INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 342-351

e-ISSN : 2583-1062

Impact Factor : 5.725

SEARCHABLE ENCRYPTION WITH FINE-GRAINED ACCESS CONTROL FOR PRIVACY PROTECTION

Shaik Azamath Hussain[1], D Murali[2]

[1]M. Tech Student, Cse, Quba College Of Engineering &Technology, Nellore, Andhra Pradesh, India

[2]Associate Professor, Cse, Quba College Of Engineering &Technology, Nellore, Andhra Pradesh, India

ABSTRACT

Searchable encryption facilitates cloud server to search over encrypted data without decrypting the data. Single keyword based searchable encryption enables a user to access a subset of documents, which contains the keyword of the user's interest. In this paper, we present a single keyword based searchable encryption scheme for the applications where multiple data owners upload their data and then multiple users can access the data. The scheme uses attribute based encryption that allows user to access the selective subset of data from cloud without revealing his/her access rights to the cloud server. The scheme is proven adaptively secure against chosen-keyword attack in the random oracle model. We have implemented the scheme on Google cloud instance and the performance of the scheme found practical in real-world applications.

1. INTRODUCTION

Outsourcing data on public cloud facilitates an attractive business strategy to many organizations because of on-demand data/service availability at cheaper rates in an efficient way. However, security and privacy of data have become important concern to the service provider and the service consumers while adopting cloud service, in particular for public cloud, for organization's business goal. The outsourced data may contain sensitive information, such as financial records of an individual or organization, bids information submitted for a tender, Personal Health Records (PHRs) and so on, where the data can allow the cloud server or unauthorized users to access and/or infer sensitive information. To address the issue of data privacy and access control, one practical solution is to encrypt the documents before outsourcing them on cloud storage server. Let us consider the applications where multiple data owners use the public cloud storage services to upload their encrypted documents and multiple users can access the documents stored on the cloud storage server. In such applications, applying fine- grained access control policy will enable intended security control on document access.

2. LITERATURE SERVEY

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

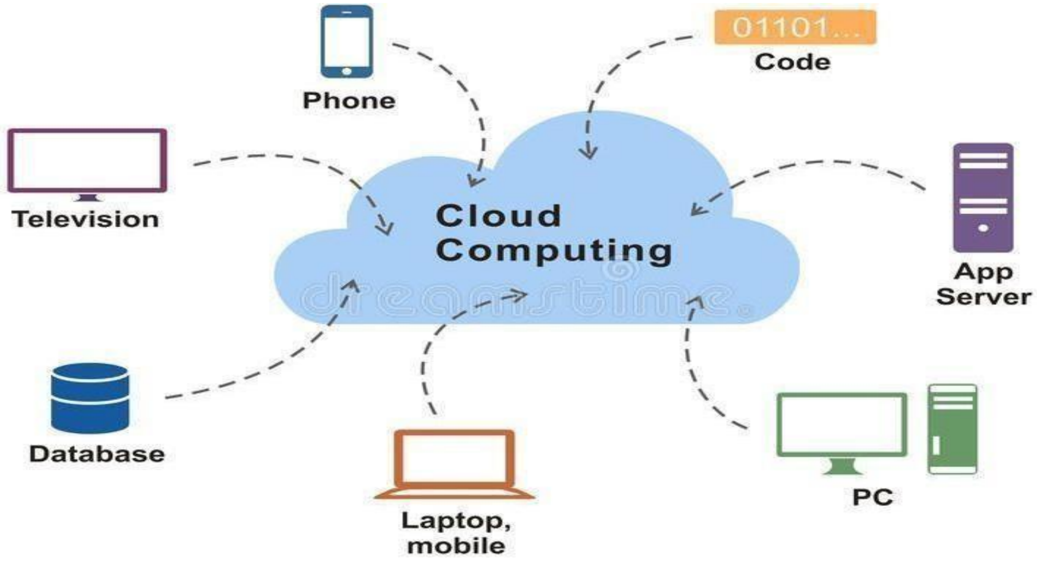


Fig1: Cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high- performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data- processing chores across

This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Service Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed,controlled, and reported providing transparency for both the provider and consumer of the utilized service

