www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Stamp enabled energy efficient search scheme over encrypted cloud data

V.Manimaran[1], M.Pavithra[2], P.Sanmati[3], S.Savitha[4], P.VasanthaRohini[5]

[1]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College

[2-]5UG Scholars Department of Computer Science and Engineering, Nandha Engineering College

ABSTRACT

Cloud storage provides a convenient, massive, and ascendible storage at low price, however information privacy could be a major concern that forestalls users from storing files on the cloud trustfully. A way of enhancing privacy from information owner purpose of read is to encode the files before outsourcing them onto the cloud and decode the files when downloading them. However, encoding could be a serious overhead for the mobile devices, and information retrieval method incurs an advanced communication between the information user and cloud. Commonly with restricted information measure capability and restricted battery life, these problems introduce serious overhead to computing and communication also as the next power consumption for mobile device users that makes the encrypted search over mobile cloud terribly difficult. In TEES while searching information requires more bandwidth and batter life will be low. In this paper, we tend to propose traffic and energy saving encrypted search, an information measure and energy economical encrypted search design over mobile cloud. The projected design offloads the computation from mobile devices to the cloud, and that we more optimize the communication between the mobile shoppers and also the cloud. It's incontestable that the information privacy doesn't degrade once the performance improvement ways area unit applied. Our experiments show that's STAMP reduces the computation time by 23 to 46% and save energy consumption by 35 to 55% per file retrieval; in the meantime the network traffics throughout the file retrievals are considerably reduced.

Index Terms: Mobile cloud storage, Searchable encoding, Energy potency, Traffic potency.

INTRODUCTION

Cloud storage system could be a service model during which information square measure main tained, managed, backup remotely on the cloud facet, and meantime keeps on the market to the users over a network. Mobile Cloud Storage (MCS) [1], [2] denotes a family of more and more widespread on-line services, and even acts because the primary file storage for the mobile devices [3]. MCS permits the mobile device users to store and retrieve files or information on the cloud through wireless communication that improves the information accessibility and facilitates the file sharing method while not exhausting the native mobile device resources [4]. The data privacy issue is an dominant in cloud storage system, that the sensitive information is encrypted by the owner before outsourcing onto the cloud, and information users retrieve the interested information by encrypted search theme. In MCS, the fashionable mobile devices square measure confronted with several of of constant security threats as , PCs, and encoding strategies square measure foreign in MCS [5], [6]. However, mobile cloud storage system incurs new challenges over the standard encrypted search schemes, in thought of the restricted computing and battery capacities of mobile device likewise as information sharing and accessing approaches through wireless communication. Therefore, an acceptable and

Author for correspondence:
Department of Computer Science Engineering, Nandha Engineering College

economical encrypted search theme is important for MCS. Generally speaking, the mobile cloud storage is in nice way of an information measure and the energy potency for information encrypted search theme, because of the restricted battery life in the system and collectible traffic fee. Therefore, we have a tendency to specialize in the look of a mobile cloud theme that's economical in terms of each energy consumption and therefore the network traffic, whereas keep meeting the security by necessities through wireless communication channels.

To this finish, we have a tendency to introduce Traffic and Energy saving Encrypted Search (TEES) design for mobile cloud storage applications. TEES achieves the efficiencies through using and modifying the graded keyword search because the encrypted search platform basis that has been wide used in cloud storage systems. Historically, two categories of encrypted search strategies exit, which will modify the cloud server to perform the search over the encrypted data: graded keyword search and mathematician keyword search. The graded keyword search adopts the connection scores [7] to represent the connection of a file to the searched keyword and sends the top-k relevant files to the shopper. it's additional appropriate for cloud storage than the mathematician keyword search approaches (e.g., [8], [9], [10]), since mathematician keyword search approaches got to an send all the matching files to the purchasers, and thus incur a bigger quantity of network traffic and a heavier post-processing overhead for the mobile devices.

By carefully plan of graded keyword search procedure, TEES offloads the protection calculation to the cloud fact to avoid wasting the energy consumption of mobile devices, and TEES additionally modify the encrypted search procedure to scale back the traffic quantity for retrieving information from encrypted cloud storage. Besides the energy and traffic efficiencies, TEES is enforced with improvement in thought of the changed encrypted search procedure so as to mitigate statistics data leak and keywords-files association leak [12], [13] for MCS, by adding noise in Term Frequency (TF) distribution perform and keeping the Order protective secret writing (OPE) attributes.

