IJSEAT International Journal of Science Engineering and Advance Technology

A New Architecture and Energy Efficient Keyword Search in Cloud

[1]V.Ganga Bhavani, [2]P.Radhika Krupalini

[1]Final year student, MCA, Dept. of Computer Science, Ideal College of Arts & Sciences, Kakinada, AP, India

[2]Associate Professor, Dept of Computer Science, Ideal College of Arts & Sciences, Kakinada, AP, India

ABSTRACT:

Normally with limited bandwidth capacity and limited battery life, these issues acquaint substantial overhead with registering and correspondence just as a higher power utilization for cell phone clients, which makes the encrypted search over mobile cloud very testing. In this paper, we propose TEES (Traffic and Energy saving Encrypted Search), a data transfer capacity and vitality effective encoded search design over mobile cloud. The proposed design offloads the calculation from cell phones to the cloud, and we further improve the correspondence between the versatile customers and the cloud. It is exhibited that the data security does not corrupt when the execution upgrade strategies are connected.

KEYWORDS: Searchable Data Encryption, Traffic Efficiency, Network Traffic.

1] INTRODUCTION:

The data protection issue is fundamental in distributed storage framework, so the delicate data is scrambled by the proprietor before re-appropriating onto the cloud, and data clients recover the intrigued data by encoded search plot. In Mobile Cloud Storage(MCS), the cutting edge cell phones are gone up against with huge numbers of indistinguishable security dangers from Public Storages's(PCs), and different conventional data encryption strategies are imported in MCS [5], [6]. In any case, versatile distributed storage framework brings about new difficulties over the conventional encoded search plans, in light of the restricted registering and battery limits of cell phone, just as data sharing and getting to approaches through remote correspondence. In this manner, a reasonable and proficient scrambled scan conspire is essential for MCS. As a rule, the versatile distributed storage is in incredible need of the transmission capacity and vitality effectiveness for data scrambled search plot, because of the constrained battery life and payable traffic expense. In this way, we center around the structure of a versatile cloud conspire that is effective as far as both vitality utilization and the system traffic, while continue meeting the data security necessities through remote correspondence channels..

2] LITERATURE SURVEY:

[1] R. Curtmola we start by inspecting existing thoughts of security and propose new and more grounded security definitions. We at that point present two developments that we show secure under our new definitions. Strikingly, notwithstanding fulfilling more grounded security ensures, our developments are more productive than every single past development. Further, earlier work on SSE just considered the setting where just the proprietor of the data is fit for submitting search questions. We consider the characteristic expansion where a self-assertive gathering of gatherings other than the proprietor can submit search questions. We formally characterize SSE in this multi-client setting, and present a productive development.

[2]C. Wang we characterize and tackle the issue of secure positioned keywordsearch over encoded cloud data. Positioned search extraordinarily upgrades framework ease of use by empowering query item significance positioning as opposed to sending undifferentiated outcomes, and further guarantees the document recovery precision. In particular, we investigate the factual measure approach, i.e., significance score, from data recovery to construct a safe accessible file, and build up a one-to-many request saving mapping procedure to appropriately secure those delicate score data. The subsequent plan can encourage effective server-side positioning without losing keyword protection. Intensive examination demonstrates that our proposed arrangement appreciates "as-solid as could be expected under the circumstances" security ensure contrasted with past accessible encryption plans, while accurately understanding the objective of positioned keyword search.

3] PROBLEM DEFINTION:

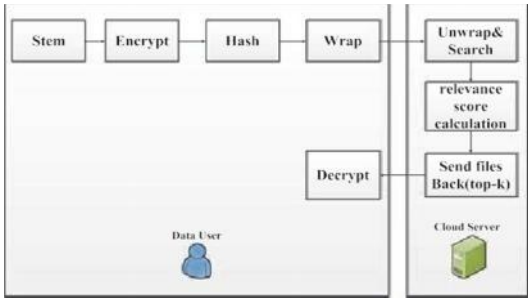
Customarily, two classifications of scrambled search strategies leave, that can empower the cloud server to play out the pursuit over the encoded data: positioned keyword search and Boolean keyword search. The positioned keyword search embraces the significance scores to speak to the pertinence of a document to the sought keyword and sends the top-k applicable records to the customer. It is more reasonable for distributed storage than the Boolean keyword search approaches, since Boolean keyword search approaches need to send all the coordinating documents to the customers, and in this manner cause a bigger measure of system traffic and a heavier post-preparing overhead for the cell phones.

