VOL. 13, NO. 16, AUGUST 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A NOVEL AND EFFICIENT MOBILE CLOUD SERVICE FOR SEARCHING ENCRYPTED DATA

K. Aravind[1], J. Granty Regina Elwin[2], T. Sujatha[2] and S. Balakrishnan[2]
[1]Department of Information Technology, Sri Venkateswara College of Engineering and Technology, Chittoor, India
[2]Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India
Email: ramesh4477@gmail.com

ABSTRACT

Document storage in the cloud framework is quickly picking up ubiquity all through the world. Nonetheless, it postures dangers to customers unless the information is scrambled for security. Encrypted data ought to be viably searchable and retrievable with no protection spills, especially for the versatile customer. Albeit late research has settled numerous security issues, the design can't be connected on cell phones straightforwardly under the portable cloud condition. This is because of the difficulties forced by remote systems, for example, latency sensitivity, poor connectivity, and low transmission rates. This prompts a long inquiry time and additional system activity costs when utilizing customary hunt plans. This review addresses these issues by proposing a productive encrypted data search plot as a mobile cloud service. This creative plan utilizes a lightweight trapdoor (encrypted keyword) pressure strategy, which enhances the information correspondence handle by decreasing the trapdoor's size for activity effectiveness. In this review, we additionally propose two enhancement techniques for record seek, called the trapdoor mapping table (TMT) module and ranked serial binary search (RSBS) calculation, to speed the inquiry time.

Keywords: mobile cloud, encrypted data search, trapdoor mapping table, ranked serial binary search.

1. INTRODUCTION

Cloud computing [4] has an awesome request asset, and web based processing and which can be utilized to store the information and get to. It is valuable in business application by utilizing cloud we may get benefits in business and it is exceptionally shoddy at cost of administration and get elite. It is exceptionally useful to people in general clients.

The outsourced information contain sensible data in view of that we are giving security to the information and put away in the cloud server in this we need to scan for watchwords by utilizing searchable encryption. The searchable encryption has been as of late created. In this we have an information proprietor, cloud server and an inquiry client. The information proprietor creates catchphrases for (outsourced) a record set .In this document set; we have entire reports which can be kept in a document organization which can be inquiry by the hunt clients. Information proprietor scramble the aggregate document set and send to the cloud server and inquiry clients can get to the catchphrases by utilizing trapdoor once we can look in one heading and get the outcomes. In this we have different clients need to seek the information at once. Beforehand we have positioned look, file seek and versatile inquiry are there. It should be possible on predefined. Fine grained hunt is utilized to seek top to bottom and detail and we get the fine points of interest in results.

Mobile cloud computing is a type of circulated figuring innovation. It is an improvement of circulated handling, parallel preparing and matrix figuring. Its most fundamental ideas is that consequently split a tremendous measure of count program into various littler subroutines through the system, and after that given over to the operation framework that comprises of a few servers. Subsequent to computing and breaking down, it will handle the outcomes and return them to the client [1], [2]. Notwithstanding the buildup accomplished by portable distributed computing, the development of the versatile distributed computing supporters is still beneath desires because of the dangers related with the security and protection. To have an in profound comprehension of Mobile Cloud Computing and its system security, it is important to get the total handle on portable distributed computing. Where client can lease programming and equipment foundation and computational assets according to client fundamental computing idea, innovation and designs have created and solidified in the most recent decades.

Mobile computing let you get to all your application and archives from anyplace on the planet. It is simpler for gathering individuals in various areas to work together. Distributed computing is not arranged registering. Also, it is a great deal greater than that. The mobile cloud computing (MCC) is internet-based information; applications and related administrations (figuring) get or recover from a capacity gadget as of data on gotten to through Smartphone's, PCs, and other compact gadgets [1], [2]. For secure correspondence over open system information can be ensured by the technique for encryption. Encryption changes over that information by any encryption calculation utilizing the "key" in mixed shape. Just client approaching the key can unscramble the encoded information [3].

2. RELATED WORK

Software protection is a standout amongst the most the ranked keyword search will return archives to the significance score. Zero *et al.* proposed a novel procedure that makes the server side complete the hunt operation. Consequently it will be send inconsequential reports then client need to channel these archives. It might drives

misuse of activity which is unsafe to portable cloud. Groves *et al*. proposed an appropriated cryptographic framework that protected the security of the report recovery prepare and the high accessibility of the framework, however this framework experiences two system round treks and figuring multifaceted nature for target records.

Wang *et al,* [5] proposed a plan which is single scrambled hunt plot; however their framework is not sufficiently secure, as it releases the watchword and related record data from different catchphrase seeks. Li et.al, [6] proposed a solitary watchword encryption look conspire using positioned catchphrase seek, which arrange correspondence between the client and the cloud by exchanging the processing trouble from the client to the cloud.

In these reviews we proposed Encrypted data search framework which is help for stay away from system trafficking and less inquiry time when contrasted with the past framework and furthermore help for break down with the past encoded look framework and bottleneck in the versatile cloud.