Moreover, we advise that a cloud storage service supplier is semi-honest and can't conspire with wrongdoer in TEES, as most of the connected works. TEES employs the design red surrender ancient encrypted search procedure, and our comprehensive experiments prove the TEES has following blessings compared with the normal advanced encrypted search procedure:

- TEES reduces the energy consumption by 35 ~ f55 p.c by offloading the computation of the connectedness scores to the cloud server. This reduces the computing work on the mobile device facet where a sat a similar time considerably rushing up the mobile file access speed (e.g., it doubles the speed for accessing a one hundred KB file).
- With a simplified search and retrieval method, TEES reduces the network traffic for the communication of the chosen index, and reduces the file retrieval time by twenty three ~ forty six p.c in our experiments.
- In implementing the redesigned encrypted search procedure, TEES redistributes the encrypted index to avoid statistics data leak, and wraps key- words adding noise so as to render them indistinguishable to the attackers. Security analysis show that the protection level of TEES is secured and increased for MCS wireless communication channels.

FILE RETRIEVAL IN CLOUD STORAGE

Traditional Encrypted Search over Cloud Data

The ancient Encrypted Search over Cloud knowledge ancient cloud storage system design and general procedures are shown in Fig.2.1, that include: file/index encryption by the info owner, outsourcing the info to the cloud storage, and encrypted knowledge search/retrieval procedure of the info users in cloud computing. The data is unique for the encrypted search over the cloud. Most of the pre- various schemes below this design use Order conserving secret writing to cipher the file index. This module can be used to the user can upload the file in encrypted form.

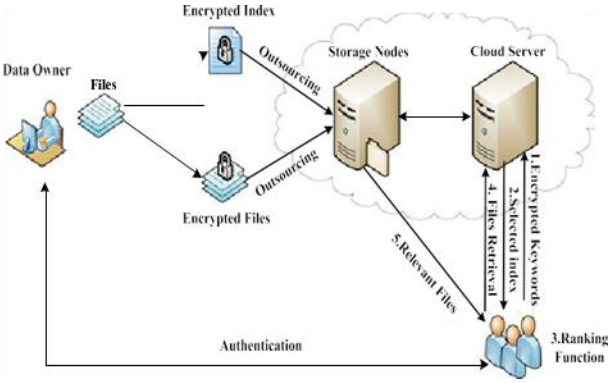

Fig.2.1. Traditional encrypted search architecture

File/Index encryption

The data owner initial executes the preprocessing and categorization work as shown on Fig. 2.1.1. He ought to invert files that reelect to store on the cloud, for text search engines .Each word in these files undergoes stemming to retain the Words term. Once this step, the information owner encrypts and hashes each term (word stem) to repair its entry within the index. The index is then created by the information owner. Finally, the information owner encrypts the index and stores it into the cloud server, at the side of the encrypted file set. Most of the pre- various schemes below this design use Order conserving secret writing to cipher the file index. This file index is usually a Term Frequency table composed of TF values. The TF-IDF table may well be accustomed confirm word relevance in documents.

Data Search and Retrieval after Authentication

A data user will solely access file once being attested by information owner. In the method of authentication user the information user sends his identity to the information owner. The information owner sends the encrypted keys back if the user may be a legal user. In the method of search and retrieval, the cloud server helps the users to search out the top-k relevant files for a given key- word while not decrypting it. Searches incur following the steps, as illustrated in Fig.2.1:

- An attested user stems the keyword to be queried, encrypts it with the keys and hashes it to urge its entry within the index. Then the encrypted keyword is distributed to the cloud server.
- On receiving the encrypted keyword, the cloud server 1st searches for it within the index. Then the index associated with this keyword is distributed back to the information user.
- The information user calculates the connection scores with the chosen index to search out the top-k relevant files and sends a follow-up request to the cloud server so as to retrieve the files.
- The position of those files is chosen and that they area unit sent back to the information user from the cloud server.
- The information user decrypts the files and recovers the first information.

