International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Enhanced Privacy with Multiple Search Over Cloud Data using EPSS

Amara S A L G G Gupta, K.Aneesha, T.Chakradhar,

Abstract: ***Cloud computing is the service-oriented platform which will provide security for the various data uploaded by the users. Security is the service which can be provided by the service providers. There is a lot data that can be stored in the cloud with the help of various security algorithms. The data which can be stored in the cloud is called outsourced data. Every user wants to store the sensitive data to cloud storage. In this paper, the Enhanced Privacy and Secure Storage data (EPSS) can be searched with the multiple keywords. For the searching of multiple keywords the Enhanced Keyword Search (EKS) which retrieve the data very fast and with multiple records. Experimental results show the performance of the searching and security.***

Keywords: Security, privacy, encryption and decryption.

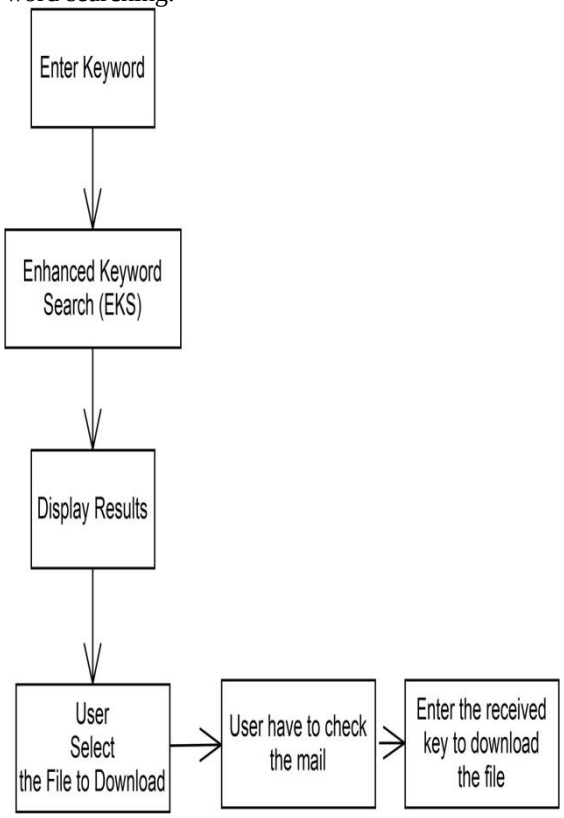
I. INTRODUCTION

Because of the rapid development of data, the data proprietors can once all is claimed in done store their information into the cloud to discharge the greatness of data amassing and support [1]. In any case, because the cloud shoppers and therefore the cloud server aren't within the proportionate confided in the zone, our re-appropriated info could be beneath the introduction to the hazard. Thusly, before sent to the cloud, the touchy info ought to be emulsified to verify for info security and battle free gets to. Shockingly, the quality plaintext look frameworks cannot be remarkably connected with the encoded cloud info any further. The common knowledge recovery (IR) has as lately given multi-watchword organized solicitation to the knowledge shopper. Basically, the cloud server desires outfit the knowledge shopper with as so much as potential, whereas confirming the info and solicitation security. It's basic corroboratory it into the cloud server exactly once info will be fittingly hunted for and used. In this paper, Enhanced Security is most widely provided to secure the data in cloud storage. The Enhanced Multi-Keyword search with secure data storage is implemented with advanced encryption and decryption algorithm. This is the most secure algorithm which provides high security with the generated private key that can be accessed by the user.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Amara S A L G G Gupta*, Department of Computer Science and Engineering, K L Educational foundation, Deemed to be University, Vaddeswaram, Andhra Pradesh, India.
K.Aneesha, Department of Computer Science and Engineering, K L Educational foundation, Deemed to be University, Vaddeswaram, Andhra Pradesh, India.
T.Chakradhar, Department of Computer Science and Engineering, K L Educational foundation, Deemed to be University, Vaddeswaram, Andhra Pradesh, India.

