OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

PRAVACY PRESERVATION MULTIKEYWORD SEARCH SCHEME USING ED SERVER ON MOBILE CLOUD

Mr. Rajan Nemade[1] Mr.Harish Barapatre[2] Prof.Ankit Sanghavi[3] Ms. Juli Sarode[4]

PG Scholar, ARMIT , University of Mumbai, rajan.nemade@gmail.com[1]
Assistant Professor, YTIET, University Of Mumbai, harishkbarapatre@gmail.com[2]
Assistant Professor, ARMIET, University Of Mumbai, ankit.s.sanghvi1@gmail.com[3]
PG Scholar, YTIET , Mumbai University, juili.sarode01@gmail.com[4]

Abstract- In the Mobile Cloud Data security is most important and valuable are in the research field which provides storage security with low cost and high confidentiality, but people are afraid of data privacy which prevent them from storing files on the mobile cloud storage. Most of the mobile cloud systems provide the low security which means our valuable data in cloud easily access by the third party users. Here we have consider data Privacy and multi keyword searching scheme from encrypted mobile cloud data which Encryption scheme reduces overhead on mobiles. Most of the mobile cloud system consumed more energy while encrypt their data that is main region which loss their data privacy. Our main aim is to minimize the energy consumption and reduces the burdon of mobile cloud data. In this paper, our proposed symbolic encrypted algorithm system gives the encrypted data in different symbolic because we need to achieve the data privacy. ED server is important part of this research is to reduce the burdon the computing power and accessing Trapdoor with the Special OTP which achieved high security and improves the performance of the computing power.

Keywords: *ED Server, OTP, OWNER, Privacy.*

I INTRODUCTION

In today’s world, Mobile cloud computing system is portable, secure, energy saving and fast data searching technology as well as many researcher has found the original research in this area. In day by day every users uses the smartphone for securely uploading and downloading the structure and unstructured data in the cloud system but the unauthorized activity can’t do this while uploading and downloading and easily third party access this valuable data. Researcher mainly focuses on security of the data that is data privacy which reduces the burdon of the mobile computing system and network Traffic. Most of the mobile cloud data encrypted multi keyword searchable techniques are depends on network bandwidth, energy consummation while retrieving the data. Mobile Cloud storage is a Service model where data is managed, maintained and backup remotely which continually maintained encrypted data on client side [1] [4]. Every cloud system maintained the data privacy in encrypted form that is uploading and downloading operation is performed in the form of encrypted/ decrypted data. The main drawback of the system is data have not much more secure while uploading and downloading; Traffic energy consumption is more [1]. To overcome the all drawbacks of existing system, in mobile cloud storage needs best cryptographic high data privacy algorithm which reduces the burdon of cloud storage.

Here we have described the need of mobile cloud computing. [7] [13] A company having 1000 of employers, each and every employee has to upload and download the company data from its own cloud. While they transfer their own data through mobile to mobile, they required the more storage space in mobile as well as in receivers side they can’t gets the exact data because the more packet are loss in network traffic consumption while transferring the data through a mobile to mobile. So in the today's world every smart user has access their own private or public data from cloud storage but the important point is that the third party accessory (Hackers) are accessed these valuable data from cloud and performed their illegal activity and loss our valuable data. Here we can't achieve data Privacy, for that purpose we need the data in encrypted and symbolic format so we can easily achieve the data privacy.

