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 12, December 2018

# Traffic and Energy Efficient Encrypted Search

Tanvi Lalit Sardare, Dr. Dayanand R. Ingle

M. E Students, Department of Computer Science Engineering, Bharati Vidyapeeth College of Engineering, Kharghar, Navi Mumbai, India.

HOD, Department of Computer Science Engineering, Bharati Vidyapeeth College of Engineering, Kharghar, Navi Mumbai, India

**ABSTRACT:** Cloud storage delivers cost-effective, massive and scalable storage at very low cost, but data security is a major concern that prevents users from storing files in the cloud reliably. One way to improve privacy from a data owner's perspective is to encrypt files before uploading them in the cloud and decrypting files after downloading them. However, data encryption is a high cost for devices and the data recovery process entails complicated communication between the data user and the cloud. Normally, with a limited bandwidth capacity and a limited battery charge, these problems represent a huge overhead for processing and communication, as well as increased power consumption for users, which makes encrypted searching in the remote cloud is very difficult. In this paper, propose the encrypted search for energy and traffic savings, an encrypted, broadband and energy efficient cloud search architecture. The proposed architecture downloads computing from remote devices in the cloud and we further optimize communication between clients and the cloud. It is shown that data security is not degraded when performance improvement methods are applied. We also apply auditing and regenerating techniques on files it's improve the cloud security.

**KEYWORDS**: cloud storage, searchable data encryption, energy efficiency, traffic efficiency.

## I. INTRODUCTION

Cloud computing refers to the provision of IT resources through the Internet. Instead of keeping data on your hard disk or updating applications for your needs, use a service through the Internet, in another location, to store information. In other words, cloud computing is Use of computer resources that are provided as service through a network. "So, you push your data to the cloud tells the cloud what computing is to execute. The cloud calculates the result and sends the answer to you. Thus, data can be accessed from any remote location via the internet. However this could involve some privacy transcendence. How the cloud is not reliable.

The cloud it could act maliciously, so this is the reason why the data provider encrypts the data before loading them on cloud. When the user needs to consult certain documents send the search request first. Existing system stores a Pre-calculated Trap Mapping Table (TMT) in devices, which map common words in English. To the corresponding traps. The trap mapping table stores the information. Necessary to map and search, the heavy No calculation is required to generate trapes be guided online. However, it is inevitable the trapes of some keywords were not archived in the early trapdoor mapping table. In this case, the keyword is encrypted by the user. So the new one the reclaimed or generated pure manhole has been added A little 'noise of a series of noises, to avoid the cloud. To examine the same traps. The trap is sent to the cloud by users to get the required document. The cloud uses that trap to search the document requested using Classified Serial Binary search algorithm. Serial binary evaluation research is a different approach to finding a particular record. The idea is to divide all records into. Two, one upper half and one lower half. So, try to see in which half of the register do you want to be? It's not inside, you're discarding. So now you're left alone Half of the original records. So divide that half in two and repeat the process until the end Find the disc you want. In the end, the user receives these search results are encrypted and use private the supplier's key to decrypt documents.

