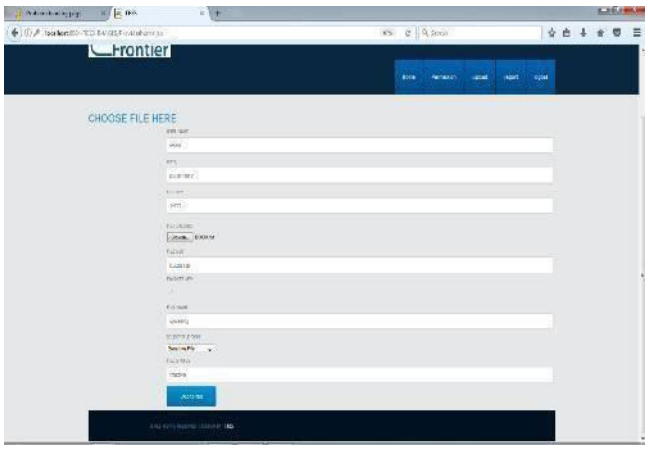

Fig.7 Owner Data Uploading Module

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

The fig 8 illustrates the file search page

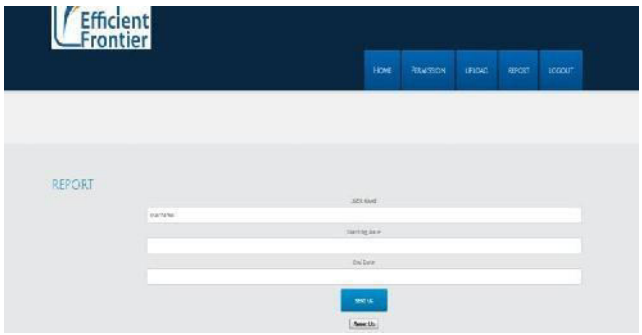

Fig.8 File search

The fig 9 illustrates the admin login page of the proposed system.

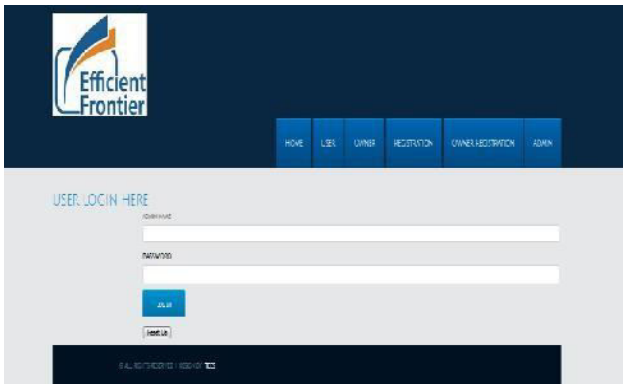

Fig.9 Admin

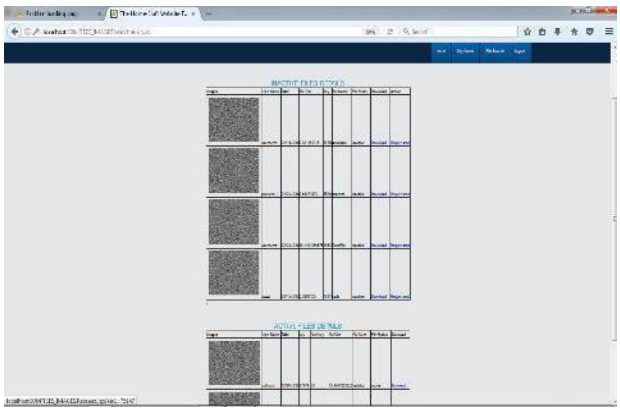

Fig.10 User File Requisition

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

The fig 10 illustrates the user file Requisition.

The fig 11 illustrates verify request.

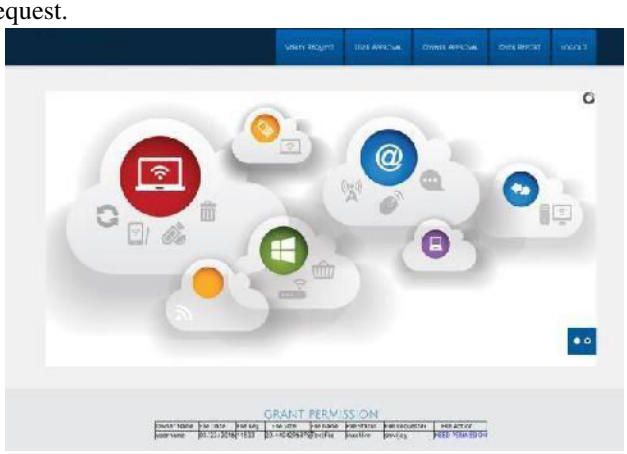

Fig.11 Verify Request

Fig.12 Grant Permission

The f i g 12 illustrates grant permission.

VII. CONCLUSION

In the existing approach, the keys were produced which can be easily hacked and it was done by Data Encryption Algorithm (DES).This is the one of the major disadvantage in that system and it is lack of security. Huge organisations stores their information in cloud and invest more money on cloud server. Hence we propose a new technique by replacing the keys by images in AES algorithm.

VIII. FUTURE WORK

Our future system will be by transferring numerous records in to the cloud server in order to keep away from hacking. Further more to give security, by using AES algorithm with images and can process huge number of files in safe cloud storage.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

REFERENCES

1. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYP'04,volume 3027 of LNCS. Springer, 2004.
2. L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. of ICICS'05, 2005, pp. 414-426
3. D. Boneh and B. Waters. "Conjunctive, Subset, and Range Queries on Encrypted Data," in Proc. of TCC'07, 2007, pp. 535-554.
4. Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS'05,2005.
5. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions, "in Proc. of ACM CCS'06, 2006.
6. N. Cao, C. Wang, M. Li, K. Ren. W. J. Lou, "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data," in Proc. of IEEE INFOCOM 2011, 2011, pp. 829-837.
7. M. Chuah, W. Hu, "Privacy-aware Bed Tree Based Solution for Fuzzy Multi-keyword Search over Encrypted Data," in Proc. of 31st International Conference on Distributed Computing Systems Workshops (ICDCSW), 2011, pp. 273-281
8. P. Golle, J. Staddon, and B. R. Waters, "Secure Conjunctive Keyword Search over Encrypted Data," in Proc. of ACNS04, 2004, pp.31-45.
9. E.-J. Goh, "Secure indexes," Crytology eprint
10. Archive, Report 2003/216, 2003, http://eprint.iacr.org/.
11. Y.H. Hwang and P.J. Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System, "in Proc. of Pairing'07,2007,pp.31-45.
12. J.Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W.
13. j. Lou, "Fuzzy Keyword search over encrypted data in cloud computing," in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March2010.
14. C. Liu, L. H. Zhu, L. Li, and Y. Tan "Fuzzy Keyword search on Encrypted cloud storage Data with Small Index," in Proc. of IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS) 2011, pp.269-273.
15. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00,2000.
16. E. Shi, J. Bettencourt, T.H.H. Chan, and D. Song,
17. Perrig. "Multi-Dimensional Range Query over Encrypted Data," in Proc. Of IEEE Symposium on Security and Privacy (SP'07), 2007, pp.350C364.
18. C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure Ranked Keyword Search over Encrypted cloud Data," in Proc. of IEEE 30th International Conference on Distributed Computing Systems (ICDCS), 2016, pp.253-262.