Useful Privacy Promotion Keyword Search Mode

B.V. Pranay Kumar

Associate Professor, Christu Jyothi Institute of Technology and Science, Yeshwanthapur

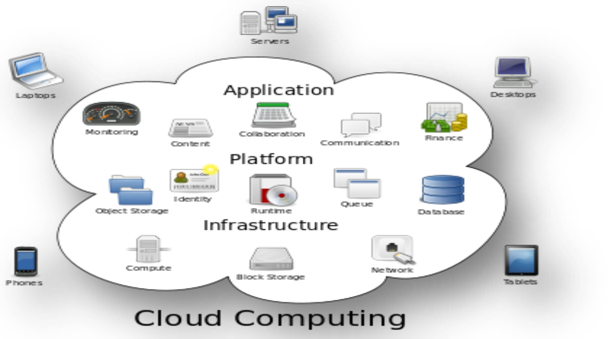
Abstract- **For the purpose of maintaining the confidentiality of owners, Claude prefers to outsource outsourcing documents to documents. Therefore, there is the development of an effective and reliable, which is code-text search technology. The size of the data is also seen in sufficient detail in the data centers. These plans are designed to make it more difficult to find a large quantity of encrypted data storage in an efficient and reliable access to information on the internet to be more difficult text code. In this paper, the hierarchy is a compilation of more research on Earth science and also suggested to support big data environments in a way faster to meet the demand for text search code. The relevance of the proposed approach is to at least introduce the introduction on the basis of a hierarchy documents, and then the maximum size limit is to combine divided into sub groups of groups. Research phase, versus the complexity of ordinary arithmetic, increase the size of documents in the exponential approach collection. To validate the results of order search, in this paper, the minimum retail sub-tree structure of design is called so- called. The experiments were conducted using a collection made in II exploration. Apart from this, the importance of the proposed method and the seizure of documents seized has more benefits in the traditional way of privacy.**

Index Terms- **Cloud computing, cipher text search, ranked search, multi-keyword search, hierarchical clustering, security**

1. INTRODUCTION

What is cloud computing?

Cloud computing resources (hardware and software) use a network (usually distributed as a service on the Internet). The name schemes come from the general use of the code, such as abstract complex cloud infrastructure. Cloud computing is the longest service assigned to customer data, software and accounts. Cloud computing has Internet resources management services for third parties available for hardware and software. Usually forward software applications and servers access the high-end network computer services.



Structure of cloud computing

How Cloud Computing Works?

The economic portfolio does not perform billions of military tens and the research facilities, application-based consumer consumers will provide personal information such as computation cloud computing, or high-performance computing power, with the use of application-based consumer per second, data or large power, computer games storage, attractive Generally PC technology running servers is a low cost with links to separate data through processing commercial use requirements for large groups of cloud computing networks. It shared the basic information systems with the big pool of IT connected. Often, they use virtualization techniques to boost the power of cloud computing.

Features and Services Model: The standards and definitions provided by the terminology (NIST) are based on the National Institutes listed below:

Unusual features of cloud computing: Each service that needs server and storage, such as networking time without the need for human interaction, can automatically consumer user arbitrage capabilities such as computing

- Demand on self-service building.

Client platforms are thin or thicker extrinsic (e.g., mobile phones, laptops, and PDAs) accessible through the use of broadband access network capacity across the network and standard system.

• Assigning resources: is a multi-rented service that provides an important model to serve many customers with various physical and virtual resources and customer demands to restore such as the services computing and provider resources. Users usually do not have the ability to control the spirit of knowledge for freedom or the exact position of resources available, but you may not be able to detect the high level of abstraction (eg, country, state or data center). Examples include storage, processing, memory, and network bandwidth resources, and virtual machines.

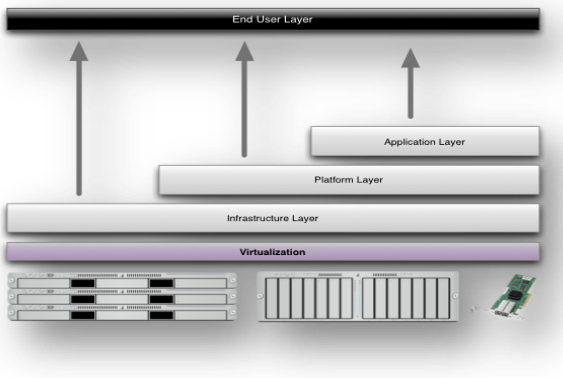
• Rapid elasticity: In some instances where the capabilities are rapidly expanding, the details are faster and conditional flexibility and quicker to quickly release. For the consumer, it is often seen that potential terms are unlimited and can be purchased at any time at any time.