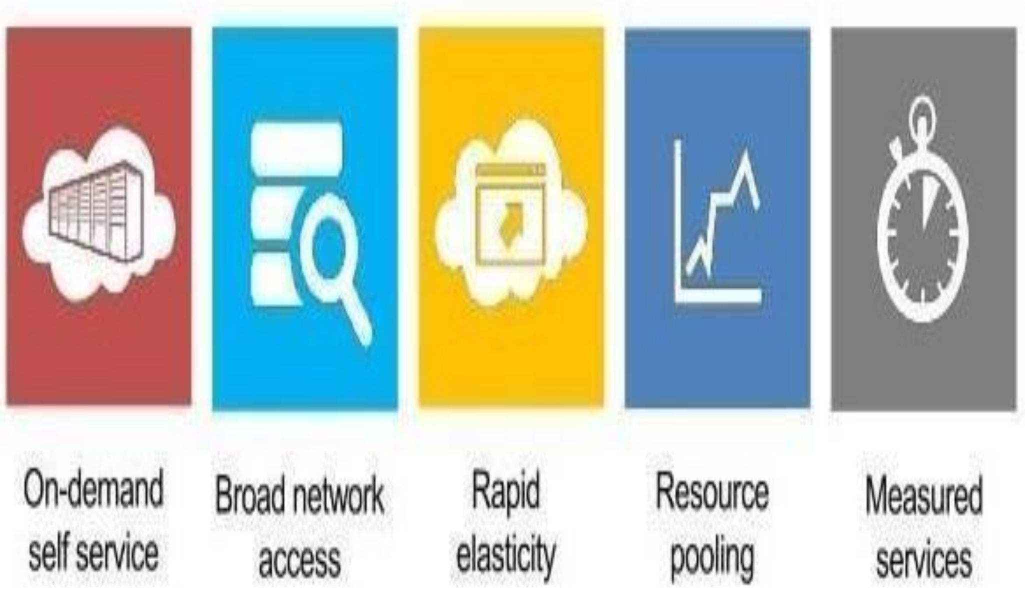


Fig2: Characteristics Service Model

- **Services Models**: Cloud Computing comprises three different service models, namely Infrastructure-as-a Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a- Service (SaaS). The three service models or layer are completed by an end user layer thatencapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider

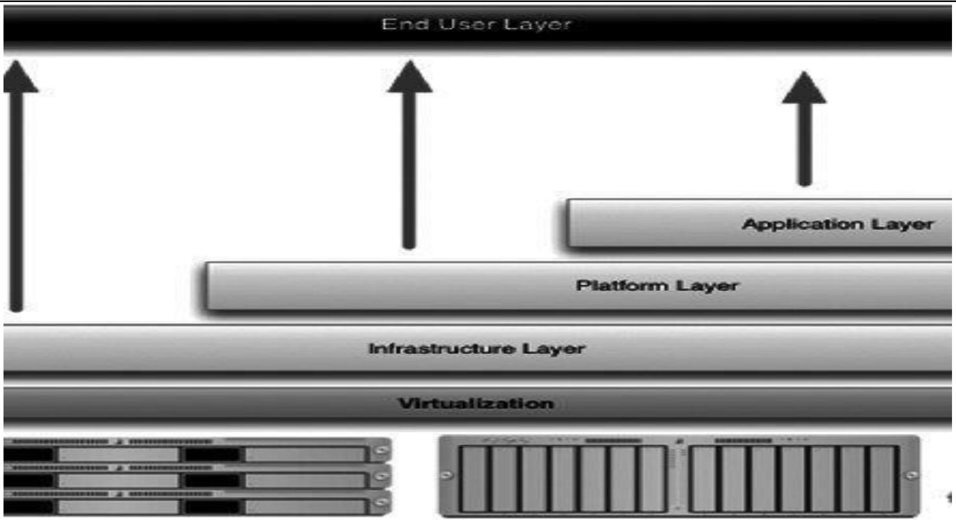


Fig3: End User Layer

Benefits of cloud computing:

- **Achieve economies of scale** – increase volume output or productivity with fewer people.Yourcost per unit, project or product plummets.
- **Reduce spending on technology infrastructure**. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
- **Globalize your workforce on the cheap**. People worldwide can access the cloud, provided they have an Internet connection.
- **Streamline processes**. Get more work done in less time with less people.
- **Reduce capital costs**. There’s no need to spend big money on hardware, software or licensingfees.
- **Improve accessibility**. You have access anytime, anywhere, making your life so much easier!
- **Monitor projects more effectively**. Stay within budget and ahead of completion cycle Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues
- **Minimize licensing new software.** Stretch and grow without the need to buy expensivesoftware licenses or programs
- **Improve flexibility.** You can change direction without serious “people” or “financial” issuesat stake.
- **Advantages:**
- **Price**: Pay for only the resources used.
- **Security:** Cloud instances are isolated in the network from other instances for improvedsecurity.
- **Performance**: Instances can be added instantly for improved performance. Clients have accessto the total resources of the Cloud’s core hardware
- **Scalability:** Auto-deploy cloud instances when needed

3. SYSTEM ANALYSIS

The access policy attached with cipher text in clear form can reveal the receiver attributes which helps adversary in identifying the receiver. For this concern, in many scenarios the access policy is considered as confidential information, as the cipher text should not reveal the purpose of the contents inside the cipher text.For example, in healthcare organization, from the access policy of a patient’s medical report, an adversary can guess the information about the disease of the patient. Therefore, in addition to data confidentiality, preserving privacy of data access is a practical requirement, as one could guess the purpose of the cipher text by identifying the receiver of the cipher text.

If the access policy of an encrypted document is listed in clear form, then it helps the adversary to extract the receiver information, where the receiver information can in turn disclose the statistical information about the encrypted data

4. DISADVANTAGES OF EXISTING SYSTEM

- There exists many attribute based keyword-searchable encryption schemes in literature.
- However, These schemes do not address the important issue of receiver anonymity.
- The major limitation of the Shi et al’s scheme is that the user has to acquire the search token from the trusted

authority, which increases the per query interaction overhead for search operation on user side.

- Furthermore, the scheme works in the scenario, where there are fixed number of keywordfields for which the search should be carried out.

PROPOSED SYSTEM

We present a privacy preserving single keyword-based searchable encryption scheme (PSE) with fine-grained access control. The proposed PSE scheme provides a keyword based search facility over attribute based encrypted data with hidden access policy. The scheme is applicable in a scenario where there are multiple data owners and multiple data receivers.The scheme allows each user in the system with a set of attribute values, where a trusted authority verifies the user's attributes and assigns him a secret key. One of the key features PSE scheme is that once the secret key obtained, the user can generate the search query himself in the form of a trapdoor using the secret key assigned to him

ADVANTAGES

- The PSE scheme preserves the confidentiality of data and privacy of user's access rights.
- The search functionality of the PSE scheme is proven adaptively secure against chosen-keyword attack.
- PSE scheme allows an authorized user to retrieve a subset of documents, over encrypteddocuments stored on CSP

5. SYSTEM REQUIREMENTS

Hardware Requirements:

➢ System	:	Pentium/ Intel Core.
➢ Hard Disk	:	120 GB.
➢ Monitor	:	15'' LED
➢ Input Devices	:	Keyboard, Mouse
➢ Ram	:	1GB.

SOFTWARE REQUIREMENTS:

➢ Operating system	:	Windows family
➢ Coding Language	:	JAVA
➢ Tool	:	APACHE TOMCAT
➢ Back End (Data Base)	:	MYSQL

6. SOFTWARE ENVIROMENT

Client Server Overview-With the varied topic in existence in the fields of computers, Client Server is one, which has generated more heat than light, and also more hype than reality. This technology has acquired a certain critical mass attention with its dedication conferences and magazines. Major computer vendors such as IBM and DEC, have declared that Client Servers is their main future market. A survey of DBMS magazine reveled that 76% of its readers were actively looking at theclient server solution. The growth in the client server development tools from $200 million in 1992 to more than $1.2 billion in 1996.Client server implementations are complex but the underlying concept is simple and powerful. A client is an application running with local resources but able to request the database and relate the services from separate remote server. The software mediating this client server interaction is often referred to as Middleware-The typical client either a PC or a Work Station connected through a network to a more powerful PC, Workstation, Midrange or Main Frames server usually capable of handling request from more than one client. However, with some configuration server may also act as client. A server may need to access other server in order to process the original client request.The key client server idea is that client as user is essentially insulated from the physical location and formats of the data needs for their application. With the proper middleware, a client input from or report can transparently access and manipulate both local database on the client machine and remote databases on one or more servers. An added bonus is the client server opens the door to multi-vendor database access indulging heterogeneous table joins.