The possibility of searchable symmetric encryption (SSE) is at first made by Song *et al*. likewise, Wang *et al*. are developed the positioned catchphrase look plot, which consider record document. On the other hand, the above arrangements can't beneficially support multikeyword look for which is for the most part used to give the better understanding to the chase customer. Afterward, Sun *et al* [7] propose a multikeyword look for plan which considers the rundown record of watchwords, and it can fulfil profitable request by utilizing the multidimensional tree technique.

Balakrishnan *et al,* [8] show that different stage recuperation of areas is feasible to decrease the record recuperation delay. We initially add to a defer show for various stage recuperation arranges material to our considered system. By utilizing LT– code ask for systems we can defeat the current issues, and the while n-number of client attempt to get the download a similar record in the meantime, document will get the download from the server hub, all the document would originate from the splited server hubs. While transferring the record into the cloud that will consequently will get splited into "n" documents. Janet *et al* [9] expand on how enhanced information exchange planning and streamlining can moderate the vast scale information move issue in distributed computing.

3. PROPOSED ARCHITECTURE

The trapdoor era prepare and the cloud seek calculation are retrofitted to decrease look deferral and system movement. For trapdoor era, this framework stores a precomputed Trapdoor Mapping Table (TMT) in cell phones, which maps regular English words to relating trapdoors. At the point when the cell phone starts a pursuit demand, the trapdoor is turned upward from the table as opposed to being asked for from the supplier. This enhancement spares one system round trek for the trapdoor era. Moreover, this framework additionally gives new calculations to advance and pack trapdoors to lessen arrange activity to transmit trapdoors.

The proposed system architecture is given in the Figure-1.

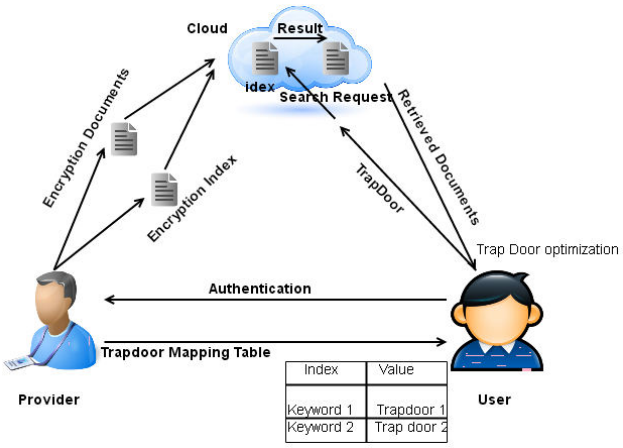

Figure-1. Proposed system architecture.

The proposed system consists of the following parts, namely: mapping table module, compression module, ranking search module, encrypted search module, mobile cloud module and index encryption

Mapping table module

"Denoting the total calculation time for generating trapdoors for one keyword, two keywords and three keywords respectively the encryption time occupies nearly 85% of the total calculation time". This is because that the encryption operation requires more computing resources than others, as it accumulates all terms together to generate a hash code. To reduce trapdoor construction time, our method ships the encryption process from the online approach to offline.

Compression module

It uses "Trapdoor compression method. The key idea behind this trapdoor compression method is that we utilize the location of each trapdoor's characteristic bit to represent this trapdoor, since characteristic bit 0 can show all the features of the trapdoor and also occupy a much smaller proportion compared with non-characteristic bit 1". We first analyze the availability and then provide the detailed design for the compression Method.

Ranking search module

The efficient search algorithm proposed by this system relies on a binary search tree structure to accelerate indexing. In the section, we will first "introduce the conventional privacy-preserving index construction procedures, including index construction, index slicing as well as index encryption, and then elaborate our binary search tree construction to accelerate index matching". Finally we will present our RSBS algorithm which leverages this data structure to perform privacy-preserving searches more efficiently.

Use case diagram is given in the Figure-2.

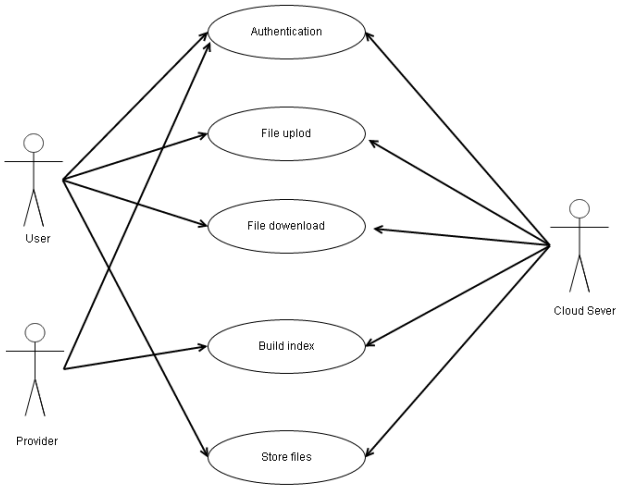

Figure-2. Use case diagram.