II. LITERATURE SURVEY

Public Encryption with Keyword search (PEKS) [2] will take a look at the given keyword present within the report while not taking in no matter else from the record.
data place away within the untrusted server will be disorganized. Search the data by utilizing the keyword. By utilizing PEKS reduces the handling time by recover simply the selected documents. By its hurt by utilizing the applying, as an example, tolerant record and examinations, a bit trip-up on writing system on watchword cannot deliver any outcome. during this means by going Fuzzy Keyword searching.



Zhihua Xia et.al,[3] projected a secure, effective and dynamic pursuit conspire, that underpins the precise multi watchword positioned look yet because the dynamic cancellation and inclusion of records. They build an Associate in Nursing uncommon motto adjusted paired tree because the list Associate in Nursingd projected an "Eager Depth-first Search" calculation to urge desirable productivity over direct search. Moreover, the parallel hunt procedure will be done to in addition diminish the time price. the protection of the set up is ensured against 2 risk models by utilizing the protected KNN calculation. Results show the proficiency of projected system.

the benefits of the projected framework area unit accessible coding plans empower the client to store the encoded data to the cloud and execute watchword search over figure content house and a protected tree-based inquiry conspire over the disorganized cloud data, that bolsters multi-catchphrase positioned search and dynamic activity on the record assortment. The disservices area unit the cloud service providers (CSPs) that keep information for purchasers could get to clients delicate data while not approval. A general thanks to influencing make sure the data secrecy is to scramble the data before redistributing. Be that because it could, this may cause a colossal expense relating to data simple use.

Bing Wang et.al, [4] projected a completely unique development of Associate in Nursing open key accessible coding plot keen about upset list. This set up conquers the one-time-just search constraint within the past plans. The impediments of the projected framework area unit as a matter of 1st importance, the motto protection is undermined once a watchword is looked. consequently, the record should be reconstructed for the watchword once it's been looked. Such arrangement is harmful thanks to the high overhead endured. Besides, the present reversed file based mostly accessible plans do not bolster conjunctive multi-catchphrase search, that is that the most generally recognized sort of queries currently a days. The preferences area unit investigate the difficulty of building Associate in Nursing accessible coding plot keen about the remodeled file, deliver the goods secure and personal coordinative between the inquiry trapdoor and therefore the protected file, style a completely unique trapdoor age calculation therefore the question connected reversed records area unit consolidated along on the sly while not telling the cloud server that changed records area unit recovered.

Yanzhi Ren et.al, [5] projected a light-weight search approach that supports productive multi-watchword positioned search in cloud process framework. the elemental set up utilizes the polynomial capability to shroud the encoded watchword and quest styles for effective multi-catchphrase positioned search. At that time improve the essential set up and propose a security safeguarding set up that uses the safe internal item strategy for making certain the protection of the looked multi-watchwords. The side of the projected framework is it breaks down the protection assurance of the projected set up and lead broad analyses keen about this gift reality dataset. The hurt is there's a chance of spillage of data in the cloud.

Hongwei Li et.al, [6] projected a multi-watchword positioned search to attempt to empower precise, effective and secure inquiry over encoded moveable cloud data. Security examination has shown that projected set up will adequately accomplish the classification of reports and file, trapdoor protection, trapdoor unlinkability, and covering access examples of the hunting consumer. The focal points Construct a skilled list to boost inquiry productivity. what is additional, it takes care of the trapdoor unlinkability issue. It likewise accomplishes improved productivity as a way as utility and search proficiency contrasted and existing proposition.

Mikhail Strizhov et.al, [7] projected Associate in Nursing accessible coding system that empowers secure quests over encoded data place away on remote servers. They characterize and beware of the difficulty of multi-watchword positioned search over encoded cloud data. Specifically, they gift a productive similitude accessible coding conspire that supports multi-catchphrase linguistics. The arrangement depends on 2 structure squares: Term Frequency Inverse Document Frequency (TF-IDF) estimation and ring LWE-based variation of the homomorphic cryptosystem. the benefit of this framework is it restores the coordinative data things during a positioned organized means. The Disadvantage is in the typical framework it underpins simply single keyword search.