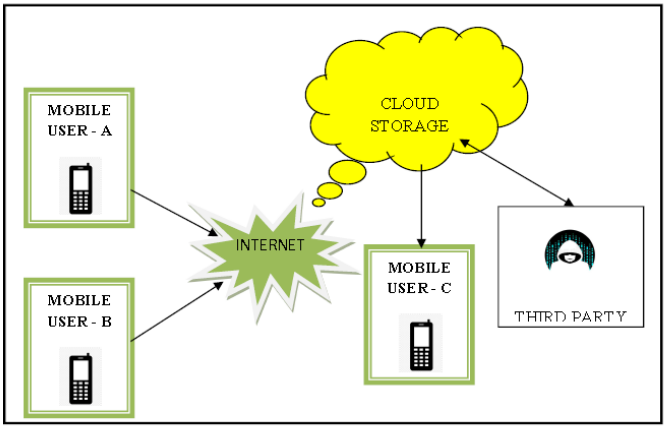


Figure No-1: Mobile to Mobile Cloud Communication

As in figure no-1 represents mobile user-A and B are upload their company valuable data , mobile user- C wants to download their company data but the third party (Hackers) has corrupt their company data. So here we need the cloud storage data in unreadable format and security from third party accesscer. Our research is mainly focusing on data privacy algorithm [6] [15] and how to reduce the burdon of the cloud server which reduces the network traffic.

In the next section we will explain the views and ides of the various authors that was work on related to this topic. We have introduced about ED (Encryption and Decryption) server which reduces the traffic energy consumption and maintaing the data privacy which explained in sanction III. Than after we w explain proposed architecture in module IV and rest of the section we described the proposed algorithm and results.

II RELATED WORK

Earlier cloud server has to perform search over the encrypted content. They used Boolean keyword search and [3] Boolean keyword search and ranked keyword search. Rank keyword search sends all the matching retrieved files to client basing on the match of keywords where as Boolean key word search is bringing Large network traffic and not so much efficient keyboard search is efficient than Boolean keyword search . Here In the above two approaches all the data encrypted is downloaded, decrypted and giving results to client, which is not so efficient. [7] Later on conjunctive keyword search they have been proposed thus implement features like aggregation query computation and range query search but these methods all suffered with huge computation cost. No, [4] previous (BKSE) Boolean keyword search encryption scheme has supported multiple keywords ranked search, on the encrypted cloud content or data. Private Information Retrieval problem was introduced by the person named Chor et al. [6] It was published in IEEE publication in the year **06** August 2002. This paper was entitled as" Private information retrieval". Now in recent past by Growth et al who proposed multi query PIR method which followed constant communication rate. PIR-based technique need to hide access patterns so, it uses costly cryptographic operations. This is impossible task in large scale cloud system. Privacy preserving search is designed to hide the content of the retrieved data. Ogata and Kurosawa based on RSA blind signatures designed privacy preserving keyword search protocol. This PIR-based technique uses for every item in the database and for every query a public key operation and the every operation done on user side. R. Curtmola **, he has** suggested the need keyword fields in the index.[13] Here user should list all valid keywords and their corresponding positions surely for information to generate a query. Said approach1 may not be applicable to all cases. This may not be efficient as it have matrix multiplication operations for square matrices and number of rows may be of several thousands and they also follow certain order for each and every row.

III. ED Server

ED (Encryption and Decryption) server is the main component of our research which reduces the burdon of the cloud server and reduces the network Traffic which saves the energy. ED server is a server which managed the multiple request and reply packets of data uploader and downloader. It also generators trapdoor for the data Privacy. ED server checks OWNER and USERS are authentic or not through Trapdoor. Trapdoor is one of the gateways which permit the authentic users and owner for the encryption and decryption. It checks the validation through the OTP (One Time Password) which generates the continues random Number.