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 12, December 2018

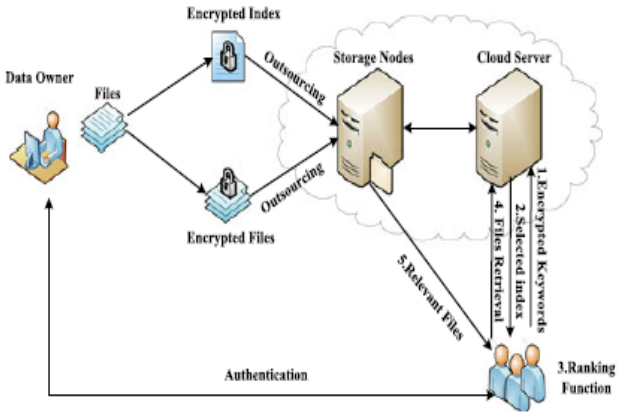


**Fig. Traditional encrypted search architecture**

We introduce traffic and energy savings Encrypted search architecture (TEES) for mobile cloud storage TEES applications achieves efficiency through Using and modifying the search by keyword classified as basis of the encrypted search platform, which has been widely Used in cloud storage systems. Traditionally, two categories output of encrypted search methods, which can enable the Servers in the cloud to search for encrypted data: Search by classified keyword and search by Boolean keyword. The classified keyword search uses relevance scores to represent the relevance of a file for the searched and sent keyword. The main files relevant to the customer. It is more suitable for Cloud storage that is searching for Boolean keyword searches, since the keyword search is Boolean the approaches must send all the corresponding files to the clients, and then incur more network traffic and an increased post-processing overhead for devices.

A. Goals and Objectives

- To implement energy efficient encrypted search system.
- To reduce time and improve performance on cloud.
- To improve the security.

B. Problem Statement:

To sufficient support an encrypted search pattern with a higher level of security in cloud data, we propose a new approach, According to some of the threats our goal is to design a solution for secure encrypted search through mobile cloud storage.

## II. RELATED WORK

In this section, we briefly review the related work on psychological disorder detection system and their different techniques.

**D. Song, D. Wagner, and A. Perrig:** In this paper, we describe our cryptographic schemes for the problem of searching for encrypted data and supply Safety test for the resulting cryptographic systems. Our techniques have a number of crucial advantages. They are safely: provide a testable secret for cryptography, in the sense that the unreliable server cannot learn all that concerns the normal text when only the cipher text is supplied; They provide query isolation for searches, that is that the unreliable server cannot learn anything anymore the plain text that the result of the research; provide controlled search, so that the unreliable server cannot search to arbitrary word without the user's authorization; they too It supports hidden queries, so the user can ask for untrusted information Server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length n, encryption and the search algorithms need only the O (n) encoding and the blocking sequence

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 12, December 2018

cryptographic operations) and almost do not introduce space and communication above, and therefore they are practical to use today [1] .

**C. Wang, N. Cao, K. Ren, and W. Lou:** In this work we define and solve the problem of secure search for classified keywords on encrypted data in the cloud. Classified research greatly improves the ease of use of the system by allowing the search result ranking of relevance instead of sending undifferentiated results and also guarantees the accuracy of file recovery. Specifically, let's explore the statistical measurement approach, i.e. the relevance score, from the retrieval of information to create a safe search index and develop a one-to-many order retention mapping technique to adequately protect sensitive scoring information. The resulting design is able to facilitate efficient server classification without losing keyword privacy. An in-depth analysis shows that our proposed solution enjoys security assurance with respect to previous search cryptography schemes, while correctly performing the objective of search by classified keyword. Numerous experimental results demonstrate the effectiveness of the proposed solution [2].

**N. Cao, C. Wang, M. Li, K. Ren, and W. Lou:** In this paper, for the first time, we define and solve the difficult problem of the private reserve Search with keywords classified in the encrypted cloud data (MRSE). We establish a series of stringent privacy requirements for a system for using data in the cloud securely. Between different multi keywords Semantics, we choose the measure of efficient resemblance of "coincidence of coordinates", that is, for as many coincidences as possible, for capture the relevance of data documents in the search query. We Use more "internal similarity of the product" to evaluate quantitatively such a measure of similarity. First we propose a basic idea for the MRSE based on the internal safe calculation of the product, and then give Two MRSE schemes significantly improved to achieve different goals strict requirements on privacy in two different threat models. Comprehensive analysis that investigates the guarantees of privacy and efficiency of the proposed schemes. Experiments in the real world data sets also show the proposed schemes, in fact, enter below General costs of calculation and communication [3].

