ISSN No. 0976-5697

Volume 4, No. 9, July-August 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Efficient and Secure Searching Model for Outsourced Cloud Data

Shynu P.G
Assistant Professor,
School of Information Technology & Engineering
VIT University, Vellore, Tamil Nadu, India
pgshynu@vit.ac.in

Meena Jose
School of Information Technology & Engineering
VIT University, Vellore, Tamil Nadu, India
josemeena@gmail.com

Merris Mary Chacko
School of Information Technology & Engineering
VIT University, Vellore, Tamil Nadu, India
merrismary@gmail.com

Abstract: Cloud computing is a current prominent technology, which has contributed numerous development in the field of computing. In addition to all the benefits of cloud computing, it initiates the efficient monitoring of data service outsourcing. The main activity the users can perform in cloud is storing, sharing and retrieving data. Cloud act like a centralized storage system where all information are well kept and anyone can access it. So there arises a need to encrypt the data before realizing it to the public cloud. To search a data in cloud is a tedious task and to minimize the difficulty level of searching, currently Boolean search technique is adopted. But it has got so many drawbacks as it is more time consuming and produces irrelevant results. To overcome this difficulty a new model is proposed which ensures more security for user's data. A ranked keyword based searching over encrypted data is put forward. In this scheme users are allowed to search over encrypted data. Whenever users take information from cloud it is produced in a ranked order. This method of ranked searching facilitates the usability of system in a great manner by finding the exact matching copy of the file in an arranged order considering important elements like keyword frequency. A privacy enabled data hosting scheme is deployed in the field of cloud computing. The facility to download and view the searched data is enabled which enhance server side ranking with no loss of data. The inefficiency of secured searching is solved in this proposed system. The proposed system is more users friendly and interactive.

Keywords: Cloud Service Provider (CSP), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Message Digest 5 (MD5), Third Party Audit (TPA).

I. INTRODUCTION

Cloud computing services are introduced to the public and more people are using the services nowadays. This hike in the usage has encouraged in bringing more safety measures in storing as well as retrieving data from cloud. Encryption methods are used to ensure security for cloud users. The usage of encryption technique has made the users of cloud to store their data in centralized repositories. Keyword based search has overcome the drawbacks of Boolean search and made searching more user friendly. Data in cloud are saved by adopting symmetric encryption methods. This provides more privacy to user's data. Only registered and authorized users who are approved by the administrator can only search data in cloud at any time. Keyword based searching is done here. One to many order preserving technique is adopted to reduce as well as avoid data leak.

In the context of cloud computing, computing is provided more like a service than a product.

Computing is delivered as a service in such a way that software, resources and other information are provided to the user or other devices as a utility through a specific network. Internet is required to maintain access to remote servers this also avoid the installation process in cloud computing. Across the internet the cloud computing is provided as a service in the form of IaaS, PaaS, SaaS. The users of cloud should pay for the services they are using.

Even if the cloud resources are stored in a remote place, users can access them through the help of mobile app or desktop or web browsers. Microsoft, Amazon web services, VMware, Rockspace, IBM are the prominent cloud computing providers.

Whenever a user needs to search a file in cloud the technique used is Boolean search. In Boolean search words like AND, OR, NOT and NEAR are used to combine words and phrases. Limitations in the Boolean search are removed in the proposed system. The benefit of the new searching model helped to reduce burden for storage maintenance, this promote wide data access independent of the location and reduce cost of hardware software and other maintenances. The prominent growth of cloud computing made cloud users to store more sensitive information into the centralized storage system like emails, personal records, financial information and other valuable documents. The realization that the data owners and the cloud servers are not in the same domain put forward the thought of encryption.

II. RELATED WORKS

The system suggested by author[1] is based on secure ranked keyword search over encrypted cloud data. This method overcome the difficulties exist in the traditional Boolean search system over encrypted cloud data such as the less user

friendliness which causes difficulty for the users who don't have any previous knowledge about the encrypted cloud data have to do lots of search to find the perfect match to retrieve the files. The ranked search methodology proposed in this system retrieves all the matching files in a ranking order depending on the criteria such as keyword frequency etc. Extensive experimental result demonstrates the efficiency of the proposed solution.

System put forward by author [2] is mainly concentrating on securing the multi-keyword ranked search over encrypted cloud data. This system comes with a definition and solution for the privacy preserving multi-keyword ranked search over encrypted cloud data. In this system we suggest certain privacy requirements for the secure utilization of the cloud data. The similarity measure coordinates matching is one of the best among various multi keyword semantics.