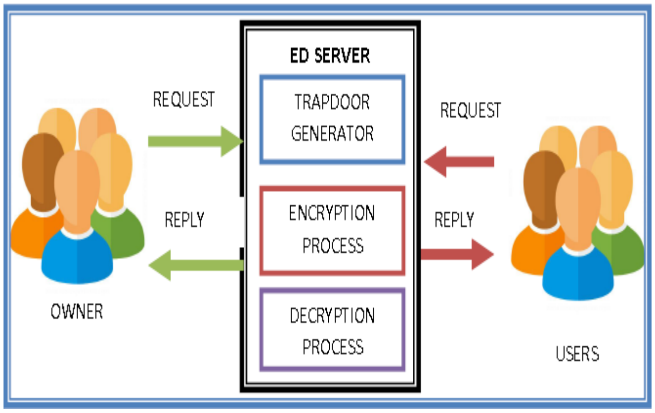


Figure No-2: ED Server Structure

ED server Consists of mainly Three Blocks which shown in figure N0-2. **OWNER** send request with file for the encryption purpose and it will go through the Trapdoor for authentication Purpose. Trapdoor checks the valid authentication through the OTP which sends random numbers on OWNER's mobile. It checks the validity. If the validity is found than it will encrypts their file for uploading on mobile cloud server. If not than Trapdoor is block the OWNERS. Same thing Decryption process was performed in Users side while downloading the Cloud data.

IV PROBLEM DEFINITION

Previously in single-owner schemes, the data owner should stay online to generate trapdoors or the encrypted keywords to data users. This is ok, if there is single user but what happens when more data owners are involved. They have to stay online simultaneously for generating the trapdoors. If, it is so, the flexibility of the search system is affected. We have many more problems with earlier systems where we are not willing to share our secret keys; data owners would use their own secret keys for encrypting the data. It is challenging to perform a secure and efficient search on the data encrypted with various keys. [13] We have one more problem where we have large number of data users and huge documents in the cloud, to access data is challenging. There is a need of multi keyword search query and effective data retrieval methods. So, as to enrich the user searching, we need ranking system which is supporting multiple keywords search and encryption methods to give encrypted data. Huge amount of data owners are asked to stay online to generate trapdoors as single or less data owners for using search system. Data owners maintain their own secret keys to encrypt or secure data with different secret keys and this task is challenging. If there are multiple data owners they should undergo enrolment and revocation techniques, so that our system enjoys security.

V. PROPOSED SYSTEM

In this proposal system a technology named traffic and energy saving encrypted search procedure. Security calculation to cloud server has been offloaded for the energy consumption of mobile device this presented system is providing security to cloud storage from the information leak with good encryption a methods multi keyword module used helps to gat accurate results based on multiple keyword concept. Our proposed research is network Traffic and Energy saving Encrypted Search using ED server approach for cloud storage in mobile applications. ED server allows changing the ranked keyword search with the encrypted search platform in cloud storage systems. ED server is focused on security level of encrypted data on cloud, that's why ED Server resolved security defects which maintained the data privacy.