The related computational components for these steps are illustrated in Fig. 2.2, which indicate the traditional two round-trip schemes for a file search and retrieval process invoked by an authenticated user. We call this file retrieval scheme abbreviated as Two Round trip Search (TRS). This scheme provides privacy protection through a complicated file retrieval process compared to a simple Plain Text Search scheme (PTS) where searching and retrieving a file is done in only one round without security service.

Data Owner

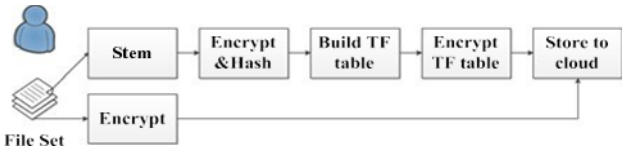

Fig. 2.1.1.Process of preprocessing and indexing

ENCRYPTED SEARCH SCHEMES

Over the past recent years, encrypted search has evolved toward the power knowledge sharing with protection of users' privacies. Song et al. [8] raised the question the way to do keyword searches on encrypted knowledge expeditiously. They planned a theme that encrypted every word of a document separately. Thus it's not compatible with existing file secret writing schemes and it cannot upset compression knowledge. at the moment several strategies of keyword search showed up like. In info Retrieval, term frequency-inverse document frequency (TF-IDF) may be a data point that reflects however necessary a word is to a document in an exceeding assortment or corpus. it's usually used as a weight think about the keyword primary primarily based retrieval and text mining The TF-IDF formula planned by Salton and McGill's book is one in every of the foremost widespread schemes, among alternative schemes. Up to now, encrypted search includes Boolean keyword search and graded keyword search. In Boolean keyword search [8], [9], [10], the server sends back files solely supported the existence or absence of the keywords.

Ranked keyword search. In hierarchical encrypted search, the server sends back the top-k hierarchical files. Most of the previous schemes used OPE to code the index of the file set, though the totally polymorphic cryptography, methodology even be used. Wang et al. [13] pro-display a one-to-many mapping OPES; they enforced a complicate formula for security protection. However, their performance and energy consumption would a probabilistic capsule since their formula was complicate and wish a lot of computing resource.

Swaminathan et al. projected a confidentiality-preserving rank-ordered search. This theme displays slow performances because the connection scores are computed on the consumer facet, increasing its employment. Zerretal. [12] introduced the Zerber+r model that includes a unique technique that renders the connection scores and number of follow-up requests for various terms in distinguish- ready for the server whereas protective the retrieval accuracy of the server-side top-k process.

The consumer then decrypts the weather came back by the server and filters them for from in efficient search time with 2 round-trip communications. Note that multi-keyword is probably the long run main stream encrypted search theme with higher searching accuracy, however current on-going an analysis cannot offer associate degree authoritative methodology. Therefore, we'll use the single-keyword with OPE TF-IDF cryptography methodology as a basis the ascertain an additional power and traffic economical and encrypted the information in search design.

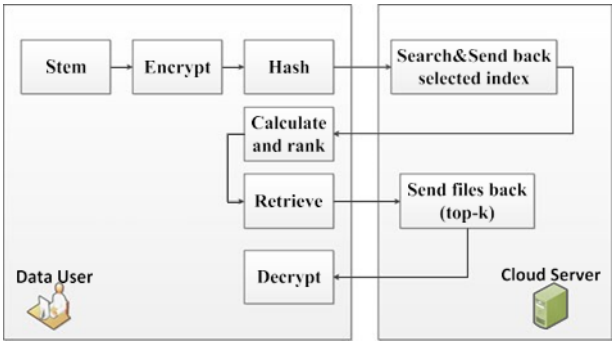

Fig. 2.2. TRS: Two-round-trip encrypted search.

TEES SYSTEM DESIGN

To effectively support associate degree encrypted the search therewithal high security level over cloud knowledge, we have a tendency to introduce a replacement design that we have a tendency to name TEES. in line with the threats introduced in Section a pair of, our aim is to style a sensible solution for secure encrypted search over a mobile cloud storage. we have a tendency to initial introduce the planning plan in the Section 3.1,and so introduce development of our own protocol with the amendment of the normal method of file search and retrieval for the cloud knowledge. Our theme achieves the protection and potency goals mentioned higher than.