Author [3] is mainly introducing a system which is efficient is effective outsourcing of data from the cloud. The main challenge is cloud computing resides in data protection as the users outsource their important data into cloud. At the same time the data collected from the users have to be secured from the unauthorised access from the cloud servers which are the containers of the sensitive user data. The two access control mechanism based on polynomial interpolation technique and multi-near map helps to prevent unauthorised access to a certain limit. The system with this schema, irrespective of the number of data items user has to store only one key material to which he has authorised access.

Author [4] is mainly discussing about the security challenges in the public cloud sector. As public clouds are accessible to everyone, security and privacy should be the main limiting factor to the cloud computing access. Several security challenges, their relevance were the key points discussed in this paper and it also peeks into the secure solutions to perform trustworthy public cloud computing. Data Service Outsourcing Security, Computation Outsourcing Security, access control etc. are the key challenges discussed in this paper.

Author [5] in the paper "A secure code based cloud storage system with secure data forwarding "proposes a policy of threshold proxy re-encryption scheme and collaborate it with central repository erasure code in a such a way that authorized storage medium is created. The storage system not only dependent on authorized data storage and retrieval but also facilitates forwarding of user data in the storage medium to other users without retrieving from other data back. This proposed method deploys encrypting, encoding and decoding, and forwarding of data. Number of parameters is adopted for message copies which are dispatched to storage servers and each storage repository is queried by a server known as key server.

Author [6] in "Toward Secure and Effective Data Utilization in Public Cloud" describes outsourcing of data services where data users and owners can maintain their information to public cloud. The most difficult part is to store and maintain data stored in cloud. The difficulty level is in performance of the system, usability of the system and searching of the data. This paper compares the demerits of fuzzy keyword search over encrypted data. This mainly concentrates on reducing the inconsistency in searching in cloud. Paper also describes about all possible searching methods which will be compactable and more advanced than the existing methods.

Author [7] in "Cloud Storage as the Infrastructure of Cloud Computing" mainly deals with a fast cloud storage. As cloud users can store, retrieve data from anywhere quick data storage need arises. Fast access to company's high performance computing profile and storage structure through web services can be performed through cloud platform. The main advantage of using cloud as a platform is its high performance, configurability and reliability. This functionality is put forward at comparatively low cost compared to other infrastructure.

Author [8] in "Data Outsourcing in Cloud Environments: A Privacy Preserving Approach" mainly deals with the outsourcing of cloud data. With the hike in rise of cost of maintaining IT centres the need for outsourcing their storage and computing necessities to a cloud provider or server. Outsourcing has put forward many crucial issues in the privacy of data in cloud. This discuss about privacy-preserving data outsourcing and the main aim is focussed on providing authentication to the end users. In order to provide security measures vertical fragmentation data outsourcing is employed. The fragments that are allocated to the cloud servers consist of many data without violating security. Confidentiality constraints are used to provide privacy to data.

Author[9] in "Reducing Extra Storage in Searchable Symmetric Encryption Scheme" suggest ways to reduce the extra storage. It is challenging to search encrypted data in cloud, this is because usually cloud users outsource the encrypted form of data to cloud. There arises a need for searchable encryption technique. These kinds of techniques allow users to search on encrypted data without changing or decrypting to cipher text or keyword based search. This paper deals with a kind of construction which can considerably reduce the size of data stored in cloud in the scheme of symmetric encryption and still shows efficiency.

Author [10] proposes a system to encourage search over encrypted data without reducing the privacy schemes. All the available searchable encryption schemes can perform query matching but they fails when it comes to similarity matching. So there arises a need for an important search methodology for easy computation and high performance. Although many cryptographic technique provides such searching schemes its performance in comparatively less compared when it comes to large scale data source searching. This paper deals with an efficient methodology for similarity find search over encrypted data.

III. MATERIALS AND METHODS

The proposed system is developed for making secure searching of cloud data. In this system we used ASP.NET as front end and SQL Azure as the back end. Windows Azure is an open platform allows building a website, deploying and managing website applications throughout the global network.

The system contains 3 modules: Registration module, Search module and Administrator module

A. *Registration Module*

This module contains registration forms for adding new user to the website. End user can search data from the

website. If he wants to download data he has to be a registered user of the site. When a new user registers he will get a username and password. Each user has a separate username and password. A registered user can download books at any time. Frequently used files can be bookmark and kept separately in the database.