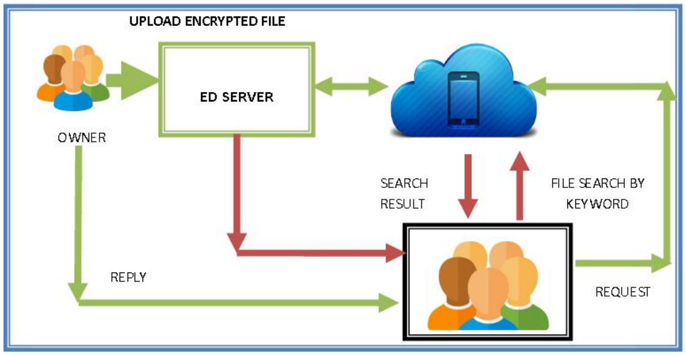


Fig No-3: Proposed System Architecture

In this proposed multi-owner and user cloud computing approach there are four entities, as illustrated data owners, cloud server, ED server and lastly data users. Data owner data module is taking care of collecting documents for uploading on cloud server which can access by authored user. ED server converts that file into encrypted form and provides the encrypted file with Data with security key which share with owner and user and data owner assign some keyword to that encrypted file and upload on mobile cloud with security key. Data User (downloader) is search a file by using multiple keyword, cloud server gives the appropriate search result to data user with the file details like filename, data owner, their authorization by the data owner before getting access to the data, user sends file access request to data owner, data owner check the user detail if found is valid than owner shares the key with user. Data User send file access request with the key to ED server than ED server again checks the validity through trapdoor that is Sending OTP verification 4 digit code if success than user can download the file and decrypt it **Cloud server** allocates huge storage space, and the resources for computation required by cipher text search. After getting request from user, server searches the encrypted index, and sends documents matched the data users query. This system protects data from leaking information also to cloud server and also we improved the efficiency of cipher text search. Whenever data owner want to view files he is authorized by ED server. ED server trapdoors all this data to cloud server and Cloud server encrypts the index files and make some calculations and rank encrypted files. Whenever the data owner wants the encrypted data is retrieved from cloud. The client is retrieving the encrypted file and is the data is decrypted at the client end. After all the operations are completed data is saved at the cloud end. This proposed system flexibilities are prompting both individuals and enterprises to convert complicated data to the cloud administration. Cloud Service provider is unaware of the original content and their data owner as data is encrypted it is more secure. There is great purity in recommended or retrieved documents by the mobile cloud.

VI. ALGORITHM DESCRIPTION

Algorithms can perform automated reasoning, calculations and processing data tasks. An algorithm is expressed within a finite amount of space and time and it defines a language to calculate a function. For encryption we used the following algorithms

Algorithm-1: Key_Generate

1. Define Constant Random String length with Randum_String_Length=10
2. Initialize CHAR_LIST Array with String is ”a TO z and A to Z also 0 To 9”
3. Collect All Character from CHAR_LIST and shuffle it.
4. Get random Number RANDUM_NUMBER with Appending All Character
5. Add Numerical Value into RANDUM_Number.
6. Get The Unique RANDUM_Number.
7. Send To Register EMAIL for the Decryption.

The algorithms are used for Random number key generation, the data owner and data user generates the security key using this algorithms. Its provides the more secure and authorised code.

Algorithm-2: Bluefish Symbolic Encryption Decryption (BSED)

1. Select the FILE URL with ATTRIBUTE Value from CONTRIBUTOR and Identify Each Attribute is Unique or Not.
2. If The ATTRIBUTE is Unique than Replace the file Contents with SUMBOLIC_ENCODER.
3. Generate SUB Keys and call KEY_GEN method Attribute Value.
4. Define 3-Array NUM[] , CHAR[] & SYMBOL[] , all special character And Numbers [Each character define a special symbol with number like A=@5 a=@1 stored into symbolic Array]
5. Initialize All Array NMU[]={0,1,2,3,4,5,6,7,8,9}, CHAR[]={a to z and A to Z}, SYMBOL[]={!@#$%^&*()+?/”:;}{|*~` And For Blank Space=}
6. Encryption Process
   a) Takes an Input as Plan text from File and Replace each character with unique symbol with number by substitution method.
   b) After Substitution Process, Start the Symbol Swapping process (swap the first and last symbol, second and second last ……. So on)
   c) Gets Encrypted text in Symbolic form.
   d) Scan the next line and goto Step a to c are repeated Upto the end of file.
7. Gets Encrypted file and allocate the Unique Key while will be uploading on cloud.
8. The Decryption Process is same as to Opposite to Encryption process.

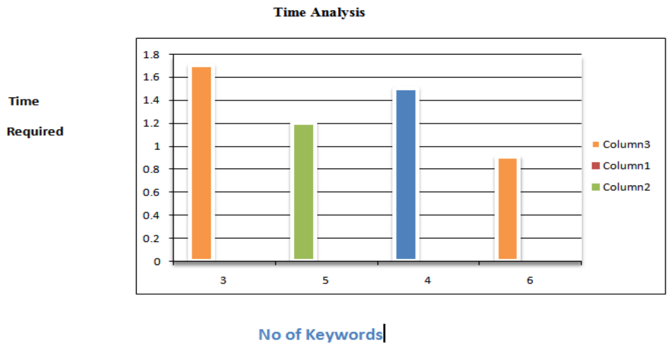
BSED algorithms are more secure and fast processing algorithms with 3 security layers used for the encryption and decryption purpose. We have compare this algorithm with AES and Bluefish 64-bit algorithms and