4] PROPOSED APPROACH:

We present TEES (Traffic and Energy saving Encrypted Search) design for versatile distributed storage applications. TEES accomplishes the efficiencies through utilizing and altering the positioned keywordsearch as the scrambled search stage premise, which has been generally utilized in distributed storage frameworks. TEES is executed with security upgrade dependent on prevalent TF-IDF, yet the fundamental security imperfections of this encryption approach can't be totally settled. To the best of our insight, there is no unbreakable security conspire, yet TEES design is general enough to host and improve different encoded search plans.

In addition, we recommend that a distributed storage specialist co-op is semi-genuine and won't plot with aggressor in TEES, as the greater part of the related works. TEES utilizes the design overhaul over customary scrambled search method

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

MODULES:

Data Owner:

The procedure of confirmation is utilized by the data proprietor to validate the data clients. The verification between the data proprietor and the data client is likewise upgraded so as to guarantee the security of TEES The document set and its record are put away in the cloud in the wake of being encoded by the data proprietor amid the preprocessing and ordering stages. TF-IDF is the result of two insights, term recurrence and backwards report recurrence. Different ways for deciding the precise estimations of the two insights exist. On account of the term frequency (TF) tf(t, d), the most straightforward decision is to utilize the crude recurrence of a term in an archive, for example the occasions that term t happens in report d.

Data User:

The Data User module is executed on the versatile customers side. The wrap capacity of the keywords is actualized to unravel the keywords records affiliation spill. In the wrap work, the stem, the encryption and the hash activity are actually equivalent to in the file building calculation. The capacity decoding the documents relates to the encryption done by the data proprietor. The confirmation work is utilized for verification. At the point when an approved data client needs to recover records, he needs to scramble the relating question keyword w, and get the hash esteem h from the hash table. This hash esteem is then sent to the cloud server and used to process the significance scores.

Cloud Server:

Cloud Server that unwraps the keywords and rank the significance scores for the cloud server module. These capacities are utilized to get the top-k pertinent records as per a given pursuit keyword. Cloud server ascertains the importance scores and return top-k pertinent records as per the searching question from data client down Ranking Function. In mobile cloud, the single-keyword is sufficient to recognize the records that clients need since our archives are grouped unmistakably. Additionally, on the off chance that we search scrambled data with multi-keywords, we should forfeit the pursuit exactness in light of the fact that most prevalent OPE (Order Preserving Encryption) does not bolster multi-keyword well.

Process of Authentication:

In TEES, the data proprietor keeps up a lot of lawful clients ("legitimate set") and a lot of clients that will wind up invalid in after a characterized postponement ("past due set"). At the point when a client means to get to the record, he initially sends his data to be validated by the data proprietor. In our structure, we utilize our bound together school verification in TEES and exchange it through https for security concern. The data proprietor sends the keys alongside the hash table back if the client has a place with the lawful set. At the point when the client's power is past due, his character data is moved to the "late" set.

Process of Data Search and Retrieval:

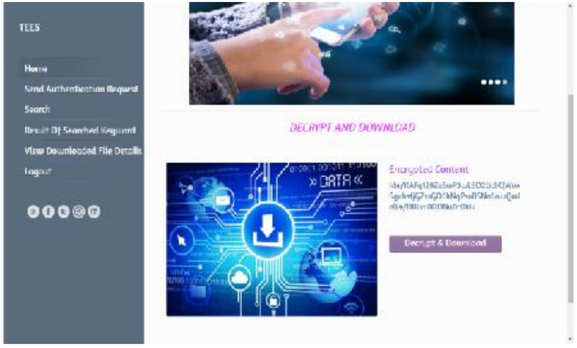
On the off chance that andata client needs to recover the top-k important records dependent on a keyword, he initially gets validation from the data proprietor and after that gets the keys to scramble the keyword. The data client wraps the encoded keyword, including some commotion; this tuple is utilized to play out the recovery. At that point, it is sent to the cloud server together with the number k. The wrap strategy renders the keywords indistinct for an aggressor. On accepting the wrapped keyword, the cloud server first ensures that it is gotten to by a lawful client. On the off chance that the server is advised by the data proprietor that this client is to end up invalid in a not so distant future, the search is performed yet a notice is additionally issued. On the off chance that this is a lawful client, the server unwraps the tuple to recoup the section of the keyword and scans for it in the list.

