A Review: Efficient Encrypted Searching and Traffic Reduction As Mobile Cloud Services

Mr. Pavan Kulkarni, Mr. Aditya More, Mr. Rahul Patil
Trinity college of Engineering and Research
University of Pune, India.
sbchaudharitrinity@gmail.com
adityamore6059@gmail.com

Mr. Ganesh Pawar , Mr. Sushil Padaghan
Trinity college of Engineering and Research
University of Pune, India.
rspatil45@gmail.com
gaikwadprashant43@gmail.com
ashitoshbelge121@gmail.com

Abstract— Documentation of information on the Cloud Computing run as fast as Cloud entirely in the world. Even so it carriage distress to partron. Unless the data are encrypted For hostage. Encrypted data should be energetically searchable and retrievable Without any concealment particularly for the cellphone user. Although modern Interdisciplinary studies has solved many distress , the architectonically can not be applied on cellphone directly under the cellphone cloud environment. This is due to the contradict charged by wireless networks, such as latency sensitivity ,Poor connectivity, and low transmission rates. due to this extend to a chronic search Time and extra network traffic value. When using the conventional search schemes. This paper solve these matter by providing an efficient encrypted data search Method as cellphone cloud service. This method include lightweight trapdoor (encrypted Keyword) differentiate method, which is optimization of data sending process by decreasing the trapdoors size for traffic efficiency. In this publication we also include two Optimization method for data search, known as the trapdoor mapping table module and Ranked serial binary search algorithm to quick the search time. So by using Efficient data search over mobile cloud it Decreases search time by 34% to 47% and also network traffic by 17% to 41% .

Keywords- *Mapping Tables, Indexes, Trapdoor, Hand-held devices.*

*****

I. Introduction

Since cloud computing can patronage flexible services and provide a parsimonious use of storage and computation assets, therefore it is growing phenomenal. With more powerful cloud assets, many data providers can colonize their data in clouds instead of directly attend to users. The cloud also allows providers to empower important tasks such as record searches. To protect data security occupants need to impeach certain records, they first send tokens to the authentic data provider. The provider then generates encrypted tokens i.e also called trapdoors and acknowledgment the trapdoors to the occupant. The occupant then sends these trapdoors to the cloud. Upon inherited the trapdoors, the Cloud uses a definite search algorithm, the records and their docket(index) are usually encrypted before outsourcing to the cloud for searches. When to select a set of appropriate records (encrypted) based on the encrypted indexes and given trapdoors. At the end, the occupant receives these encrypted search outcomes and uses the private key from the provider to decrypt records. This constitution, as illustrate in Figure 1, preserved data security while enfranchise the providers to utilize both the whole calculations and repository power of the Cloud for document searches. Due to these benefits, this constitution has already been well recommended in privacy-preserving search systems.

Handheld devices (e.g. cell phones and tablets) were interpreted to outstep two billion developments (0.5 billions for Desktop PC's) in the year 2014, which directs the general consignment of shopper hardware appliance. Now a days, occupants rapidly use handheld devices to demand archive inspect administrations.

By and large, handheld device interface with the Internet usually by assets of remote systems (WiFi/3G/4G/LTE), which gather about some perplexity when contrasted with conventional wired systems.

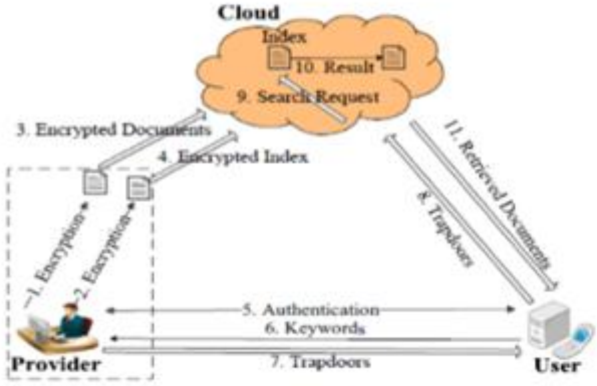


Figure 1. Traditional Encrypted Search System over Cloud

We erect to address these troubles. Our engineering incorporates a trapdoor pressure tactics to diminish process costs, and a Trapdoor Map Table (TMT) module and RSBS forecast to falling off look time.