Algorithm-3: OTP (One Time Password)

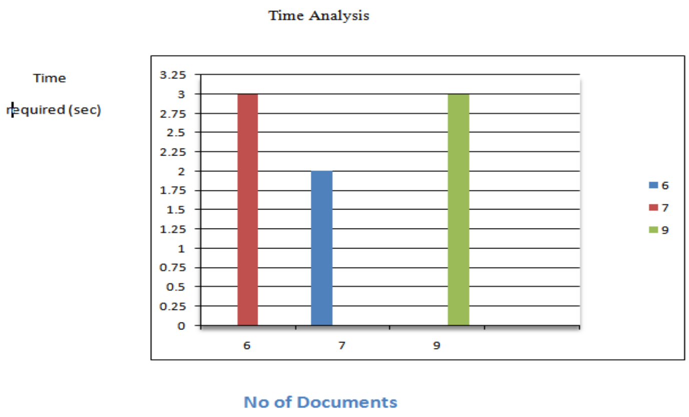
1. Collect Current User (Receiver (Uploader/ Downloader)) Registered data with Email and Phone Number.
2. Assign The Sender Authentication email with password (admin)
3. Initialize the mail server and text message server.
4. Stored Receiver Email and mobile number in variable.
5. Generate 4 Digit Random Number using mod (%) operators which calculated New OTP using Add function.
6. Stored on mail srever and call the SEND () which send the Password on receiver email and Mobile.
7. Receiver enters the 4 Digits OTP which received on his mobile and email.
8. Validation Check with email server data if correct than authorization otherwise defines illegal activity.

VII. PERFORMANCE ANALYSIS

In this scheme we analyzed Time Analysis on the time required in seconds against Number of given keywords on Y axis. Time analysis is varying with variation in total number of keywords.



Below made one more analysis basing on time required and total number of documents. Time analysis is varying with varying document size when compared with existing system. It is giving better results in less time when compared with single keyword search model.



VIII CONCLUSION

In this proposed paper, we solved the problem of mobile cloud security which multi-keyword search performed on the remote encrypted database using ED server where the existing bluefish all users are getting protection against security violations. Initially security requirements for the given problem are well defined. Secondly secure usage of total number of keywords searched is relatively limited and there are by trapdoor system which is generated by the data owner with the help of ED server. Efficiency of the scheme increased with the usage of symmetric-key encryption technique .Here algorithm called Symbolic encryption method used for accessing contents of the accessed documents without permission of data owner identity to third or other parties. This proposed method solves all the security requirements in mobile Cloud. This symbolic method very well retrieves relevant documents related to our submitted search terms. All the mentioned schemes are experimented and results demonstrate the effectiveness of our proven solution.

New architecture, it was implemented for the Secure searching and securely transferred the data between the cloud and multi users. This approach is time and energy consuming and provides 3 levels more security when compared with keyword search within plain-text.

IX FUTURE WORK

Our work can be further expanded to more new implementations. In our model we proposed a multi keyword search scheme using ED server for making the encrypted data search on mobile cloud. We have possible extensions to our current work are still remaining. But, there still remaining certain problems such as time and bandwidth consumtion.

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] 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. 222–23 2014.

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

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

[5] C. Orencik, M. Kantarcioglu, and E. Savas, `` A practical and secure multi-keyword search method over encrypted cloud data”in Proc. IEEE 6th Int. Conf. Cloud Comput., 2013.

[6] S. Kamara and C. Papamanthou, “Parallel and dynamic searchable symmetric encryption "in Proc. Finance. Cryptography Data Security, 2013.

[7] 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.

[8] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling secure and efficient ranked keyword search over outsourced cloud data”, IEEE Trans. Parallel Distrib. System., vol. 23, no. 8, pp. 1467–1479, Aug. 2012.

[9] C. Wang, K. Ren, S. Yu, “Achieving usable and privacy-assured similarity search over outsourced cloud data” in Proc. IEEE INFOCOM, 2012.

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