The Basic Idea of TEES

The basic idea behind TEES is to offload the calculation and the ranking load of the relevance scores to the cloud. It has been highlighted that offloading some computation intensive applications onto the cloud may be Associate in nursing economical low power style philosophy. Cloud suppliers will give computing cycles, and users will use these cycles to scale back the amounts of computation on mobile systems and save energy. However, at an equivalent time, offloaded applications will increase the transmission quantity and therefore increase the energy consumption from another side. This double effect motivates US to fastidiously plan the normal file encrypted search and retrieval method. we have a tendency to 1sttake Associate in Nursing over- read of major processes for all file encrypted search and retrieval schemes. There square measure unremarkably three main processes:

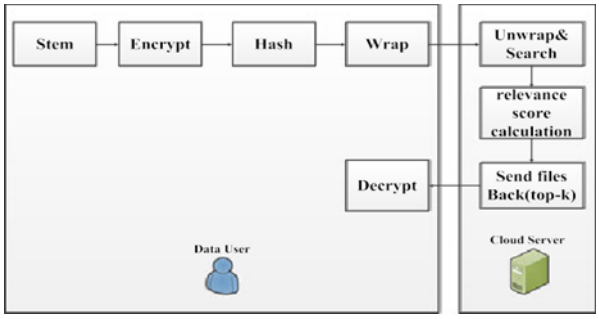

Fig.3.1 ORS: Novel process of search and retrieval.

- The method of authentication is employed by the information owner to evidence the information users.
- The file set and its index square measure keep within the cloud once being encrypted by the information owner throughout the pre-process and compartmentalization stages.
- The knowledge user searches the files resembling a keyword by causing an invitation

to the cloud server within the search and retrieval processes.

Modified Process of Search and Retrieval

During the preprocessing and categorization stages, the info owner gets a TF table as index and uses order protective cryptography to encipher it. As a result, the cloud server is in a position to calculate the connectedness scores and rank them while not decrypting the index. This renders the offloading of the machine load secure and doable. Thus, the changed search and retrieval processes of TEES follow the steps:

- If a knowledge user desires to retrieve the top-k relevant files supported a keyword, he initial obtains authentication from the info owner and so receives the keys to encipher the keyword.
- The information user stems the keyword to be queried and encrypts it victimization the keys.
- The information user wraps the encrypted keyword into a tuple, adding some noise to avoid data point data leak; this tuple is employed to perform the retrieval. Then, it's sent to the cloud server in conjunction with the quantity k. The wrap methodology renders the keywords indistinguishable or associate degree wrongdoer, which can be introduced in Section five in details.
- On receiving the wrapped keyword, the cloud server initial makes positive that it's accessed by a legal user.
- If the server is notified by the info owner that this user is to become invalid in a very close to future, the search is performed however a warning is additionally issued. If this can be a legal user, the server unwraps the tuple to recover the entry of the keyword and searches for it within the index. once shrewd the relevancy scores, the position of the files like the key- word is picked and also the top-k relevant files ar sent back to the info user's mobile shoppers while not acting any secret writing on these files.
- The information user decrypts these files within the mobile consumer and recovers the first information.

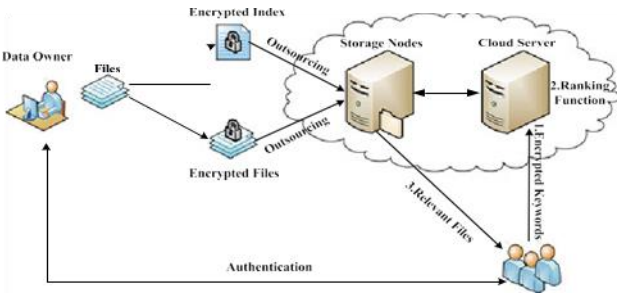

Fig.3.2 Encrypted search architecture of TEES.