**B. Wang, S. Yu, W. Lou, and Y. T. Hou:** in this paper, we propose a novel multi keyword. Widespread research scheme exploiting the sensitive location Hash technique. Our proposed scheme reaches a widespread coincidence through algorithmic design instead of expanding the index record. It also eliminates the need for a default dictionary and effectively supports fuzzy search for multiple keywords without Increase the search index or complexity. Extensive analysis Experiments with real-world data show that our proposed scheme it is safe, efficient and precise. To the best of our knowledge, this is the first job that reaches a widespread search for multiple keywords on encrypting data in the cloud [4].

**Q. Chai and G. Gong**: In this work, we investigate the cryptography of research problem in the presence of a semi-honest but curious server that you can perform only a fraction of the search operations honestly and honestly return a fraction of the search result. Fight against this strongest adversary of all is a verifiable schema of SSE (VSSE) it has been proposed to offer an additional verifiable research capability to the data. Privacy, both confirmed by our strict security analysis. Furthermore, we treat practicality / efficiency as a central requirement of a search cryptography scheme. There we demonstrate the lightness of our scheme, we implement it and tested the proposed VSSE on a laptop (which functions as a server) and a cell phone with Android 2.3.4 (which serves as an end) user). The experimental results suggest optimistically that the proposed scheme meets all our design objectives [5].

**M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou:**In this paper, we recognize the prerequisites and difficulties of the framework for getting redistributed cloud information administrations with ensured security inquire about, specifically, how to structure usable and basically effective scan designs for cloud-scrambled capacity. We present a general procedure for this utilizing cryptographic strategies with hunt usefulness, which enables clients to scan for encoded information without losing data on the information itself and client questions. Specifically, we break down three alluring highlights of the pursuit activities that can be utilized: similarity with the grouping of results, scan for similitude and research on organized information. For every one of them, we portray the ways to deal with structure proficient hunt cryptography plans with secured protection, in view of various later symmetric key cryptography natives. We break down its focal points and restrictions and depict the future difficulties that should be made plans to make this protected cloud information benefit accessible [6].

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 12, December 2018

**Boldyreva, N. Chenette, Y. Lee, and A. O_neill:** They propose a notion of security in the spirit of pseudo-random functions (PRF) and related primitives that ask that an OPE scheme appears as "as random as possible" subject to the restriction of the conservation order. So we designed an efficient OPE scheme and tested its security based on our notion based on Pseudoility of a block code below. Our construction is based on a natural relationship. We have discovered between a random function of order conservation and hypergeometric probability distribution. In particular, it makes use of the black box of an efficient sampling algorithm for finally [7].

**L. Baker and A. McCallum:** This paper describes the Distributionality application. Grouping to document the classification. This approach groups words into groups based on Distribution of class labels associated with each word. Therefore, unlike other non-supervised dimensionality reductions Techniques, such as latent semantic indexing, we are able to compress the functionality space much more aggressively, maintaining a high classification of documents Accuracy. Experimental results obtained in three real worlds. The data sets show that we can reduce the dimensional characteristics and for three orders of magnitude and only loses 2% Accuracy: significantly better than latent semantic indexing, class-based grouping, and selection of functions Mutual information or functionality based on Markov blanket selection. We also show that the less aggressive the grouping sometimes results in an improved classification Accuracy on classification without grouping [8].

**Swaminathan, Y. Mao, G. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard:**They present down to earth procedures for satisfactory importance coordination scoring strategies and cryptographic systems, for example, a request that jam cryptography, to ensure information accumulations and lists and give effective and exact hunt capacities to safely arrange reports in light of a conference. Test results in the W3C gathering. That these methods have an execution practically identical to the traditional one look frameworks intended for decoded information in pursuit exactness terms. The proposed techniques hence shape the initial steps to gather propelled data recovery and secure scan capacities for a wide scope of utilizations incorporating information the board in the legislature and in organizations tasks, permitting the scholastic investigation of touchy information and encourage the procedure of disclosure of records in case [9].