B. ***Searching Module***

In this module end users can search for books which he wants to read. Here searching is based on keyword. Administrator will set separate keywords for different books. Keywords will be related to books so user can easily search. User can download the file searched and can be saved in the system. Cloud data are secure and can be easily downloaded.

C. ***Administrator Module***

The administrator has a unique username and password by which he/she may login and upload books to the website, monitor the feedback, view the user details, bookmarked files .The new system helps to enhance the efficiency of the existing system. The system allows users to create their own accounts. It will be verified by administrator. The system is interactive and user friendly. Administrator will give keyword when the books are uploaded. Keyword will be related to the book name. When a user sends a feedback administrator takes necessary steps for the feedback.

Database Design:

In SQL Azure database we will create our website database. Administrator can view, update the book details to the database. End user can search and download details from the database.

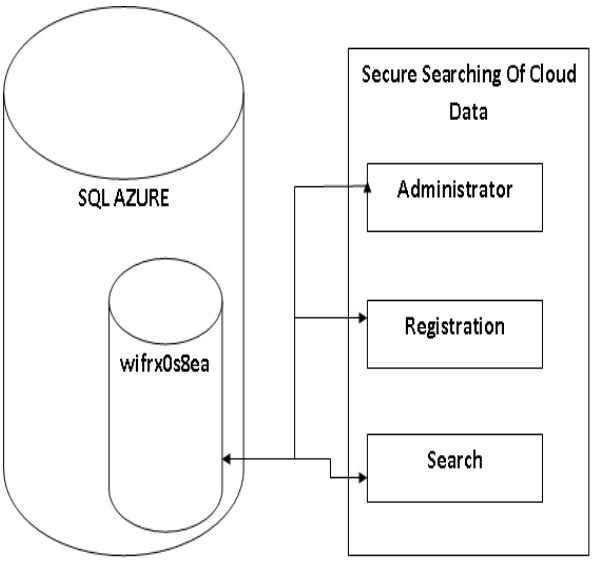

Figure 1 Data retrieval from the SQL Azure Database

IV. RESULTS AND DISCUSSION

Creating a windows azure account and a SQL azure database for our website

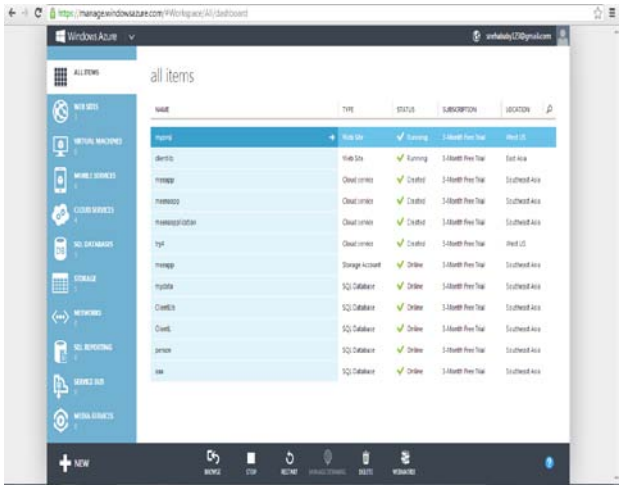

Figure 2: Windows Azure Management Portal

The Windows Azure Management Portal is the web site you will be using to manage our Windows Azure hosted service. We can here add new server, databases etc. Management portal also shows current status of our website.

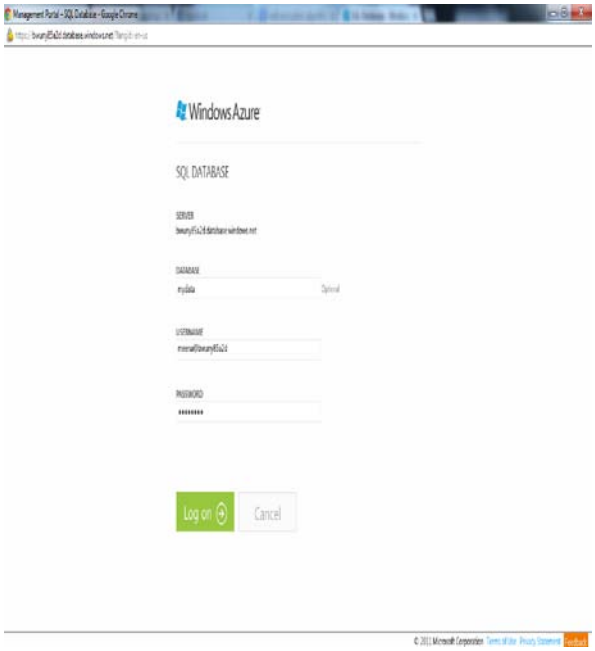

Figure 3: Login page of SQL Azure database

The above shown is the login page to a SQL Azure database. If our username and password are correct we can login the page and create the table. We can create any number of tables inside. Tables are located in distinct server. Since everything is stored in distinct servers there will not be any lack of memory.