• Measurement Service**:** Cloud systems customization using the advantage of measuring the level of resources and the ability to measure abstract service (for example, accounts, storage, processing, bandwidth, and active user). Resource consumption is maintained, providing transparency for consumer and use service providers.

5 Essential Characteristics of Cloud Computing
On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use
jpinfotech.org

Services Models:

There are three different designs, including the Service Volume, the program service (R) as the stage performance of the infrastructure, cloud computing services, presence of service (IaaS), (custom components). Complete three modal layers after a summary of the end user's perspective on service or end-user layer cloud computing services. This model is shown in the picture below. User access to basic level cloud services, for example, he can implement cloud applications and their own applications for support resources, these applications are responsible for their own maintenance and security. Service level applications and access to these actions are usually taken care of by the Cloud Service Provider.



Structure of service models

2. RELATED WORK

1. Confidentiality-Preserving Rank-Ordered Search

This paper presents a new framework for privacy And to maintain a large document system and to re-ranking group. Protected framework only Documents against external intruder / secret question, But it also protects the data center, learning faith And information about a set of question papers. We offer practical techniques to achieve the importance of proper integration And encryption methods, such as the way of scoring It has also ordered encryption, data protection and protection of groups, To provide indicators and research capabilities efficient and accurate Arrangement of safe documents in response to questions. W3C is a group of experimental results This is similar to the performance of traditional methods Search for the system built for data is encoded Search terms to be corrected Therefore, the proposed road The first step to retrieve modern information And a wide range of applications to secure search capabilities Public and business areas also include data management To enable scientific study of processes, sensitive information Simplifies the process of discovery and litigation of documents.

2.Privacy-preserving multi-keyword text search in the cloud supporting

With the increasing popularity of cloud computing, huge amount of documents are outsourced to the cloud for reduced management cost and ease of access. Although encryption helps protecting user data confidentiality, it leaves the well-functioning yet practically-efficient secure search functions over encrypted data a challenging problem. In this paper, we present a privacy- preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, we propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. To improve the search efficiency, we propose a tree-based index structure and various adaption methods for multi-dimensional (MD) algorithm so that the practical search efficiency is much better than that of linear search. To further enhance the search privacy, we propose two secure index schemes to meet the stringent privacy requirements under strong threat models, i.e., known ciphertext model and known background model. Finally, we demonstrate the effectiveness and efficiency of the proposed schemes through extensive experimental evaluation.

3.Top-k Retrieval from a Confidential Index

Privacy-preserving document exchange among collaboration groups in an enterprise as well as across enterprises requires techniques for sharing and search of access-controlled information through largely untrusted servers. In these settings search systems need to provide confidentiality guarantees for shared information while offering IR properties comparable to the ordinary search engines. Top-k is a standard IR technique which enables fast query execution on very large indexes and makes systems highly scalable. However, indexing access-controlled information for top-k retrieval is a challenging task due to the sensitivity of the term statistics used for ranking.

4. Privacy preserving keyword searches on remote encrypted data

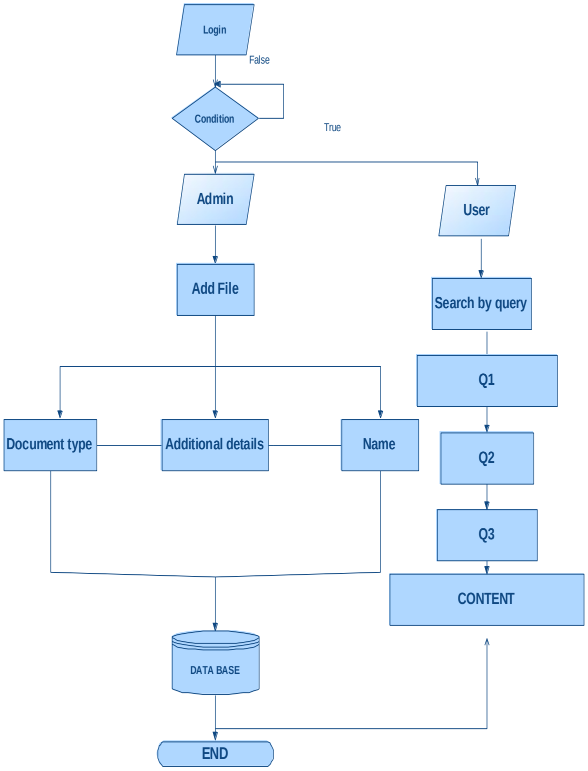
We consider the following problem: a user U wants to store his files in an encrypted form on a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In this paper, we offer solutions for this problem under well-defined security requirements. Our schemes are efficient in the sense that no public-key cryptosystem is involved. Indeed, our approach is independent of the encryption method chosen for the remote files. They are also incremental, in that U can submit new files which are secure against previous queries but still searchable against future queries.