What is a Client Server -Two prominent systems in existence are client server and file server systems. It is essentialto distinguish between client servers and file server systems. Both provide shared network access to data but the comparison dens there! The file server simply provides a remote disk drive that can be accessed by LAN applications on a file by file basis. The client server offers full relational database services such as SQL-Access, Record modifying, Insert, Delete with full relational integrity backup/ restore performance for high volume of transactions, etc. the client server middleware provides a flexible interface between client and server, who does what, when and to whom.

Steps in the execution of a JSP Application:

1. The client sends a request to the web server for a JSP file by giving the name of the JSP file within the form tag of a HTML page.
2. This request is transferred to the JavaWebServer. At the server side JavaWebServer receives the request and if it is a request for a jsp file server gives this request to the JSP engine.
3. JSP engine is program which can understands the tags of the jsp and then it converts those tags into a Servlet program and it is stored at the server side. This Servlet is loaded in the memory and then it is executed and the result is given back to the JavaWebServer and then it is transferred back to the result is given back to the JavaWebServer and then itis transferred back to the client.

Hyper Text Markup Language

Hypertext Markup Language (HTML), the languages of the World Wide Web (WWW), allows users to produces Web pages that include text, graphics and pointer to other Web pages (Hyperlinks).HTML is not a programming language but it is an application of ISO Standard 8879, SGML (Standard Generalized Markup Language), but specialized to hypertext and adapted to the Web. The idea behind Hypertext is that instead of reading text in rigid linear structure, we can easily jump from one point to another point. We can navigate through the information based on our interest and preference. A markup language is simply a series of elements, each delimited with special characters that define how text or other items enclosed within the elements should be displayed. Hyperlinks are underlined or emphasized works that load to other documents or some portions of the same document.HTML can be used to display any type of document on the host computer, which can begeographically at a different location. It is a versatile language and can be used on any platform or desktop.HTML provides tags (special codes) to make the document look attractive. HTML tags are not case-sensitive. Using graphics, fonts, different sizes, color, etc., can enhance the presentation of the document. Anything that is not a tag is part of the document itself.

Basic HTML Tags :

<!-- -->	Specifies comments
<A>……….</A>	Creates hypertext links
<B>……….</B>	Formats text as bold
<BIG>……….</BIG>	Formats text in large font.
BODY>…</BODY>	Contains all tags and text in the HTML document
<CENTER>...</CENTER>	Creates text
<DD>…</DD>	of a term Definition
<DL>...</DL>	list Creates definition
<FONT>…</FONT>	Formats text with a particular font
<FORM>...</FORM>	Encloses a fill-out form
<FRAME>...</FRAME>	Defines a particular frame in a set of frames
<H#>…</H#>	Creates headings of different levels
<HEAD>...</HEAD>	Contains tags that specify information about a document
<HR>...</HR>	Creates a horizontal rule
<HTML>…</HTML>	Contains all other HTML tags
<META>...</META>	Provides meta-information about a document
<SCRIPT>…</SCRIPT>	Contains client-side or server-side script
<TABLE>…</TABLE>	Creates a table
<TD>…</TD>	Indicates table data in a table
<TR>…</TR>	Designates a table row
<TH>…</TH>	Creates a heading in a table

- **ADVANTAGES**

➢ A HTML document is small and hence easy to send over the net. It is small because it does not include formatted information.

➢ HTML is platform independent.

➢ HTML ts are not case-s

7. BIBLIOGRAPHY

References for the Project Development were takenfromthefollowingBooks and websites.

- **Oracle-** PL/SQL Programming by Scott UrmanSQL complete reference by Livion
- **JAVA Technologies-** JAVA Complete Reference Java Script Programming by Yehuda Shiran Mastering JAVA Security JAVA2 Networking by PistoriaJAVA Security by Scotl oaks Head First EJB Sierra Bates

  J2EE Professional by Shadab siddiqui JAVA server pages by Larne PekowsleyJAVA Server pages by Nick Todd
- **HTML-** HTML Black Book by Holzner
- **JDBC-** Java Database Programming with JDBC by Patel moss.