Comparing Figs. 3.1 and 3.2, we tend to conclude that the search and retrieval processes in TEES are so simplified to one access than TRS. We call it , that offload the computation load of "relevance score calculation" from mobile users to the cloud and might intuitively cut back the communication method between the users and cloud server. More- over, since the connectedness score calculation is offloaded to the cloud server, it directly sends the top-k relevant files back to the info user once it receives the retrieval request, which might conjointly cut back the traffic quantity for file retrievals at identical time.

Note that this offloading won't jeopardize the info security in MCS because of the careful TEES design and implementation in coding sweetening, which can be elaborated in Section 4. Performance comparative experiments on ORS, TRS and PTS schemes are going to be delineate in Section six. we tend to currently1st discuss the efficiency of TEES.

Discussion: Performance Efficiency of TEES

The design of TEES is shown in Fig.3.2, during which the connectedness scores calculation is offloaded to the cloud, which eases the significant burden on mobile shoppers. Moreover, TEES's

options just round-trip communication for every search as epresented in instead of TRS as within the previous schemes as in Fig.2.2. During this theme, the file search and retrieval steps square measure as follows:

- The knowledge user sends his identity to the information owner and find the key keys if attested.
- An attested user stems the keyword to be queried, encrypts it with the keys and hashes it to urge its entry within the index. Then the encrypted keyword is shipped to the cloud server.
- On receiving the encrypted keyword, the cloud server can use perform of connectedness calculation search out the top-k relevant files and sent back to the information user wherever the top-k is organized by the users.
- The information user decrypts the files and recovers the original information.

TEES IMPLEMENTATION FOR SECURITY ENHANCEMENT FOR CLOUD

In order to realize security improvement with energy and traffic potency, we tend to implement the modules in TEES victimization changed routines and new algorithms. Our system. As antecedently mentioned, the information owner ought to build a TF table as index and encode it victimization OPE as to dump the calculation and ranking load of the connected scores to the cloud. Therefore on management the statistics info leak, we tend to implement our one-to-many OPE within the knowledge owner module (Section 4.1). we tend to the conjointly wrap the keywords to be searched by adding some noise within the knowledge user module to assist dominant the keywords-files association leak. so as to urge top-k relevant files, we tend to implement a ranking operate to calculate the relevant score on the cloud Given a keyword in ORS, the cloud server is responsible of shrewd the connectedness scores for the user to urge the corresponding top-k relevant files. There- fore, we tend to implement each the uncover and rank functions within the cloud server module Therefore these modules square measure changed compared with the normal ones.

Redesign of the Info Owner Module

We modify the method of building the index to support the ORS theme by our one-to-many OPE and implement it to control the statistics info leak. The authentication between knowledge the info the information owner and therefore the data user is additionally redesigned so as to confirm the protection of TEES. .Varied ways that for determinant the precise values of each statistics exist. In the case of the term frequency tfðt; dÞ, the simplest choice is to use the raw frequency of a term in a document, i.e., the number of times that term to occurs in document. If we denote the raw frequency of t by fðt;dÞ, then the simple TF scheme is tfðt;dÞ¼fðt;dÞ.The common inverse document frequency is a measure whether the term t is area cross all documents. It is obtained by dividing the total number of documents by the number of documents containing the term, and then taking the log algorithm of that quotient.

Let GenKeyðÞ be the operate that generates the keys. Let pðÞ be a hash operates that encrypts the terms. In TEES, pðÞ is instantiated by a hash operate like MD5. Let cðÞ be the hash of the encrypted terms, cðtiÞ be the entry of the term ti at intervals the index. Let "ðÞ be associate coding formula for the TF values. Once building associate index, it executes following two steps:

- First, the user information owner starts searching and by vocation GenKeyðÞ, to get a key a to cipher the terms, a key b to cipher the index, and therefore the noise Z> zero; m > 0 to wrap the keywords. He then outputs K ¼ fa; bg and N ¼ fZ; mg.
- Second, the information owner builds a secure index by calling Build Index; FÞ (encrypted N is distributed to cloud server) as described.