II. LITERATURE SURVEY

After 2000, D. Song, D. Wagner, A. Perring proposed various technique for the searching operation over encrypted data before that there is hardly any work about searching of encrypted data . They proposed various technique for securely searching of encrypted data with number of advantages. The Boolean Keyword Search proposed by them is not suitable for cloud search as it not identify exact file and send all matching files to client therefore it increase network traffic. After that various work done towards efficient searching technique over encrypted data. The current system consists of provider, cloud and user. The provider outsources the document and index to the cloud. The cloud is internet based commercial storage that provide share computer processing resources and data to computer and other device on demand. The user is someone who has to search, store, retrive document. User enter keyword for the searching document or matching keyword. In our scenario the smartphone is used by user instead of computer device. So the network is wireless therefore the traditional system architecture is not suitable for mobile devices due to low transmission rate, poor connectivity. Due to this search require long time and extra traffic cost.

Using lightweight trapdoor (encrypted keyword) compression method, we optimize the data communication process and increase traffic efficiency. Also with use of Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search algorithm search speed can be increased.

III. SYSTEM OVERVIEW

Cloud:

cloud as a network or internet ,cloud are provided collection service present at remote location.

Types of cloud :

Public cloud
Private cloud
Hybrid cloud

Cloud service: 1. Information as a service (IAAS): It a basic level the a provide a service like a physical machine, virtual machine and storage and also software service

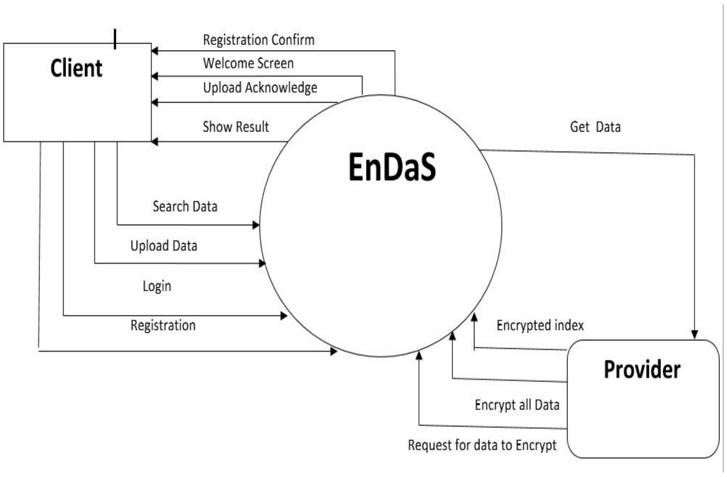
2. Platform as a service (PAAS): User can be access require a component the develop and approach application over internet

3. Software as a service(SAAS): It allow the a user software application or service user need to have physical copy can be installed on own machine

IDE: Netbeans is use for software development in written java. The platform allow application To be developed from different set of modular and software components known as module Including the NetBeans integrated development environment. Application based ntebeans platform. Netbeans basically support java and other languages like PHP,C,C++,HTML. Netbeans IDE is cross platform and runs are different operating system Microsoft window, mac OS, Linux, Solaris and required supporting a compatible JVM.

The netbeans team product and suggestions from the winder community. after every is time for community testing and feedback.

There different toll are
NetBeans profiler
GUI design tool
NetBeans JavaScript editor



IV. SYSTEM ARCHITECTURE

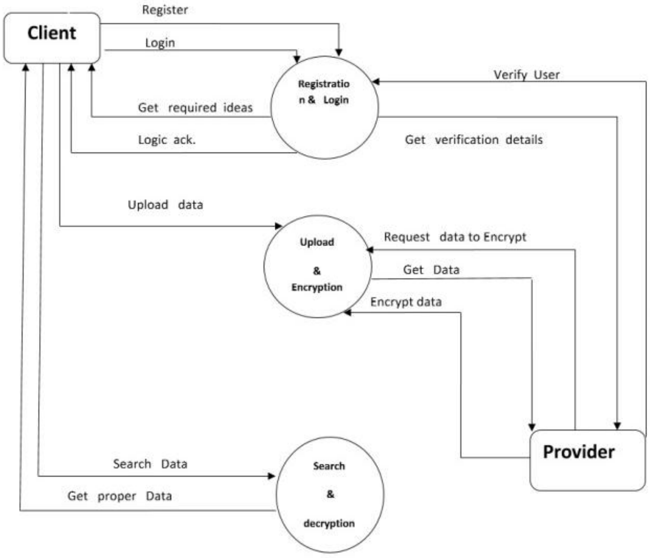


Fig (5): System Architecture

The above figure (fig.5) shows the flow of the Search Me System

Registration:

Data Owner Module

The data owner should build a TF table as index and encrypt in order to offload the calculation and ranking load of the relevance scores to the cloud. So as to control the statistics information leak, we implement our one-to-many OPE in the data owner module. The authentication between the data owner and the data user is provided in order to ensure the security of traffic and energy efficient encrypted keyword search.

