WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Reckoning Attack Resistant of E-Health Care Cloud System with Access to Critical Assets

Suresh Babu Mikkilineni [A], Murali Depuru [B]

[A] *M. Tech Scholar, Quba College of engineering, Nellore, Andhra Pradesh, India*
[B] *Associate Professor, Quba College of engineering, Nellore, Andhra Pradesh, India*

A B S T R A C T

The e-healthcare cloud system has shown its potential to improve the quality of healthcare and individuals' quality of life. Unfortunately, security and privacy impede its widespread deployment and application. There are several research works focusing on preserving the privacy of the electronic healthcare record (EHR) data. However, these works have two main limitations. First, they only support the 'black or white' access control policy. Second, they suffer from the inference attack. In this paper, for the first time, we design an inference attack-resistant e-healthcare cloud system with fine-grained access control. We first propose a two-layer encryption scheme. To ensure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we devise a specialized access policy for each data attribute in the EHR, and encrypt them individually with high efficiency. To preserve the privacy of role attributes and access policies used in the first-layer encryption, we systematically construct the second-layer encryption. To take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the EHR, we further construct a blind data retrieving protocol. We also demonstrate that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.

Keywords: **Attack Resistant, E-Health care, cloud system**

1. INTRODUCTION

Introduction About Project

The Electronic Social insurance, giving auspicious, exact, and minimal effort human services administrations, has demonstrated its potential to improve the nature of medicinal services and people's lives. Numerous organizations everywhere throughout the world have built up their social insurance administrations, e.g., Google Fit, Apple Health Kit, and so on. In the mean time, with the increasing development and advantages brought by distributed computing, thee- human services cloud framework has drowned numerous interests from both the scholastic and the business. The IBM organization has officially settled it se-social insurance cloud focus, i.e., IBM Watson Health Cloud. Lamentably, security and protection will obstruct the far-reaching ending and utilization of thee-medicinal services cloud framework. The central reason is that, when the touchy EHR information is redistributed to the cloud, information proprietors would lose their control. Despite the fact that the cloud specialist co-ops guarantee they will save this information by introducing antivirus programming projects, firewalls, and interruption discovery and aversion frameworks, they can't prevent their representatives from getting to this information. For instance, a worker in the branch of veteran's issues once takes away

26.5 million touchy information

1.2 Introduction About Domain

- **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 consist soft 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.

- **Characteristics & Services 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 consumers using a multi-tenant model, 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
- 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 optimizer source use by lever aging gamete ring 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.

❖ **Service 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 that encapsulates 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.

❖ **Benefits of Cloud Computing**

- **Achieve economies of scale**: Increase volume output or productivity with fewer people. Your cost 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.
- **Improve flexibility:** You can change direction without serious "people" or "financial" issues at stake.

2. LITERATURESURVEY

EXISTINGSYSTEM

Only support the 'black or white' access control policy. Specifically, once a data use reauthorized, he can access all the data attributes in the EHR...The inference attack includes the frequency analysis attack

PROPOSED SYSTEMS

- In the first-layer encryption, paper propose to define a specialized access policy for each data attribute in the EHR, generate a secret share or every distinct role attribute, and reconstruct the secret to encrypt each data attribute, which ensures a fine-grained access control, saves much encryption time, and conceals the frequency of role attributes occurring in the EHR.
- In the second-layer encryption, paper proposes to preserve the privacy of role attributes and access policy first-layer encryption. Specifically, merge the first-layer access policies the noisy and merged access policy.

METHODOLOGY

- At the beginning, the data owner conducts the first-layer encryption on each data attribute in the EHR with the attribute-based encryption algorithms.
- Then, to prevent the attacker from knowing the access policies used in the first-layer encryption, the data owner conceals this access policy, and conducts the second-layer encryption.
- After that, the data owner out sources the encrypted HER data, the encrypted first-layer access policy, and the second-layer access policy to the cloud.

3. SYSTEMREQUIREMENTS

SOFTWAREREQUIREMENTS

- Operating system : Windows7.
- Coding Language : JAVA
- Tool : APACHETOMCAT
- Backend (Database): MYSQL

HARDWAREREQUIREMENTS

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

4. SOFTWAREENVIRONMENT

JAVATECHNOLOGY

- **The Java Programming Language**

The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object-oriented
- Portable
- Distributed
- High-performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual link that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called Java byte codes, the platform- independent codes interpreted byte interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works.