3 BACKGROUND

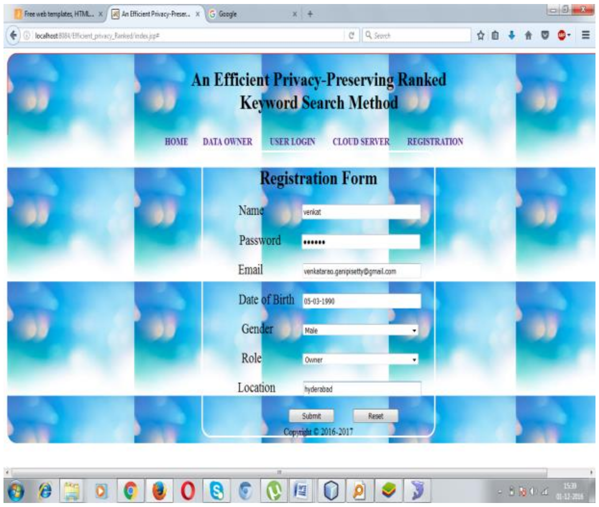
In this paper, we study an interesting problem of recommending products from e- commerce websites to users at social networking sites who do not have historical purchase records, i.e., in “cold-start” situations. We called this problem cross-site cold-start product recommendation. In our problem setting here, only the users’ social networking information is available and it is a challenging task to transform the social networking information into latent user features which can be effectively used for product recommendation. To address this challenge, we propose to use the linked users across social networking sites and e- commerce websites (users who have social networking accounts and have made purchases on e-commerce websites) as a bridge to map users’ social networking features to latent features for product recommendation. In specific, we propose learning both users’ and products’ feature representations (called user embeddings and product embeddings, respectively) from data collected from e-commerce websites using recurrent neural networks and then apply a modified gradient boosting trees method to transform users’ social networking features into user embeddings. We then develop a feature-based matrix factorization approach which can leverage the learnt user embeddings for cold start product recommendation.

4. SYSTEM FLOW

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



5. EXPERIMENTAL RESULTS


Free web templates, HTML...
An Efficient Privacy-Preser...
Google
localhost:8084/Efficient_privacy_Ranked/index.jsp#
Search
HOME
DATA OWNER
USER LOGIN
CLOUD SERVER
REGISTRATION
Submit
Reset
15:20
01-12-2016

An Efficient Privacy-Preserving Ranked Keyword Search Method

Registration Form

Name venkat

Password ••••••

Email venkatarao.genipisetty@gmail.com

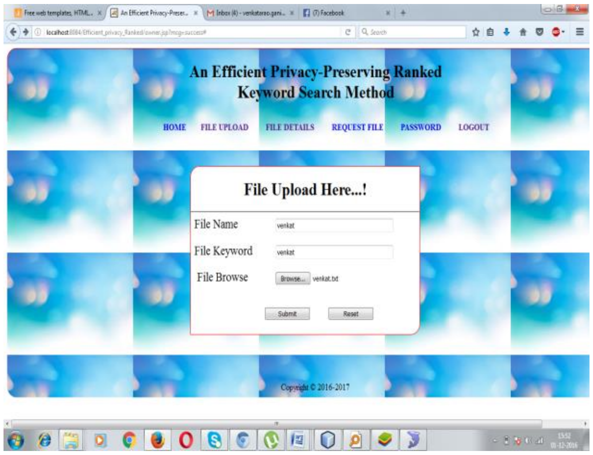
Date of Birth 05-03-1990

Gender Male

Role Owner

Location hyderabad

Copyright © 2016-2017


Free web templates, HTML...
An Efficient Privacy-Preser...
Inbox (4) - venkatarao.gani...
(7) Facebook
localhost:8084/Efficient_privacy_Ranked/owner.jsp?msg=success#
Search
HOME
FILE UPLOAD
FILE DETAILS
REQUEST FILE
PASSWORD
LOGOUT
Browse...
Submit
Reset
15:52
01-12-2016

An Efficient Privacy-Preserving Ranked Keyword Search Method

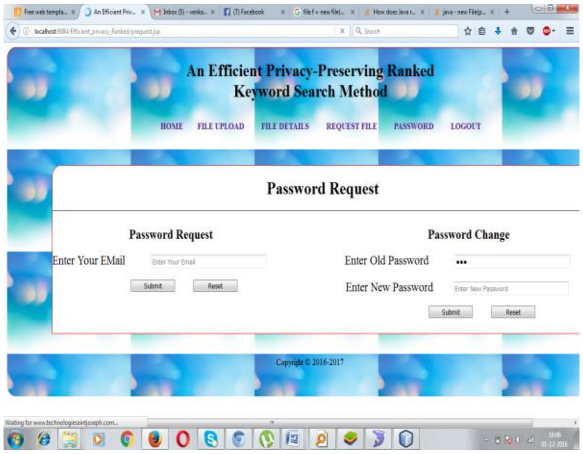
File Upload Here...!