8. SYSTEM STUDY

Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forthwith a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the majorrequirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

9. IMPLEMENTATION MODULES

- **Data owner**
- **Data user**
- **Cloud server**

Modules Description:

- **Data owner**

In this module, the data owner uploads their data in the cloud server.

For the security purpose the data owner encrypts the file and the index name and then store in the cloud. The data encryptor can have capable deleting of a specific file. And also he can view the transactions based on the files he uploaded to cloud and will do the following operations like Register and Login Data owners,Req cloud to give enc key permission and view res,Browse file, enc, Apply ABE and Upload, View all Uploaded Files with digital sign, View your files and Update contents, View Your files and Delete ,View sec req and give permission.

- **Data user**

In this module, user logs in by using his/her user name and password. After Loginuser requests search control to cloud and will Search for files based on the index keywordwith the Score of the searched file and downloads the file. User can view the search of the files and also do some operations like Req dec from cloud and view res,Req sec key permission from, Search file ,Data owner and view res,Download the file.

- **Cloud server**

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with Remote User. To access the shared data files, data consumers download encrypted data files of theirinterest from the cloud and then decrypt them.The cloud server authorizes the data owner and the data user and provides the search requests sent from the users. Also in this module it shows personalized search model and the interest search model. Can view all the file attackers and doing following operations View data owners and authorize, View End users and authorize, View enc keyand authorize, View dec key and authorize, View uploaded files, View all files and audit owner data and send log to corresponding owner, View all owner and user transactions, View file attackers, View all file content attackers, Find File rank results in chart, View Time Delay Results, View throughput Results.

10. SYSTEM ARCHITECTURE

Architecture Diagram

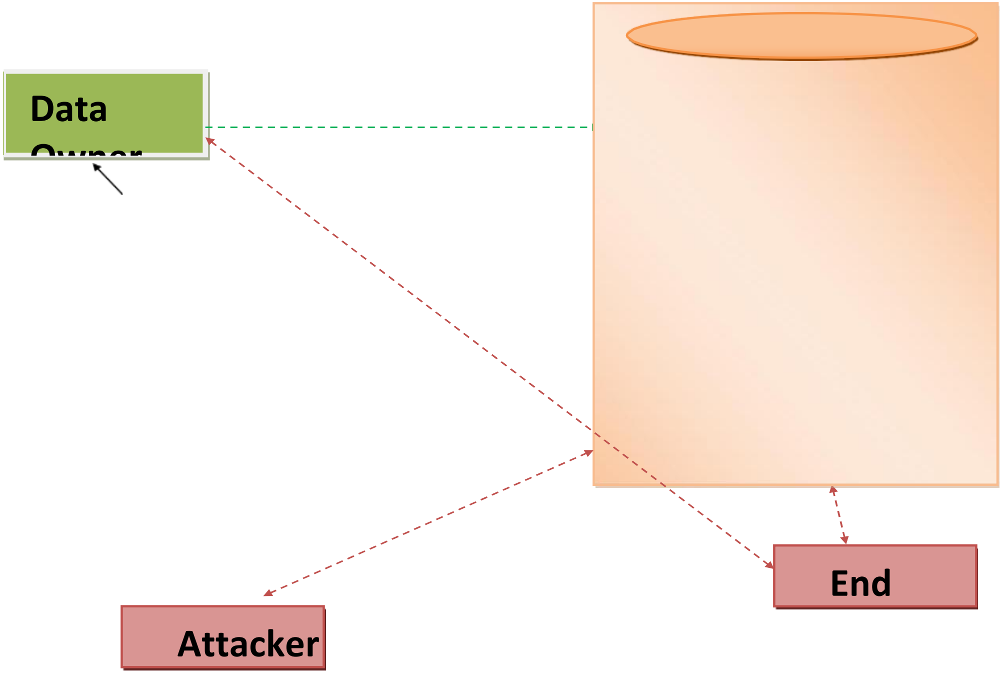


Fig8: system architecture

Cloud Server

1. Register and Login Data owners
2. Req cloud to give enc key permission and view res3.Browse file, enc, Apply ABE and Upload.
3. View all Uploaded Files with digital sign
4. View your files and Update contents
5. View Your files and Delete
6. View sec req and give permission
7. View data owners and authorize.
8. View End users and authorize.
9. View enc key and authorize
10. View dec key and authorize
11. View uploaded files
12. View all files and audit owner data andsend log to corresponding owner
13. View all owner and user transactions
14. View file attackers
15. View all file content attackers
16. Find File rank results in chart
17. View Time Delay Results
18. View throughput Results