Encrypted search module

Upon receiving a trapdoor the cloud would perform a privacy preserving search from the indexes provided by the provider. Then it selects top-k documents that contain the given search keywords. This process is achieved by using the RSBS (Ranked Serial Binary Search) algorithm. The RSBS algorithm aims to "find the top-k documents that best match the search keywords provided by the user". To this end, it maintains a score array for each document. The main idea is to compute accumulated scores for each document and then selects the top-k ones.

Mobile cloud module

In traditional systems, "the index without binary optimization is only the TF-IDF index, while the optimized index A is used in this system". In this study, we divided each document's index into 550 slices; that is, in this system, each document's index has 550*2-1=1,099 columns after they are optimized with the binary tree principle. We conducted 10,000 queries with random chosen keywords for the single keyword search, the two keyword search and the three keyword search, respectively.

Index encryption

The provider then encrypts each index with a given FAH (Fast Accumulated Hashing) algorithm by encrypting each index's slices, before sending them to the cloud. We base our scheme on previous privacy-preserving. Here the FAH encryption algorithm for document indexes is employed. By utilizing this FAH algorithm, we encrypt slices of each index.

4. ALGORITHMS USED

4.1 RSBS algorithm

The indexes provided by the provider while receiving a trapdoor, the cloud would perform a privacy preserving search. Then it pick up top-k documents that contain the given search keywords. The Algorithm 2 explain how the RSBS algorithm is achieved.

Algorithm 1:
Ranked serial binary search (RSBS) algorithm.

Input:
Noised trapdoor: t1
The number of document to return: k
Encrypted document indexes: E
Document request: D

Steps:
1. Create the scores as an N zeros
2. for i = 1 to N do
3. for n = 1 to E do
4. find the keywords appears in any of the s slice of the document
5. end for
6. end for
7. receive the top-k documents
8. return D

The binary search will start from the binary tree we constructed and descend to a slice that contains the keyword or find that the keyword does not appear in the document. If the keyword appears in the document, then the score will be calculated and updated to the Scores array. Otherwise, a zero will be recorded.

4.2 Trapdoor generation algorithm

Algorithm 2:
Trapdoor Generation Process

Input:
Keyword: K
Mapping function in FA
H algorithm: M ()
Hash function in FAH Algorithm: H ()
Noise set: N

Output:

Index: Compressed trapdoor t

Steps:
1. Extract the term t from k
2. if the term t hits in the TMT module then
3. Obtain its pure trap door without any noise
4. else
5. Hash it by H() and Map it by M() ,there will be some bits found
6. end if
7. Choose f noises from the noise set N to form a subset
8. Each characteristic bit 0 to calculate the location to get a compressed Trapdoor
9. return t

5. CONCLUSIONS

In this paper, we proposed a novel encoded search framework over the mobile cloud, which enhances arrange movement and inquiry time effectiveness contrasted and the conventional framework. We began with a careful investigation of the conventional scrambled pursuit framework and dissected its bottlenecks in the portable cloud: arrange activity and hunt time wastefulness. At that point we built up a proficient engineering of this framework which is appropriate for the portable cloud to address these issues, where we used the TMT module and the RSBS calculation to adapt to the wasteful inquiry time issue, while a trapdoor pressure technique was utilized to decrease arrange movement costs.

REFERENCES

[1] S. O. Kuyoro, F. Ibikunle and O. Awodele. 2011. Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN). 3(5).

[2] Rajesh Piplode, Umesh Kumar Singh. 2012. An Overview and Study of Security Issues & Challenges in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering. 2(9), ISSN: 2277 128X.

[3] Abid Shahzad and Mureed Hussain. 2013. Security Issues and Challenges of Mobile Cloud Computing. International Journal of Grid and Distributed Computing. 6(6).

[4] Balakrishnan S., Janet J., Spandana S. 2017. Extensibility of File Set Over Encoded Cloud Data Through Empowered Fine Grained Multi Keyword Search. In: Deiva Sundari P., Dash S., Das S., Panigrahi B. (eds) Proceedings of 2nd International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, Vol. 467. Springer, Singapore.

[5] P. Wang, H. Wang, and J. Pieprzyk. 2009. An efficient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data. pp. 145-159.

[6] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren and W. Lou. 2010. Fuzzy keyword search over encrypted data in cloud computing. in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA.

[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou and H. Li. 2013. Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. IEEE Transactions on Parallel and Distributed Systems, vol. DOI: 10.1109/TPDS.2013.282.

[8] J. Janet, S. Balakrishnan and K. Somasekhara. 2016. Fountain code based cloud storage mechanism for optimal file retrieval delay. 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, pp. 1-4. doi: 10.1109/ICICES.2016.7518901.

[9] Janet, S. Balakrishnan and E. Murali. 2016. Improved data transfer scheduling and optimization as a service in cloud. 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, pp. 1-3. doi: 10.1109/ICICES.2016.7518895.