File Name venkat

File Keyword venkat

File Browse venkat.txt

Copyright © 2016-2017



An Efficient Privacy-Preserving Ranked Keyword Search Method

Password Request

Password Request

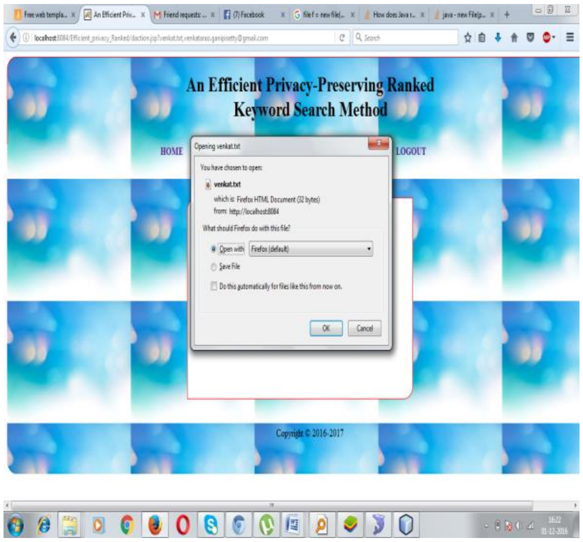
Enter Your EMail Enter Your Email

Password Change

Enter Old Password •••

Enter New Password Enter New Password

Copyright © 2016-2017



localhost:8084/Efficient_privacy_Ranked/daction.jsp?venkat.txt,venkatarao.ganipisetty@gmail.com

An Efficient Privacy-Preserving Ranked Keyword Search Method

Opening venkat.txt

You have chosen to open:

venkat.txt

which is: Firefox HTML Document (32 bytes)

from: http://localhost:8084

What should Firefox do with this file?

● Open with Firefox (default)

○ Save File

□ Do this automatically for files like this from now on.

Copyright © 2016-2017

6. CONCLUSION

In this paper, we investigated ciphertext search in the scenario of cloud storage. We explore the problem of maintaining the semantic relationship between different plain documents over the related encrypted documents and give the design method to enhance the performance of the semantic search. We also propose the MRSE-HCI architecture to adapt to the requirements of data explosion, online information retrieval and semantic search. At the same time, a verifiable mechanism is also proposed to guarantee the correctness and completeness of search results. In addition, we analyze the search efficiency and security under two popular threat models. An experimental platform is built to evaluate the search efficiency, accuracy, and rank security. The experiment result proves that the proposed architecture not only properly solves the multi-keyword ranked search problem, but also brings an improvement in search efficiency, rank security, and the relevance between retrieved documents.

7. BIBILOGRAPHY

[1] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in Proc. IEEE Int. Conf. Consumer Electron.,2011, Berlin, Germany, 2011, pp. 83–87.

[2] D. X. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Priv., BERKELEY, CA, 2000, pp. 44–55.

[3] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, Interlaken, SWITZERLAND, 2004, pp. 506–522.

[4] Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int.Conf. Applied Cryptography Netw. Security, New York, NY, 2005,pp. 442–455.

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, Alexandria, Virginia, 2006, pp. 79–88.

[6] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proc. 27th Annu. Int. Cryptol.Conf. Adv. Cryptol., Santa Barbara, CA, 2007, pp. 535–552.

[7] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. 4th Conf. Theory Cryptography, Amsterdam, NETHERLANDS, 2007, pp. 535–554.

[8] E.-J. Goh, Secure Indexes, IACR Cryptology ePrint Archive, vol. 2003, pp. 216. 2003.

[9] C. Wang, N. Cao, K. Ren, and W. J. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 14671479, Aug.2012.Fig. 12. Search precision.Fig. 13. Rank privacy.CHEN ETAL.: AN EFFICIENT PRIVACY-PRESERVING RANKED KEYWORD SEARCH METHOD 961

[10] A. Swaminathan, Y. Mao, G. M. Su, H. Gou, A. Varna, S. He, M. Wu, and D. Oard, "Confidentiality-preserving rank-ordered search," in Proc. ACM ACM Workshop Storage Security Survivability, Alexandria, VA, 2007, pp. 7–12.

[11] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+R: Top- k retrieval from a confidential index," in Proc. 12th Int. Conf.

Extending Database Technol.: Adv. Database Technol., Saint Petersburg, Russia, 2009, pp. 439–449.

[12] C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure ranked keyword search over encrypted cloud data," in 2010, pp. 253–262.

[13] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Proc. 2nd Int. Conf. Appl. Cryptography Netw. Security, Yellow Mt, China, 2004, pp. 31-45.