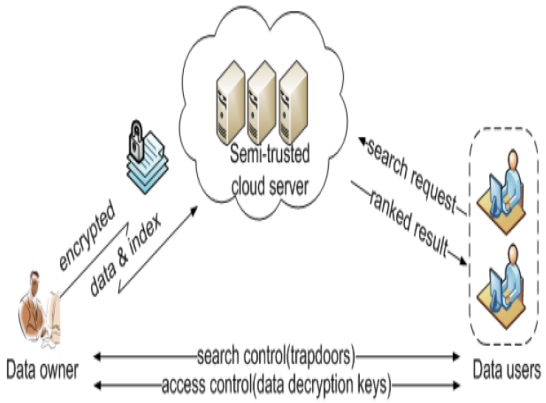


Figure 1: Architecture

Single Keyword Searchable Encryption

With the single keyword, the searching is encrypted with various schemes that are indexed with the server. This searching is done and accesses the document with a secret key. Previous research did on a secure positioned watchword search that uses shibboleth repetition to rank outcomes as opposition returning dedifferentiated outcomes [8]. even so, it simply supports a single keyword search. Wherever anybody with the open key will detain bit with the data place away on the server, but simply approved purchasers with the personal key will look. Customary single watchword accessible secret writing plans area unit generally worked in a very different manner by creating an encoded accessible record. Such files substance is lined up to the server. The information is uncovered simply once the server offers the correct trapdoors that area unit created by means that of a secret key(s). The elemental drawback of single watchword based mostly inquiry is that it is not sufficiently happy to precise advanced information desires.

III. RANKED KEYWORD SEARCH

Ranked search considerably upgrades framework simple use by restoring the coordinating documents in a much positioned request with regard to bound importance criteria (eg. keyword frequency) afterward, creating one bit nearer toward helpful causing of protection safeguarding info facilitating administrations with regards to distributed computing. To the most effective of knowledge, it offers a lawful standing simply because of the difficulty of powerful positioned keyword search over encoded cloud information. Positioned watchword search firmly offers framework simple use by restoring the coordinating records in positioned request disquieted to bound significance criteria,

during this means moving shut towards the helpful activity of security saving info exhibiting administrations in the cloud.

IV. EXISTING SYSTEM

The immense number of data customers and records in cloud, it is huge for the request organization to allow multi-watchword question and give result likeness situating to meet the convincing data recuperation need. The open encryption revolves around single watchword look for or Boolean catchphrase look, and only from time to time isolates the rundown things [9].

Disadvantage:

- Searching of single keyword is time taking process.
- Keyword searching without ranking.
- This will support only single keyword.
- Very less results.

Enhanced Privacy and Secure Storage data (EPSS) can be searched with the multiple keywords. For the searching of multiple keywords the **Enhanced Keyword Search (EKS)**

In this paper, multiple keyword searches play the major role because every end user wants to search the data available in cloud storage. To access the data after searching the key is sent to the mail of the authorized user. If the key is correct only then the file can be accessed.

Enhanced Algorithm Steps:

Step: 1 Enter Keyword

Step: 2 function matchtext(text[], pattern[]){

// let n be the size of the text and m the size of the// patternfor(i = 0; i < n; i++) {

for(j = 0; j < m && i + j < n; j++)

if(text[i + j] != pattern[j]) break;

// mismatch found, break the inner loopif(j == m) // match found

}

}

Step: 3 Calculate time to retrieve the results

Step: 4 Show results

Step: 5 Display time (sec)