Attack contents

Register and Login

1. Req dec from cloud and viewres
2. Req sec key permission from
3. Search file
4. Data owner and view res.
5. Download the file

11. SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement. They are :

- Unit Testing.
- Integration Testing.
- User Acceptance Testing.
- Output Testing.
- Validation Testing.

UNIT TESTING

Unit testing focuses verification effort on the smallest unit of Software design that is the module. Unit testing exercises specific paths in a module’s control structure to ensure complete coverage and maximum error detection. This test focuses on each module individually, ensuring that it functions properly as a unit. Hence, the naming is Unit Testing. During this testing, each module is tested individually and the module interfaces are verified for the consistency with design specification. All important processing path are tested for the expected results. All error handling paths are also tested.

INTEGRATION TESTING

Integration testing addresses the issues associated with the dual problems of verification and program construction. After the software has been integrated a set of high order tests are conducted. The main objective in this testing process is to take unit tested modules and builds a program structure that has been dictated by design.

USER ACCEPTANCE TESTING

User Acceptance of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes wherever required. The system developed provides a friendly user interface that can easily be understood even by a person who is new to the system.

OUTPUT TESTING

After performing the validation testing, the next step is output testing of the proposed system, since no system could be useful if it does not produce the required output in the specified format. Asking the users about the format required by them tests the outputs generated or displayed by the system under consideration. Hence the output format is considered in 2 ways – one is on screen and another in printed format.

VALIDATION CHEACKING

Validation checks are performed on the following

- **Text Field:**

  The text field can contain only the number of characters lesser than or equal to its size. The text fields are alphanumeric in some tables and alphabetic in other tables. Incorrect entry always flashes and error message.

- **Numeric Field:**

  The numeric field can contain only numbers from 0 to 9. An entry of any character flashes an error messages. The individual modules are checked for accuracy and what it has to perform. Each module is subjected to test run along with sample data. The individually tested

- **Using Live Test Data:**

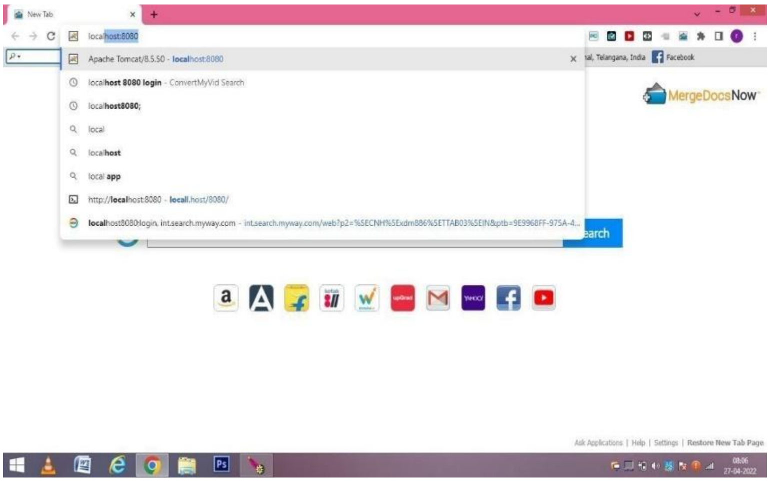
  Live test data are those that are actually extracted from organization files. After a system is partially constructed, programmers or analysts often ask users to key in a set of data from theirnormal activities. Then, the systems person uses this data as a way to partially test the system. In other instances, programmers or analysts extract a set of live data from the files and have them entered themselves.It is difficult to obtain live data in sufficient amounts to conduct extensive testing. And, although it is realistic data that will show how the system will perform for the typical processing requirement, assuming that the live data entered are in fact typical, such data generally will not test all combinations or formats that can enter the system. This bias toward typical values then does not provide a true systems test and in fact ignores the cases most likely to cause system failure.