ALGORITHM 1- KEY GENERATION

Input: TFTable
Output: G~ðTFÞ;H~ðTFÞ
1: Get the distribution histogram C of the TF table and get TFx
as all TF values occur in C.
2: fortfi2 TFxdo
3:Get the occurrence.
4: end for
C jTFx jc
i¼1
6: fortfi2 TFxdo
7: Calculate p¼ci=C.
8: end for
9: fortfi2 TFxdo
10: if i ¼¼ 1then
11: GetGðtfiÞ¼1andHðtfiÞ¼floorð2B×pi 12: else
13: Get GðtfiÞ¼ HðtfiÞ—1Þþ 1 and HðtfiÞ¼ HðtfiÞ—1Þþfloor
14: end if
15: end for
16:returnG~ðTFÞ;H~ðTFÞ.

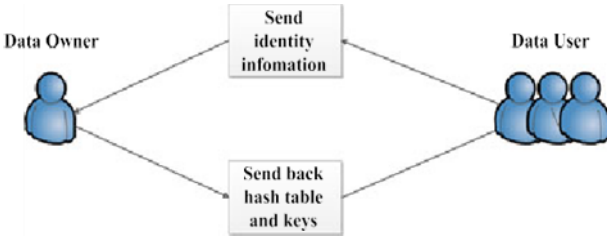

Fig.4.1 .Process of authentication.

The TF values bar chart over a file set therefore on make sure the System security. In TEES, the data owner maintains a set of legal Users ("legal set") and a set of users that will become invalid in after a defined delay ("overdue set"). The process of authentication is shown on Fig.4.1.

Redesign Of The Data User Module

The data user module is dead on the mobile purchaser's aspect. The wrap operate of the keywords is enforced to solve the keywords files association leak. In the wrap to function, the encoding done by the info owner. The authentication operate is employed for authentication. We tend to currently detail the wrap operate. This module Wrap perform with noise. Once a licensed information user desires to retrieve files, he must code the corresponding question keyword and obtain the hash price h from the hash table. This hash price is then sent to the cloud server and wont to reckon the connectedness scores. so as to render this hash price indistinguishable for associate aggressor, the cloud consumer ought to wrap it, adding some noise before sending itto the cloud server.The wrap perform wrap can, initial of all produce a random range r, so build a tuple ðh1; h2Þ supported algorithmic rule four (Z> 0; m > 0):

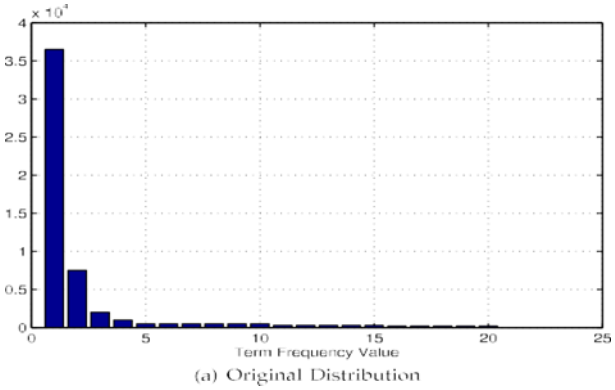

Fig. 4.2 .TF distribution.

Redesign of the Cloud Server Module

We will describe the functions that unwraps the keywords and rank the connection scores for the cloud server module. These functions ar accustomed get the top-k relevant files per a given search keyword. Unwrap perform. Note that the cloud server is semi- sure, and therefore the expose perform may be processed by the server. Upon receiving the tuple WrapðwÞ ¼ ðh1; h2Þ, the server calls Unwrapððh1; h2ÞÞ to get cðpaðw~ÞÞ ¼ h, searches into the TF table, and so sends back the corresponding files. Assuming that the random range (noise) created by the wrap operate is positive, the expose operate behave obviously. Since h could be a positive whole number, we tend to might recover h victimization Unwrap (2).

TEES may also support alternative document modeling methodology like Latent Dirichlet allocation. we are able to conjointly realize the likelihood for a term to seem in an exceedingly file employing a middle tier "topic", and so store its encrypted price within the index. Note that TEES employees single-keyword search, however the essential for ideas like style potency by offloading and security for an improvement by adding noise, may be extended to all or any alternative encrypted search schemes. Moreover, it's acknowledged that multiple-keywords search will offer a lot of correct the search results, however makes the search a lot of sophisticated at identical time (as mentioned in Section a pair of.2). In mobile cloud, the single-keyword is enough to differentiate the documents that users would like since our documents square measure classified clearly. More- over, if we have a tendency to search encrypted knowledge with multi key