Data User Module

The data user sends his identity to the data owner and gets the secret keys if authenticated. An authenticated user stems the keyword to be queried, encrypts it with the keys and hashes it to get its entry in the index. Then the encrypted keyword is sent to the cloud server. On receiving the encrypted keyword, the cloud server will find the top-k relevant files and sent back to the data user where the top-k is configured by the users. The data user decrypts the files and recovers the original data.

Cloud Server Module

During the file retrieval process, the authenticated data user sends the encrypted keywords to the cloud server and gets top-k ranked files back

Advantages

- The traditional encrypted searchable scheme architecture in terms of network traffic and search time is examined. Results show that the typical approach is not applicable in mobile cloud environments.
- An efficient searchable encryption scheme to address these challenges is developed. The architecture includes a access key compression method to reduce traffic costs, as well as a access key FHA algorithm to reduce search time.
- The efficiency of an efficient searchable encryption scheme in network traffic and search time is evaluated.
- Data owner encrypts data before outsourcing onto the cloud, and users retrieve the interested data by encrypted search scheme it take less time of search
- Save computing and battery capacities of mobile device

V. IMPLEMENTATION

For trapdoor production, EnDAS stocks a pre-computed Trapdoor Mapping Table (TMT) in Hand-held devices, which maps casual English vocable to corresponding trapdoors. When the handheld device begin a search request , the trapdoor is examine up from the table rather than of being requested from the provider. This accumulation recover one network round trip for the trapdoor formation. A graceful trapdoor compression method is used to pull out each trapdoors characteristic bits, record as well as collect location of each individuality bit in order and forward the compressed trapdoor to the cloud. Since these characteristic bits only absorb a small volume in this trapdoor, the compact trapdoor will lead to extra compressed traffic cost for address the trapdoors to the cloud.

VI. CONCLUSION

The traditional search scheme is an initial attempt to create a less traffic and energy efficient encrypted keyword search tool over mobile cloud storages. An encrypted search is achieved in a mobile cloud an efficient implementation Searchable encryption developed. The security study of searchable encryption showed that it is secure enough for mobile cloud computing, to retrieve the data with less traffic and energy consumption efficiently. Searchable encryption over plain-text slightly consumes more time and energy than keyword search, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. Single keyword search scheme is proposed to make encrypted data search efficient.

REFERENCES

[1] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Commun. Tech. Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27– 31, 2011.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” in Proc. Int. Conf. Comput. Commun. (INFOCOM), Apr. 2011, pp. 829–837

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

[4] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2010, pp. 253–262.

[5] C. Gentry and S. Halevi, “Implementing gentrys fullyhomomorphic encryption scheme,” in Advances in Cryptology– EUROCRYPT 2011, 2011, pp. 129–148.

[6] C. Orencik and E. Savas¸, “Efficient and secure ranked multi- ̈ keyword search on encrypted cloud data,” in Proc. Joint EDBT/ICDT Workshops, Mar. 2012, pp. 186–195.

[7] Gartner, “Worldwide traditional pc, tablet, ultramobile and mobile phone shipments on pace to grow 7.6 percent in 2014,” http://www.gartner.com/newsroom/id/2645115.

[8] Trellian, “Keywords number,” http://www.keyworddiscovery. com/keyword-stats.html?date=2014-03-01.

[9] V. Rijmen and J. Daemen, “Advanced encryption standard,” Federal Information Processing Standard, pp. 19–22, 2001.

[10] X. Lai, “On the design and security of block ciphers,” Ph.D. dissertation, Diss. Techn. Wiss ETH Zurich, Nr. 9752, 1992. Ref.: ̈ JL Massey; Korref.: H. Buhlmann, 1992.