- **Using Artificial Test Data:**

  Artificial test data are created solely for test purposes, since they can be generated to test all combinations of formats and values. In other words, the artificial data, which can quickly

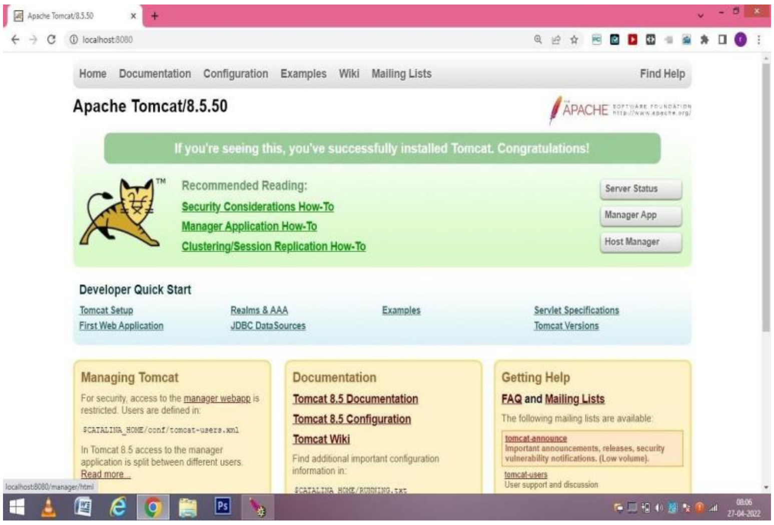
  be prepared by a data generating utility program in the information systems department, make possible the testing of all login and control paths through the program.

12. SCREEN SHOTS



localhost:8080
Apache Tomcat/8.5.50 - localhost:8080
localhost 8080 login - ConvertMyVid Search
localhost8080;
local
localhost
local app
http://localhost:8080 - locall.host/8080/
localhost8080login. int.search.myway.com - int.search.myway.com/web?p2=%5ECNH%5Exdm886%5ETTAB03%5EIN&ptb=9E9968FF-975A-4...

screen1: local host: 8080



Apache Tomcat/8.5.50

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

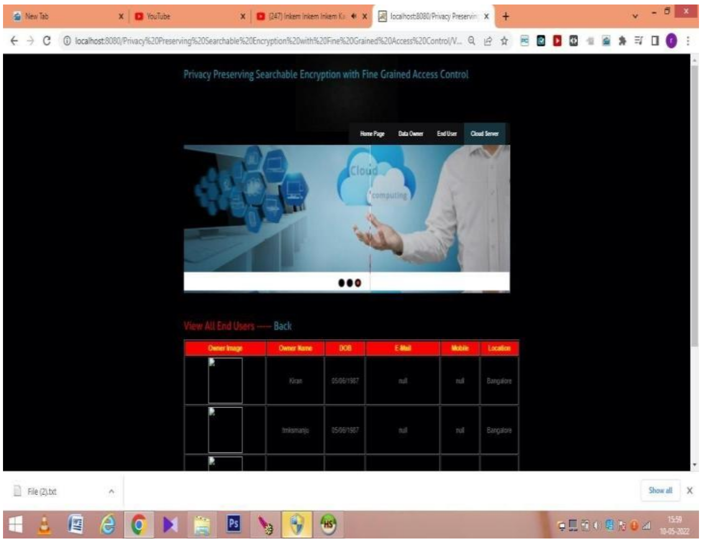
Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
`$CATALINA_HOME/conf/tomcat-users.xml`
In Tomcat 8.5 access to the manager application is split between different users. Read more...

Documentation
Tomcat 8.5 Documentation
Tomcat 8.5 Configuration
Tomcat Wiki
Find additional important configuration information in:
`$CATALINA_HOME/RUNNING.txt`