We should always sacrifice the search accuracy as a result OPE might guarantee the order between 2 values, however once these two values increased by many factors so get the arithmetic add (as multi-keyword search process), we have a tendency to can- not insure the order between the arithmetic sums. Another vital respect is that, decreasing the quantity of key-

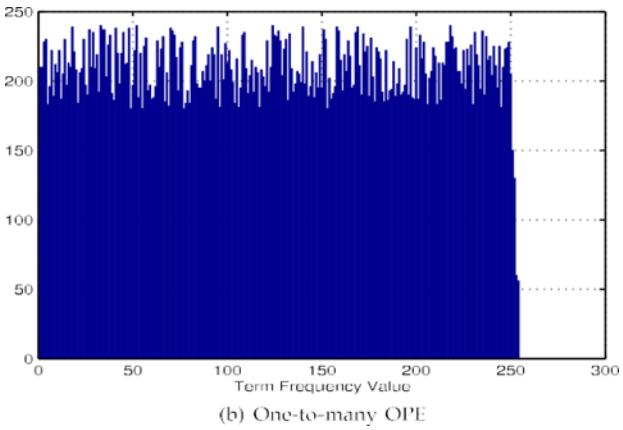

Fig. 4.3 .TF distribution.

Words might decrease the consumption of energy for mobile device. Overall, developing one keyword search theme could be a correct resolution of encrypted search information sharing for mobile cloud storage.

Moreover, TEES could be a general architecture where ever the OPE technique projected here will be substituted by alternative novel schemes. TEES protects the terms from being determined by analyzing the distribution of the TF values through mobile cloud communication channels. Fig.4.2 shows the histogram of the TF values over a data set, and we can see that the TF histogram are very sharp originally. It means that an attacker may get statistical information from the TF table as previously explained. In TEES, we encrypt the TF table with one-to-many order preserving encryption. Every TF value is mapped to a mapping range. The mapping value should identify the content on searching data in cloud. The cloud should retrieve the data and display the content to the system

FILE SEARCH AND RETRIVAL TIME

We compare the File looking out and Retrieval Time (FSRT) we tend to take a look at the FSRT for various files with size starting from one hundred K to one MB. We tend to observe that the FSRT of PTS is that the shortest since it doesn't have to be compelled to perform any security computation. The FSRT of ORS is effectively reduced once com- pared to the one in all TRS. This distinction is because of the benefits of the TEES style in terms of connection score calculation offloading, and sounds up in reduction of file search and retrieval method. The FSRT worth of ORS is incredibly as regards to the one in all PTS, implying a awfully low price to security on the mobile device. for instance, TEES saves FSRT by Battor, a phone power monitor to accurately live the system energy consumption. The energy is consumption of TRS and ORS. Though slight changes relying upon the setting may occur, the comparison is sort of accurate as controlled trials were performed.

Table 1: FSRT Analyse of PTS, TRS and ORS

	PTS	TRS	ORS
Request/Response	190 ms	370 ms	190 ms
Stemming and Encryption	0	10 ms	10 ms
Hash and Wrap	0	145 ms	150 ms
Server file search	80 ms	70 ms	75 ms
Client file search	0	260 ms	0
Sum	270 ms	855 ms	425 ms

Observe that the energy consumption is reduced from 0.08 to 0.036 mAh once looking out and retrieving files of size a hundred K, which suggests that ORS saves fifty five p.c energy compared to TRS. once looking out and retrieving files of one MB size, the energy consumption is reduced from zero.164 to 0.106 mAh, meaning a 35 p.c energy saving. So, TEES provides a awfully economic power consumption. as an example, to exhaust our one,650 mAh battery, ORS (of TEES) will per- type ~22,000 retrievals whereas TRS may solely retrieve ~13,000 files of size 600 K. File Search and Retrieval Time. We compare the File looking out and Retrieval Time (FSRT) for the 3 schemes during this section as illustrated. we have a tendency to take a look at the FSRT for various files with size starting from a hundred K to 1 MB. we have a tendency to observe that the FSRT of PTS is that the shortest since it doesn't need to perform any security computation.

