International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

FAST PHRASE SEARCH FOR ENCRYPTED CLOUD STORAGE

P.RAGUL PRASAD
B.E. Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India
S.RAKKESH
B.E. Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India
V.P.SHANMUGAM
B.E. Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India
Mr. S. SURESH KUMAR
Assistant Professor (Sr.G), Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India

---

Abstract - Cloud computing has generated much interest in the research community in recent years for its many advantages, but has also raise security and privacy concerns. The storage and access of confidential documents have been identified as one of the central problems in the area. In particular, many researchers investigated solutions to search over encrypted documents stored on remote cloud servers. While many schemes have been proposed to perform conjunctive keyword search, less attention has been noted on more specialized searching techniques. In this paper, we present a phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost.

Our technique uses a series of n-gram filters to support the functionality. The scheme exhibits a trade-off between storage and false positive rate, and is adaptable to defend against inclusion-relation attacks. A design approach based on an application's target false positive rate is also described.

***Key Words*: CLOUD COMPUTING, ENCRYPTED DOCUMENTS,CONJUCTIVE KEYWORDS**

1. INTRODUCTION

As organizations and individuals adopt cloud technologies, many have become aware of the serious concerns regarding security and privacy of accessing personal and confidential information over the Internet. In particular, there cent and continuing data breaches highlight the need for more secure cloud storage systems. While it is generally agreed that encryption is necessary, cloud providers often perform the encryption and maintain the private keys instead of the data owners. That is, the cloud can read any data it desired, providing no privacy to its users. The storage of private keys and encrypted data by the cloud provider is also problematic in case of data breach. Hence, researchers have actively been exploring solutions for secure storage on private and public clouds where private keys remain in the hands of data owners.

Although phrase searches are processed independently using our technique, they are typically a specialized function in a keyword search scheme, where the primary function is to provide conjunctive keyword searches. Therefore, we describe both the basic conjunctive keyword search algorithm and the basic phrase search algorithm.

2. RELATED WORK

Cloud computing provides elastic data storage and processing services. Although existing research has proposed preferred search on the plaintext files and encrypted search, no method has been proposed that integrates the two techniques to efficiently conduct preferred and privacy-preserving search over large datasets in the cloud.

Enterprises outsourcing their databases to the cloud and authorizing multiple users for access represents a typical use scenario of cloud storage services. In such a case of database outsourcing, data encryption is a good approach enabling the data owner to retain its control over the outsourced data. Searchable encryption is a cryptographic primitive allowing for private keyword based search over the encrypted database. The above setting of enterprise outsourcing database to the cloud requires multi-user searchable encryption, whereas virtually all of the existing schemes consider the single-user setting.

Due to the high popularity of cloud computing, more data owners are motivated to outsource the data to the cloud server. In that sensitive data will be encrypted before outsourcing to the cloud server for security purpose. In this paper, we introduce a secure multi-keyword ranked search over encrypted cloud data, which performs dynamic update

operations like deletion and insertion of documents. By combining the vector space model and widely used TFxIDF model for the index construction and query generation

Due to the high popularity of cloud computing, more data owners are motivated to outsource the data to the cloud server. In that sensitive data will be encrypted before outsourcing to the cloud server for security purpose. In this paper, we introduce a secure multi-keyword ranked search over encrypted cloud data, which performs dynamic update operations like deletion and insertion of documents. By combining the vector space model and widely used TFxIDF model for the index construction and query generation

3. OVERVIEW OF PROPOSED SYSTEM

Our framework differs from some of the earlier works, where keywords generally consist of meta-data rather than content of the files and where a trusted key escrow authority is used due to the use of Identity based encryption. When compared to recent works, where an organization wishes to outsource computing resources to a cloud storage provider and enable search for its employees, where the aim is to return properly ranked files. Most other recent works related to search over encrypted data have considered similar models such as, where the client acts as both data owner and user.

LIST OF MODULES

- HOME.
- DATA OWNER MODULE.
- DATA USER MODULE.
- CLOUD STORAGE.