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion

Screen2: Apache tomcat /8.5.50



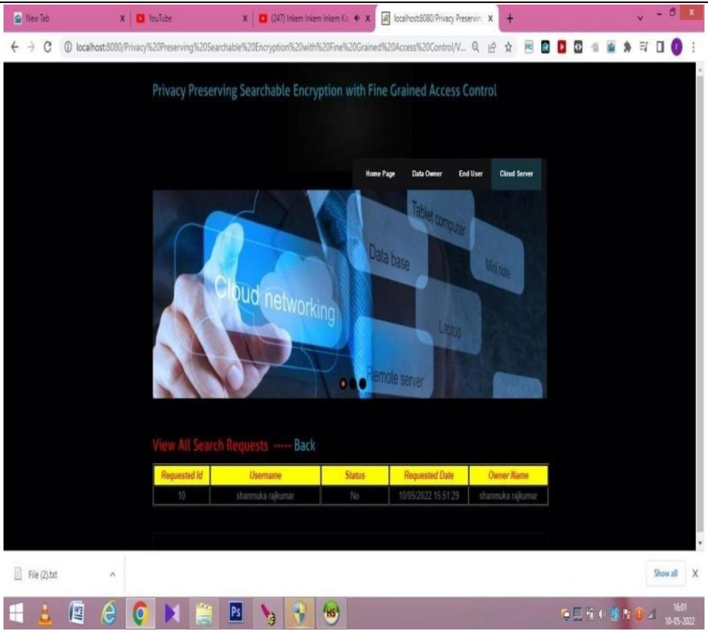
Privacy Preserving Searchable Encryption with Fine Grained Access Control

View All End Users ---- Back

Owner Image	Owner Name	DOB	E-Mail	Mobile	Location
	Kiran	05/06/1987	null	null	Bangalore
	tmksmanju	05/06/1987	null	null	Bangalore

New Tab
YouTube
(247) Inkem Inkem Inkem Ka
localhost:8080/Privacy Preservin
localhost:8080/Privacy%20Preserving%20Searchable%20Encryption%20with%20Fine%20Grained%20Access%20Control/V...
Home Page
Data Owner
End User
Cloud Server
Cloud
computing
File (2).txt
Show all
15:59
10-05-2022

Screen22: View all end user


New Tab
YouTube
(247) Inkem Inkem Inkem Ka
localhost:8080/Privacy Preservin
localhost:8080/Privacy%20Preserving%20Searchable%20Encryption%20with%20Fine%20Grained%20Access%20Control/V...
Home Page
Data Owner
End User
Cloud Server
Cloud networking
Tablet computer
Data base
Mini note
Laptop
Remote server
File (2).txt
Show all
16:01
10-05-2022

Privacy Preserving Searchable Encryption with Fine Grained Access Control

View All Search Requests ----- Back

Requested Id	Username	Status	Requested Date	Owner Name
10	shanmuka rajkumar	No	10/05/2022 15:51:29	shanmuka rajkumar

Screen25: View all search requests

13. CONCLISION

We proposed a privacy preserving attribute based search-able encryption scheme. The proposed PSE scheme allows an authorized user to retrieve a subset of documents, over encrypted documents stored on CSP, pertaining to his chosen keyword and satisfying his access rights. The PSE scheme preserves the confidentiality of data and privacy of user's access rights. The search functionality of the PSE scheme is proven adaptively secure against chosen-keyword attack under DBDH assumption in random oracle model. We have implemented the PSE scheme on Google cloud instance and the performance of the scheme is found practical in real -world applications

14. REFERENCE

[1] Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

[2] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In Proceedings of Applied Cryptography and Network Security, LNCS 5037, Springer, pp. 111–129, 2008.

[3] J. Li, K. Ren, B. Zhu, and Z. Wan. Privacy-aware attribute-based encryption with user accountability. In Proceedings of Information Security, LNCS 5735, Springer, pp. 347– 362, 2009.

[4] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li. Anonymous attribute-based encryption supporting efficient decryption test. In Proceedings of the ACM SIGSAC Symposium on Information, Computer and Communications Security, pp. 511–516, 2013.

[5] P. Chaudhari, M. L. Das, and A. Mathuria. On Anonymous Attribute Based Encryption. In Proceedings of the International Conference on Information Systems Security, LNCS 9478, Springer, pp. 378–392, 2015.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Search- able symmetric encryption: improved definitions and efficient constructions. Journal of Computer Security. 19(5), pp. 895– 934, 2011.

[7] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. C. Rou, M. Steiner, Highly-scalable searchable symmetric encryption with support for boolean queries. In Advances in Cryptology-

[8] CRYPTO, Springer, pp. 353-373, 2013

[9] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, M. Steiner. Outsourced symmetric private information retrieval. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM pp. 875-888, 2013.