Database Creation

In SQL Azure database have a option "New query" for giving query. Each query can be executed using the "Run" button. Creation of table is same as that in SQL server. After creating a table we have to create a clustered index before using the table. Tables can have any number of data and files. Take the

connection string of database and place it in our project.

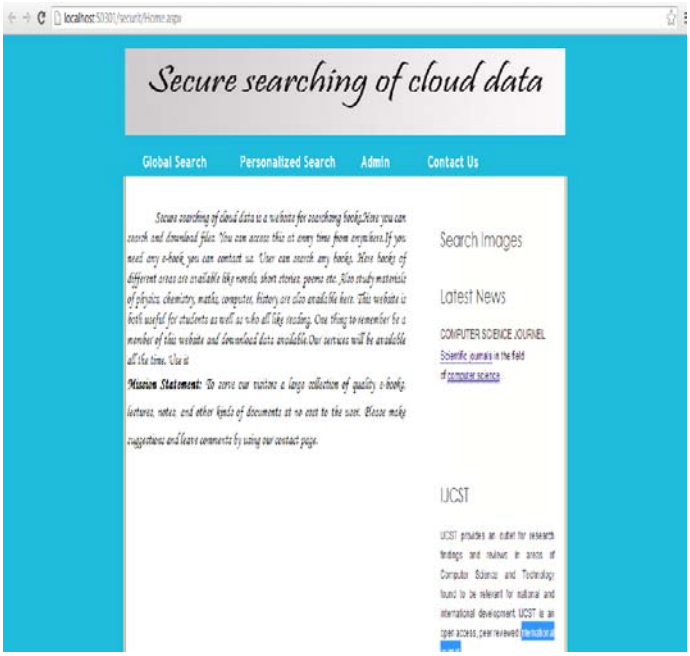

Figure 4: Shows the start page

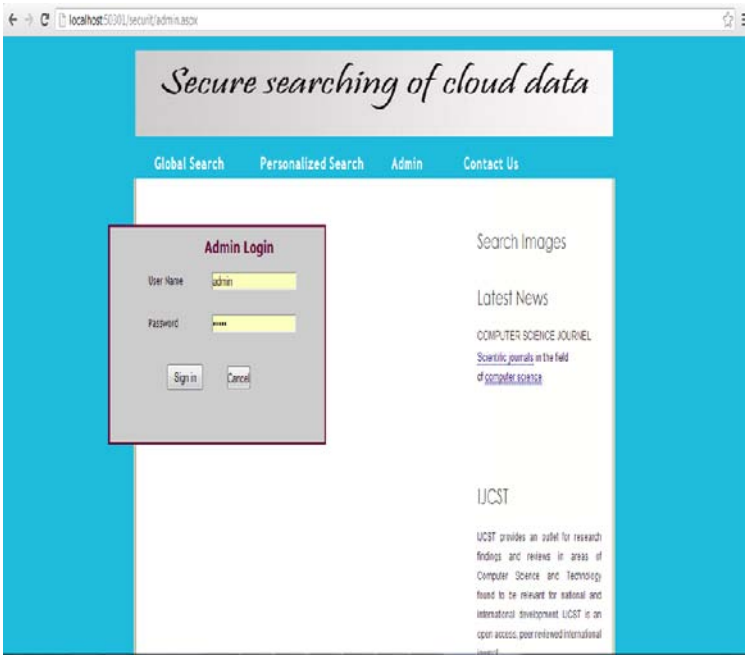

Figure 5: Administrator login page

The above shown is the login page of an administator. Admin is the main user of the system. A seprate username and password for administrator. He can login and upload files. Files can be of any type.