Multi keyword Search	Time (MSec)
Existing System	10.987
Proposed System	5.987

Table: 1 keyword searching results for a multiple keywords

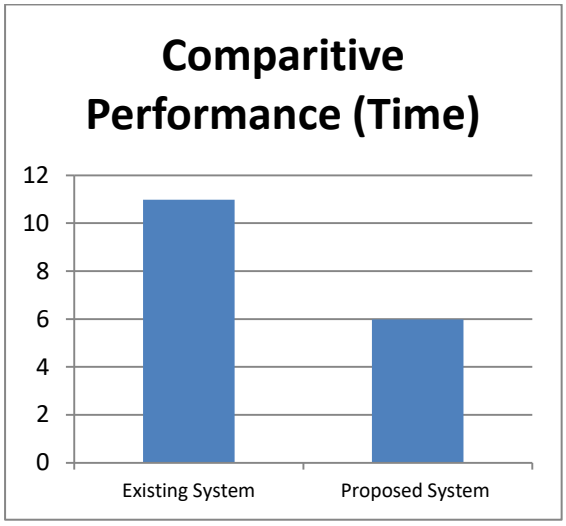


Figure: 3 time (msec)

Enhanced Privacy and Secure Storage data (EPSS)

There are many searching algorithms are available, and to create respect for some area unit as per the following: Searchable Encryption: It allows users to search the data securely through complete encoded info through keywords. This strategy supports simply Boolean search, while not catching any applicable info. This system experiences 2 basic disadvantages once lawfully applied with regards to Cloud Computing. The initial one, users WHO do not very have pre-information on the disorganized cloud info, got to post method every document got, all at once, to get ones most coordinating their advantage; another disadvantage, usually obtaining all records containing the questioned shibboleth any causes pointless system traffic, once recover over one records.

Algorithm Steps

Step: 1 after the searching results retrieved.
Step: 2 select the required document
Step: 3 Download
Step: 4 Enter key to download
Step: 5 User have to check the mail for encryption key.
Step: 6 key received by the user.
Step: 7 enter for document.
Step: 8 document downloaded.

V. CONCLUSION

In this paper, Enhanced Security is most widely provided to secure the data in cloud storage. The Enhanced Multi-Keyword search with secure data storage is implemented with advanced encryption and decryption algorithm. This is the most secure algorithm which provides high security with the generated private key that can be accessed by the user.

REFERENCES

1. M. Armbrust, "A perspective on distributed computing", Interchanges of the ACM, vol. 53, no. 4, (2010), pp.50-58.
2. Peng Xu and Hai Jin. "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack". Cryptology ePrint Archive, Report 2010/626, 2010. http://eprint.iacr.org/.

3. Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE TPDS, VOL., NO.1,2015.
4. Bing Wang, Wei Song, Wenjing Lou, and Y. Thomas Hou "Inverted Index Based Multi-Keyword Public-key Searchable Encryption with Strong Privacy Guarantee", IEEE INFOCOM, 2015.
5. Yanzhi Ren, Yingying Chen, Jie Yang, Bin Xie " Privacy-preserving Ranked Multi-Keyword Search Leveraging Polynomial Function in Cloud Computing", GCISSS 2014.
6. Hongwei Li, Dongxiao Liu,Yuanshun Dai, Tom H. Luan, And Xuemin (Sherman) Shen "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", December 2014.
7. Mikhail Strizhov and Indrajit Ray "Multi-keyword Similarity Search Over Encrypted Cloud Data" ICPC, 2012.
8. Syamala M., Maguluri L.P., Gupta A.G., Akhila T., Bhargav T. (2018), "Optimized Image Compression Method for Portable Devices". In: Sa P., Bakshi S., Hatzilygeroudis I., Sahoo M. (eds) Recent Findings in Intelligent Computing Techniques. AISC, vol 709. Springer, Singapore.
9. Gupta A.S.A.L.G.G., Prasad G.S., Nayak S.R. (2019), "A New and Secure Intrusion Detecting System for Detection of Anomalies within the Big Data". In: Das H., Barik R., Dubey H., Roy D. (eds) CCGBDA. Studies in Big Data, vol 49. Springer, Cham.