The FSRT of ORS is effectively reduced once com- pared to the one amongst TRS. This distinction is because of the benefits of the TEES style in terms of connection score calculation offloading, and so results in reduction of file search and retrieval method. The FSRT worth of ORS is extremely almost the one amongst PTS, implying a awfully low value to security on the mobile device. as an example, TEES saves FSRT by 46 p.c compared to TRS for files of size a 100 K, and by 23 p.c for one MB files. The file retrieval time solely depends on the file size and network information measure. As shown in Table one, ORS will improve the "request/response" time considerably than TRS from 370 to a hundred 90 ms (saving a 100 and 90 ms), and eliminate the "client file search" time by offloading it onto the server (saving 260 ms).

Notice that the "sever file search" calculation employment of ORS is 70 ms, that is 5 ms longer than that of TRS. This is often explained by the very fact that the server takes the offloaded search calculation of the mobile user. within the different words, TEES eliminates the "client file search" time at the price of a bit heavier "server file search" time. This proves that the offloading is very economical (5 vs. 260 ms). Moreover, ORS spends a lot of five ms on wrapping the hash worth than TRS for enhancing the safety. Note that the "server file search" time of PTS is above the opposite 2 schemes, since the server ought to execute stem and hash perform for plaintext file search, whereas the hash functions square measure dead by the mobile information user in each TRS and ORS. Overall, ORS is secure and effective.

CONCLUSION AND FUTUREWORK

In this paper, the security study of STAMP (Spatial Temporal Provenance Assurance with Mutual Proofs) showed that it's secure enough for mobile cloud computing, STAMP is used to identify the location of where the searching data are stored. STAMP is used efficient search on the data on cloud. Then we can retrieve the data in encrypted form using the key generation algorithm. We have projected one keyword search theme to make encrypted information search economical. Next we have to download the data in decrypted form in cloud database. This data should used into our needs. STAMP technique provides a more security and more bandwidth. We have to use this technique they provide high battery life in mobile cloud.

Acknowledgement

The authors would love to acknowledge the many beneficial recommendations of the reviewers and the members on earlier variations of this paper. We also thank the authors of the references.

REFERENCES

[1]. L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: Towards a cloud definition," ACM SIGCOMMComput.Commun.Rev., 39(1), 2008, 50–55.

[2]. X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. New York, NY, USA: Springer, 2012,.255–263.

[3]. D. Huang, "Mobile cloud computing," IEEE COMSOCMultimedia Commun.Techn.CommitteeE-Letter, 6(10), 2011, 27–31.

[4]. O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Proc. IEEE 5th Int. Conf. Cloud Computer., 2012, pp.646–653.

[5]. S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy pre- serving multiple keyword search for confidential emoteforensics,"inProc.3rdInt.Conf.MultimediaInf.Netw.Secu- rity, 2011, 595–599.

[6]. P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Appl. Cryptography Netw. Security, 2004,.31–45.

[7]. Aizawa, "An information-theoretic perspective of tf-idfmeas- ures," Inf. Process. Manage.39, 45–65, 2003.

[8]. G. Salton and M. J. McGill, Introduction to Modern Information Retrieval. New York, NY, USA: McGraw-Hill, 1986.

[9]. E. Han and G. Karypis, "Centroid-based document classification: Analysis and experimental results," in Proc. 4th Eur. Conf. Princi- ples Data Mining Knowl. Discov. 2000, 116–123.

[10]. L.BakerandA.McCallum,"Distributional clustering fwordsfortext classification," in Proc. 21st Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 1998, 96–103.

[11]. A.Boldyreva,N.Chenette,Y.Lee, and A.On´eill,"Order-preserv-ing symmetric encryption," in Proc. 28th Annu. Int. Conf. Adv. Cryptol.: Theory Appl. Cryptographic Techn., 2009, 224–241.

[12]. M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in Proc. 28th Int. Conf. Theory Appl. Cryptographic Techn., 2010, 24–43.

[13]. C.GentryandS.Halevi,"Implementinggentry´sfully-homomor-phic encryption scheme," in Proc. 30th Annu. Int. Conf. Adv. Cryp- tol.: Theory Appl. Cryptographic Techn., 2011,.129–148.

[14]. 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, 7– 12.