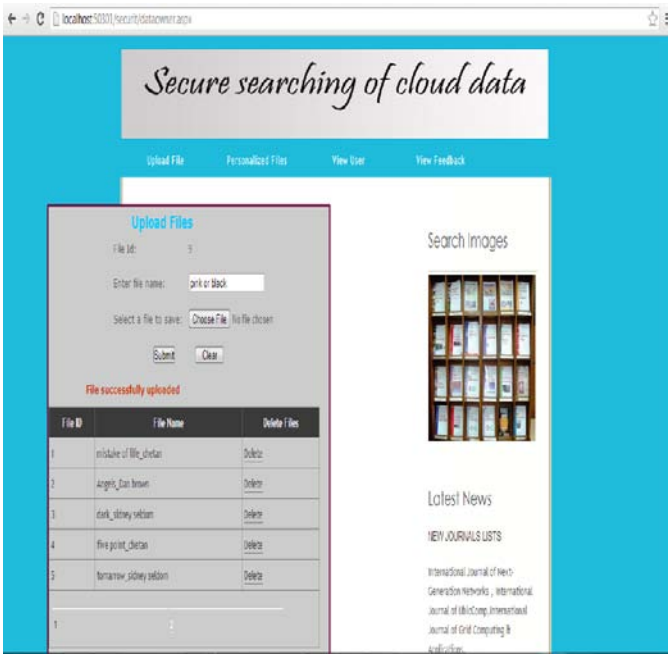

Figure 6: File Uploading

This function is used to upload a file. Here we can specify the location of file in our system. Administrator can specify a name for the file uploaded.

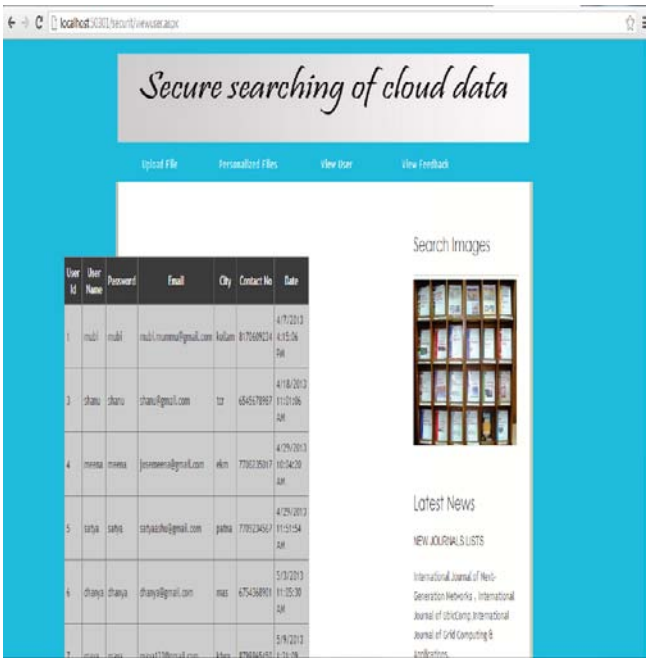

Figure 7: View user

This is used to show who all the registered users of the system. All the registered users will have a username and password. Administrator can view the details of all registered users.

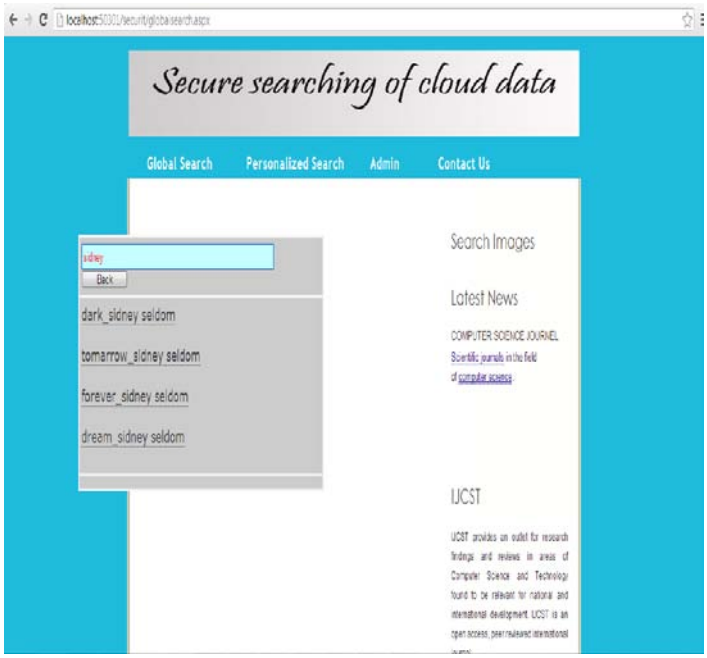

Figure 8: Keyword search

End user can search the file in global search. End users have to specify a keyword for searching. All the search results are displayed. If any file have to be vied press on the file name and we can download the file.