**C.Orencik and E. Sava¸s:**In this paper, we propose a viable security saving positioned watchword seek plot dependent on PIR that permits multi-catchphrase inquiries with positioning capacity. The proposed plan expands the security of the watchword seek plot while as yet fulfilling effective calculation and correspondence necessities. To the best of our insight the dominant part of past works are not productive for expected situation where reports are expansive documents. Our plan beats the most productive recommendations in writing regarding time unpredictability by a few requests of size [10].

## III. PROPOSED APPROACH

This section introduces the design of the proposed system. As compared to existing system, this system main processes are:

- The process of authentication is used by the data owner to authenticate the data users.
- The file set and its index are stored in the cloud after being encrypted by the data owner during the pre-processing and indexing stages.
- The data user searches the files corresponding to a keyword by sending a request to the cloud server in the search and retrieval processes.
- Auditor audit the all files if corrupt any file then regenerate corrupted files.

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 12, December 2018

*System Architecture:*

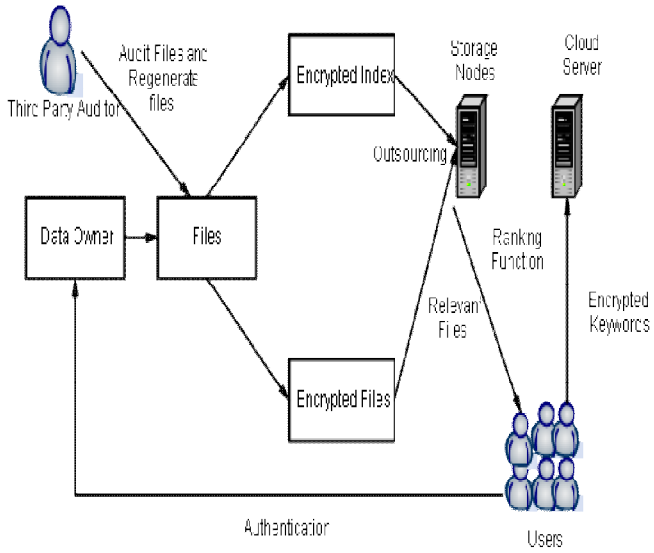


**Fig. System Architecture**

## IV. CONCLUSION

In this paper, develop a new proposed system to create traffic and energy efficiency Keyword search tool encrypted in cloud archives. Let's start with the introduction of a basic structure that we have compared with the previous encrypted search tools for cloud computing and showed its inefficiency in a cloud context. So we develop an efficient one implementation to get an encrypted search in a remote cloud. Enough for cloud computing, while a series of the experiments have highlighted its efficiency. Proposed system is a bit more Consume time and energy for searching for keywords Simple text, but at the same time saves a lot of energy. Compared to traditional strategies that offer increase security level using auditing and regenerating methodology. This work can be extended to other new implementations.

## REFERENCES

[1] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.
[2] 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. 1467–1479, Aug. 2012.
[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.
[4] 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 Conf. Comput. Commun., 2014, pp. 2112–2120.
[5] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Proc. IEEE Int. Conf. Commun., 2012, pp. 917–922.
[6] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "Toward privacy assured and searchable cloud data storage services," IEEE Netw., vol. 27, no. 4, pp. 56–62, Jul./Aug. 2013.
[7] Boldyreva, N. Chenette, Y. Lee, and A. O_neill, "Order-preserving symmetric encryption," in Proc. 28th Annu. Int. Conf. Adv. Cryptol.: Theory Appl. Cryptographic Techn., 2009, pp. 224–241.
[8] L. Baker and A. McCallum, "Distributional clustering of words for text classification," in Proc. 21st Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 1998, pp. 96–103.
[9] Swaminathan, Y. Mao, G. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, "Confidentiality-preserving rank-ordered search," in Proc. ACM Workshop Storage Security Survivability, 2007, pp. 7–12.
[10] C.Orencik and E. Sava¸s , "Efficient and secure ranked multi-keyword search on encrypted cloud data," in Proc. Joint EDBT/ICDT Workshops, 2012, pp. 186–195.