ALGORITHM

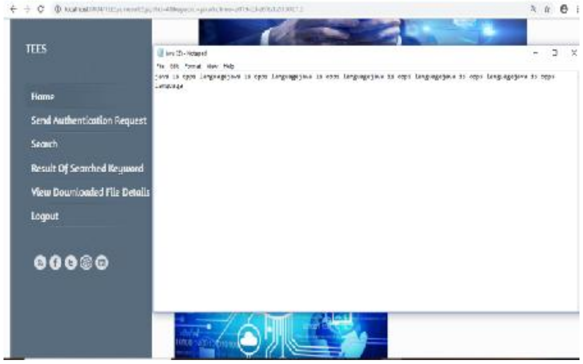
TEES: Traffic and energy saving encryption search algorithm

INPUT: key, index, file, keywords, tf, tf-idf, r
Step1: data owner generates key and encrypt the file and keywords.
Step2: secured index and files are sent to cloud.
Step3: owner maintains a set of legal users and a set of users that will become invalid in after a defined delay.
Step4: user intends to access the file, he first sends his information to be authenticated by the data owner.
Step5: data user needs to encrypt the corresponding query keyword w, and get the hash value h from the hash table.
Step6: hash value is then sent to the cloud server and used to compute the relevance Score.
Step7: Given a keyword, the data user searches the corresponding top-k ranked files.
Step8: download relevant files from cloud server.

8] RESULTS:



User Searched Encrypted File


TEES
Home
Send Authentication Request
Search
Result Of Searched Keyword
View Downloaded File Details
Logout
Notepad
File Edit Format View Help

java is oops languagejava is oops languagejava is oops languagejava is oops languagejava is oops languagejava is oops language

Searched File

9] CONCLUSION:

We developed a new architecture, TEES as an initial attempt to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. We started with the introduction of a basic scheme that we compared to previous encrypted search tools for cloud computing and showed their inefficiency in a mobile cloud context. Then we developed an efficient implementation to achieve an encrypted search in a mobile cloud. The security study of TEES showed that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency.

10] REFERENCES:

[1] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] X. Yu and Q. Wen, “Design of security solution to mobile cloud storage,” in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[3] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[4] O. Mazhelis, G. Fazekas, and P. Tyrvainen, “Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage,” in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized in-cloud security services for mobile devices,” in Proceedings of the

First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[6] J. Oberheide and F. Jahanian, “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

[7] A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.

[8] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. S&P 2000.Proceedings.2000 IEEE Symposium on.IEEE, 2000, pp. 44– 55.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology Eurocrypt 2004. Springer, 2004, pp. 506–522.

[10] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[11] Y. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.

[12] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, “Zerber+ r: Topk retrieval from a confidential index,” in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 439–449.

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

[14] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010, pp. 253–262.

[15] 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. 222–233, 2014.

V.Ganga Bhavaniis a student of P G Department of Computer Science in Ideal College of Arts and Science Kakinada. Presently she is in Final year Master Computer Applications (MCA) in this college and affiliated to Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh. She received her B.Sc(CS) from Aditya Degree college For Women, Kakinada in the year 2016.Her areas of interest include Cloud Computing, Web Designing and all current trends and techniques in Computer Science.

Mrs.P.Radhika krupalini is presently working as Associate Professor in P.G.Department Computer Science, Ideal College of Arts & Sciences, Kakinada.She obtained her MCA from Andhra University, M.Tech(CSE) from University College Engineering, JNTUK. She qualified AP SET Computer Science and Applications and has an experience of 13+ years of teaching experience at Post Graduate level. Her areas of interest are Operating System, Network Security & Cryptography, Artificial Intelligence, Cloud Computing and Big Data.