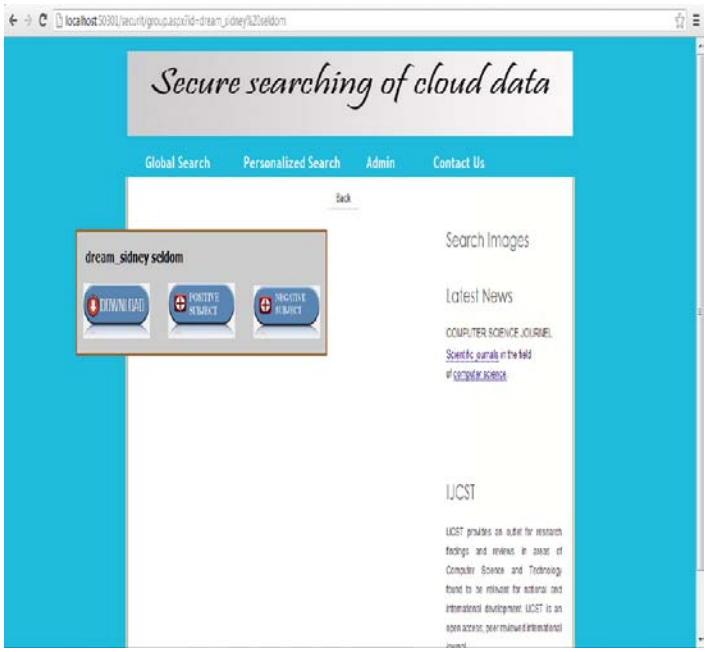

Figure 9: Download a file

End user can download a file if he is a registered user. Here data can be search and according to choice we can download file also.

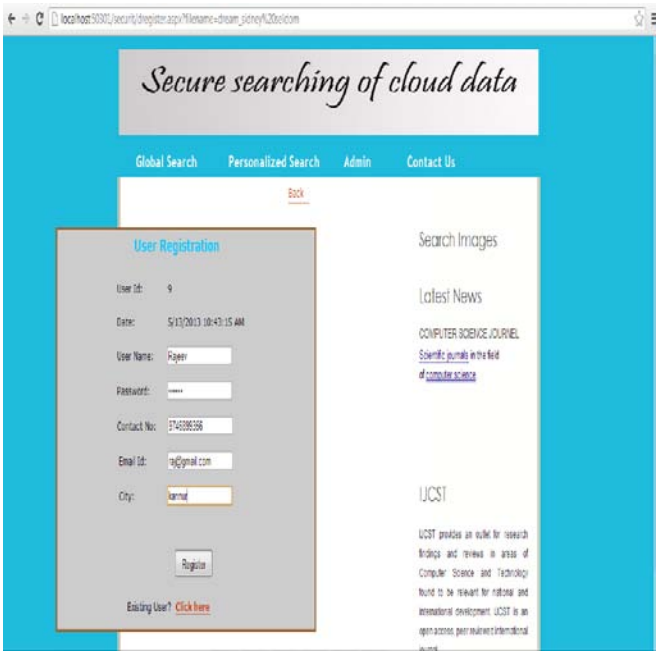

Figure 10: User Registration

End user can be registration can be done using this. When a user is registered he becomes the regular user of the website. He can view; download the files stored in the database.

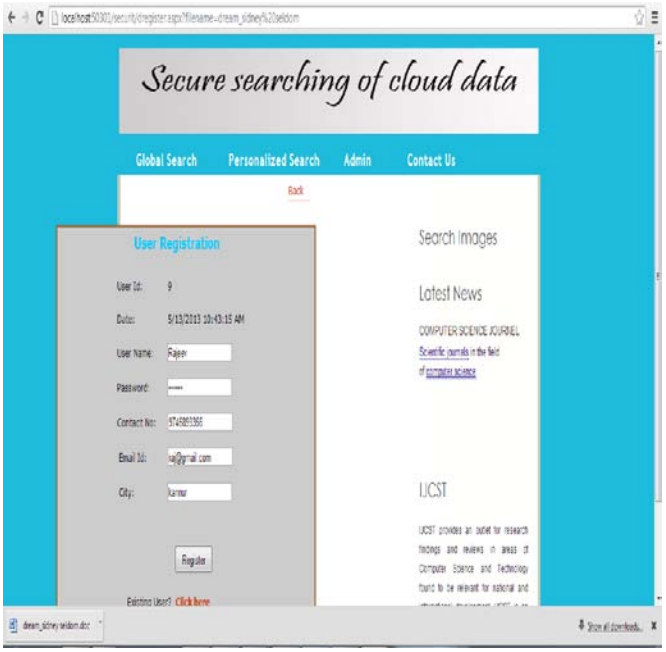

Figure 11: Downloaded File

The above shown is the downloaded file. End user can read the downloaded files. Here searching is done based on keyword search.