DATA OWNER MODULE:

a) Registration Module:

Registration module is used for admin authentication purpose in which administrator can only access this admin module. It contains authentication type and personal details of admin such as name, designation, mail id, phone number, address, username, password, date of birth, photo and also it can be stored and maintained in database. The person who is authenticating it will access it by using username and password.

b) Login Module:

This module checks the admin register page by checking with mail id and password which is already stored in database. It true data is authenticated that allows to go for main admin module or otherwise that will stay in current page by showing up alert message as Invalid User.

c) Home Module:

In this module Data Owner Home this contains Basic functionalities of cloud that can be helpful for data Owner who is logged on already in session.

d) Upload Module:

In which, the files are uploaded in format of file name, keywords .In this case single keyword does not helps in the searching to avoid this we are using three types of keyword to fetch the file. The file are stored in the encrypted formats.

e) My Files Module:

My Files page shows files which is uploaded by particular data user.

F) Approvals Module:

In this module, the request send by the data user can be authenticated by the data owner. Either accepts the request or rejects the request.

G) Logout:

This module which completely moves you out from the data owner session to the home session.

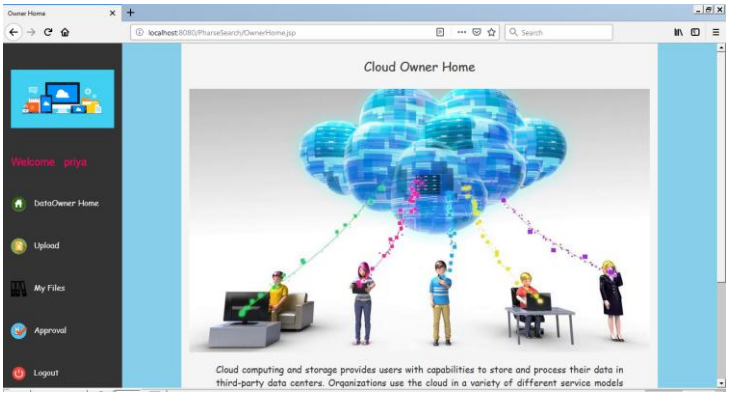


Fig1:data owner module

DATA USER MODULE :

a) Registration Module:

Registration module is used for data user authentication purpose in which administrator can only access this admin module. It contains authentication type and personal details of admin such as name, designation, mail id, phone number, address, username, and password, date of birth, photo and also it can be stored and maintained in database. The person who is authenticating it will access it by using username and password.

b) Login Module:

This module checks the admin register page by checking with mail id and password which is already stored in database. It true data is authenticated that allows to go for main admin module or otherwise that will stay in current page by showing up alert message as Invalid User.

c) Home Module:

In this module Data user Home this contains Basic functionalities of cloud that can be helpful for data Owner who is logged on already in session.

d) Search:

Search module, in which you can search the file that you want. The search request is send as query that finds the data from the cloud and shows your approximate search, you can send request to the file so that particular data owner either accept/decline request as their wish.

e) Requested files:

This shows your file is either accepted or not. If accepted you can view file by particular generated decryption key so that encrypted file will be downloaded as decrypted the readable format.

g)Logout:

This module which completely moves you out from the data user session to the home session.

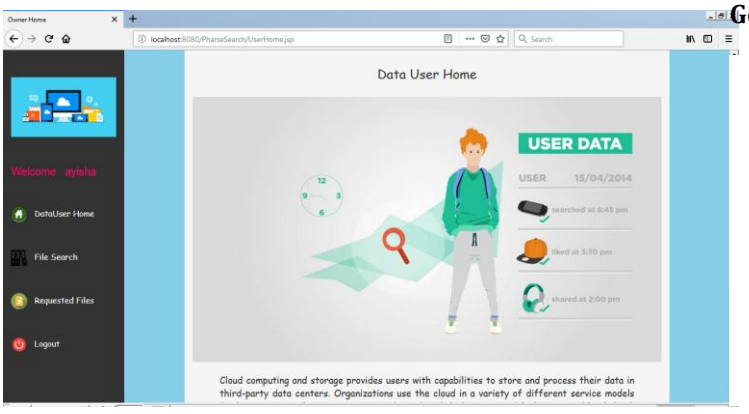


Fig2:data user module

CLOUD STORAGE:

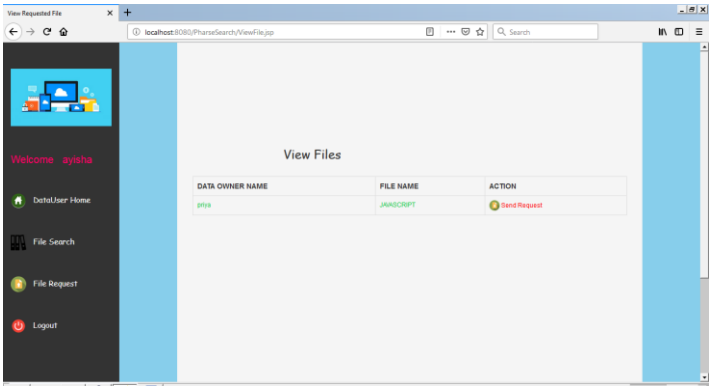


Fig3:cloud storage

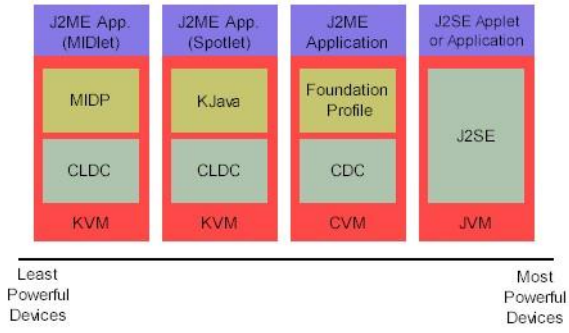
This module completely shows the accurate data stored in the cloud storage .This help you search file that you needed.

4. SOFTWARE SPECIFICATION

J2ME

Sun Microsystems defines J2ME as "a highly optimized Java run-time environment targeting a wide range of consumer products, including pagers, cellular phones, screen-phones, digital set-top boxes and car navigation systems." Announced in June 1999 at the Java One Developer Conference, J2ME brings the cross-platform functionality of the Java language to smaller devices, allowing mobile wireless devices to share applications. With J2ME, Sun has adapted the Java platform for consumer products that incorporate or are based on small computing devices.

General J2ME architecture



J2ME uses configurations and profiles to customize the Java Runtime Environment (JRE). As a complete JRE, J2ME is comprised of a configuration, which determines the JVM used, and a profile, which defines the application by adding domain-specific classes. The configuration defines the basic run-time environment as a set of core classes and a specific JVM that run on specific types of devices. We'll discuss configurations in detail in the profile defines the application; specifically, it adds domain-

specific classes to the J2ME configuration to define certain uses for devices. We'll cover profiles in depth in the following graphic depicts the relationship between the different virtual machines, configurations, and profiles. It also draws a parallel with the J2SE API and its Java virtual machine. While the J2SE virtual machine is generally referred to as a JVM, the J2ME virtual machines, KVM and CVM, are subsets of JVM. Both KVM and CVM can be thought of as a kind of Java virtual machine -- it's just that they are shrunken versions of the J2SE JVM and are specific to J2ME.

5. CONCLUSION

A phrase search scheme based on Bloom filter that is significantly faster than Existing approaches, requiring only a single round of communication and Bloom filter verifications. Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The technique of constructing a Bloom filter index enables fast verification of Bloom filters in the same manner as indexing. According to our experiment, it also achieves a lower storage cost than all existing solutions except where a higher computational cost was exchanged in favor of lower storage. While exhibiting similar communication cost to leading existing solutions, the proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application.

Various challenges in the area of Hidden web data extraction and their possible solutions have been discussed. Although this system extracts, collects and integrates the data from various hidden websites successfully, this work could be extended in near future. In this work, a search engine shell has been created which was tested on a particular domain. This work could be extended for other domains by integrating this work with the unified search interface.

6. REFERENCES

1) K. Cai, C. Hong, M. Zhang, D. Feng, and Z.Lv, "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in IEEE International Conference on Cloud Computing Technology and Science, 2013.
2) Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in IEEE Third International Conference on Cloud Computing Technology and Science, 2011.
3) C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in International Conference on Distributed Computing Systems, 2010.
4) **Hus**M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, "Practical oblivious storage," in Proceedings of the Second ACM Conference on Data and Application Security and Privacy, 2012.
5) Mark Grand and Jonathan Knudsen, "Java Fundamental Classes Reference", Tata McGraw-Hill Publishing Company Limited, 1st Edition, May 1997.
6) Dietel & Deitel, Java How To Program, BPB Publishers, New Delhi, 2000.
7) O'reilly, Java Swings, Tata McGrawHill, Fifth Edition, 2002.