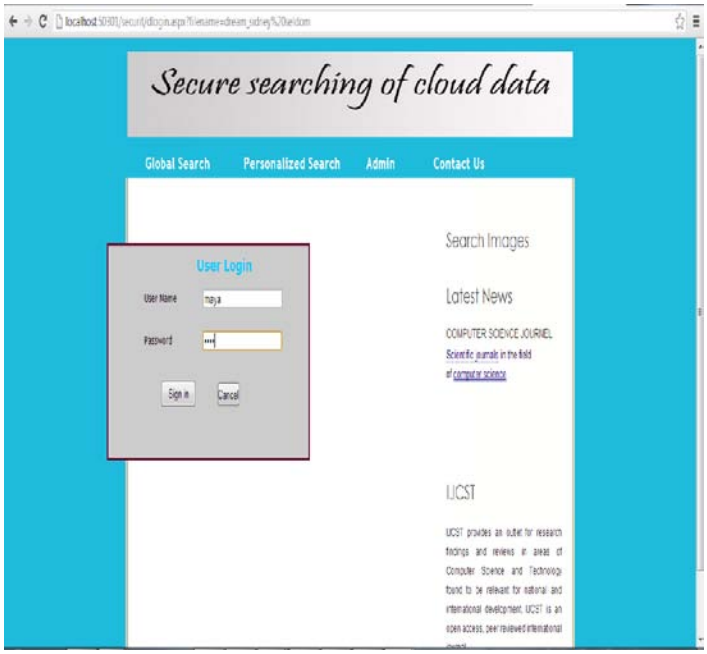

Figure 12: Existing user login

Each user has an individual username and password. They can login that id and download and read books.

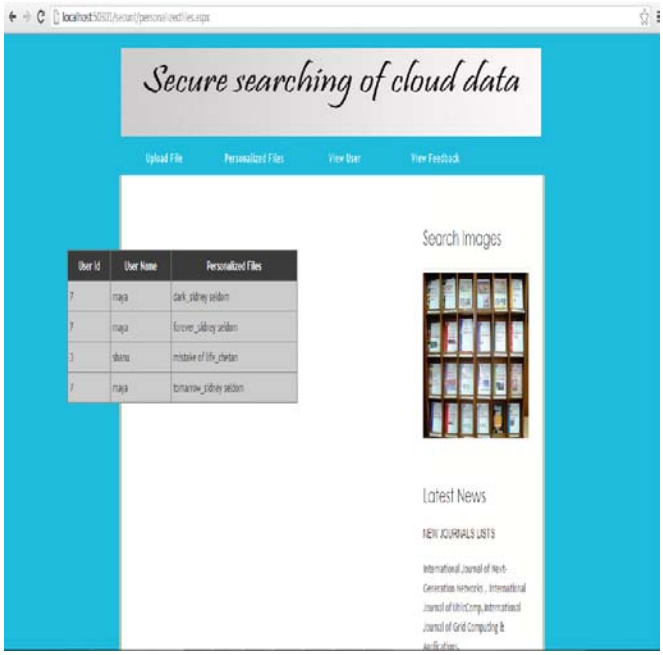

Figure 13: Shows all personalized files

The above shown is the personalized file details. End user can add some files to there account for easy access. Administrator can see all the added files and who added that file. This is to improve the searching speed.

Given below, Figure 14 shows how to send feedback to administrator. In this feedback form user can send the website rating details if any files needed he can ask the administrator. Administrator will upload the requested files as soon as possible. Every file can be identified by the keyword name specified in it.

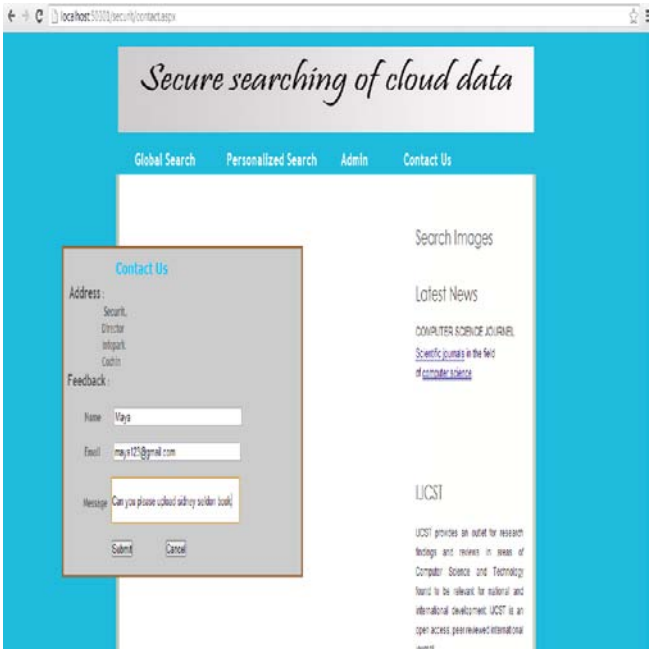

Figure 14: shows how to send feedback

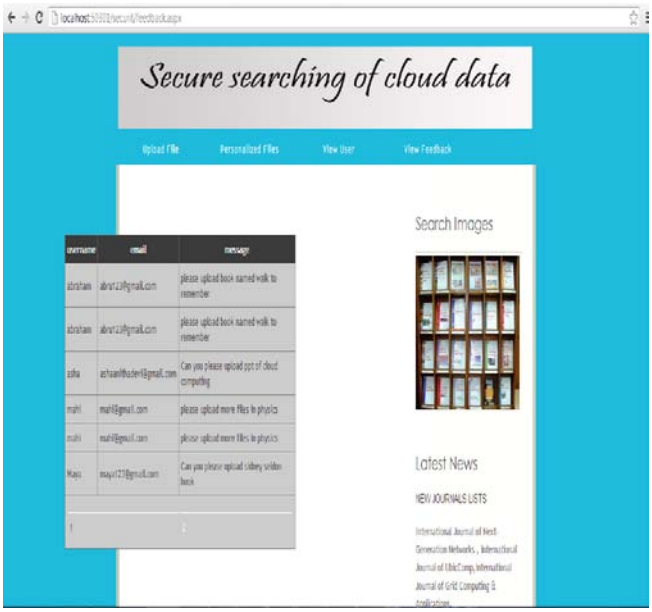

Figure 15: shows the feedback

Figure.15 shows all the feedback came about the site. Administrator can read all feedback.

V. CONCLUSION

With the help of cloud computing a secure searching of outsources cloud data using ranked keyword is developed. Efficient services and easily access is facilitated in this system. Registered and authorized cloud users can store, retrieve data as per there wish at any time. In this system searching is performed on the basis of keywords by adopting a method called ranked search. Ranked search proved to be efficient method as it facilitates system usability by finding and giving back the exact copy of the matching file in ranked order using criteria's like keyword frequency. This facilitates

the deployment of privacy preserving data storing in cloud. This adds to the advancement of cloud computing. The advantage of using cloud computing is that even if the whole data is stored in cloud it leads to low maintenance cost of system and high performance.

VI. REFERENCES

[1] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou (2010). Secure Ranked Keyword Search over Encrypted Cloud Data, Worcester Polytechnic Institute

[2] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou (2011). Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data,Worcester Polytechnic Institute

[3] Purushothama B R, B B Amberker (2012). Access Control Mechanisms for Outsourced Data in Cloud. National Institute of Technology Warangal, INDIA

[4] Kui Ren, Cong Wang, and Qian Wang (2012) .Security Challenges for the Public Cloud, Illinois Institute of Technology

[5] Lejiang Guo, Fangxin Chen, Li Chen, Xiao Tang (2012). A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding , National Chiao Tung University, Hsinchu City

[6] Kui Ren, State University Of New York At Buffalo Cong Wang, (2012). Toward Secure And Effective Data Utilization In Public Cloud Kyung Hee University, City University Of Hong Kong Qian Wang, Wuhan University

[7] Jiyi WU, Lingdi PING, Xiaoping GE,Ya Wang, Jianqing FU (2011). Cloud Storage As The Infrastructure Of Cloud Computing, Hangzhou Normal University

[8] Krishna,Mukkamala R,Baruah(2012).Data Outsourcing In Cloud Environment: A Privacy Preserving Approach,SriSathya Sai Inst.Of Higher Learving,India

[9] Haining Lu, Dawu Gu, Chongying Jin, Yinqi Tang (2012). Reducing Extra Storage In Searchable Symmetric Encryption Scheme, Shanghai Storbridge Information Technology, China

[10] Mehmet Kuzu, Mohammad Saiful Islam, Murat Kantarcioglu (2010). Efficient Similarity Search Over Encrypted Data, University Of Texas At Dallas