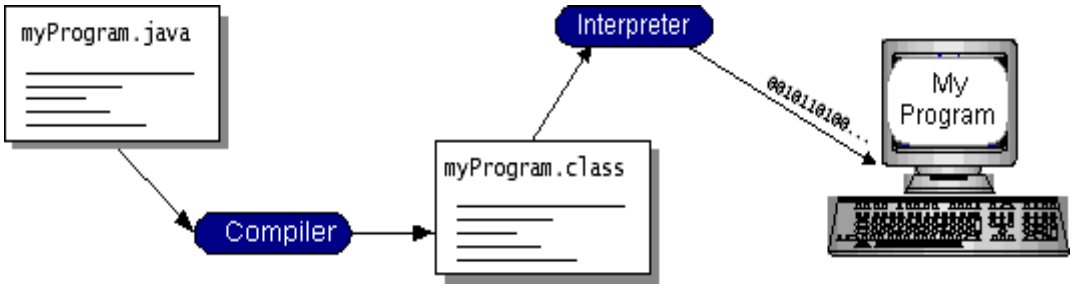


Fig.4: Interpretation

You can think of Java byte codes as the machine code instructions for the Java Virtual Machine (JavaVM). Every Java interpreter, whether it's a development to olora Web browser.

That can run applets, is an implementation of the Java VM. Java byte codes help make "write once, run anywhere" possible. You can compiley our program into by the codes on any plat form that has a Java compiler. The byte codes can then be run on any implementation of the JavaVM. That means that as long as a computer has a Java VM, the same program written in Windows2000.

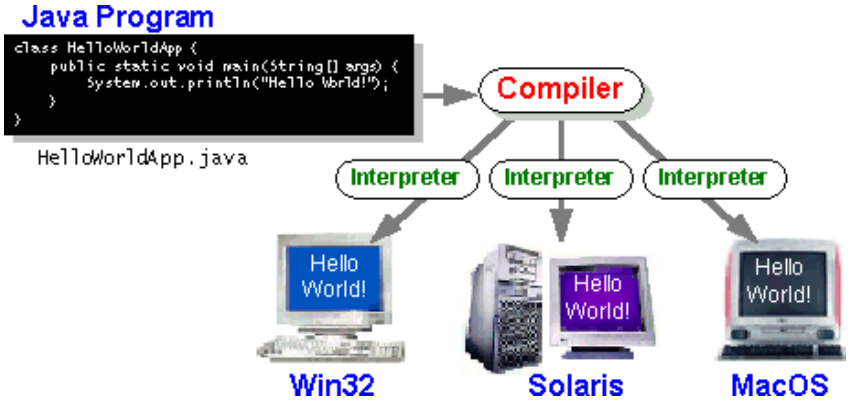


Fig.1: Compiler

- The Java Virtual Machine (Java VM)
- The Java Application Programming Interface (Java API)

The following figure depicts a program that's running on the Java platform. As the figure shows, the Java API and the virtual machine insulate the program from the hardware.

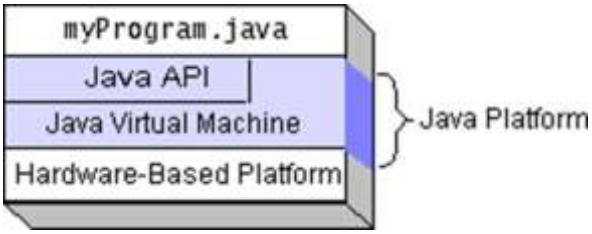


Fig.2: Java Platform

- **What Can Java Technology Do?**

- **The essentials**: Objects, strings, threads, numbers, input and output, data structures, system properties, date and time, and soon.
- **Applets**: The set of conventions used by applets.
- **Networking**: URLs, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) sockets, and IP (Internet Protocol) addresses.
- **Internationalization**: Help for writing programs that can be localized for users worldwide. Programs can automatically adapt to specific locales and be displayed in the appropriate language.
- **Security**: Both low level and high level, including electronic signatures, public and private key management, access control, and certificates.
- **Software components**: Known as Java Beans , can plug into existing component architectures.

- **How Will Java Technology Change My Life?**

- **Get started quickly**: Although the Java programming language is a powerful object-oriented language, it's easy to learn, especially for programmers already familiar with Core C++.
- **Write less code**: Comparisons of program metrics (class counts, method counts, and so on) suggest that a program written in the Java programming language can be four times smaller than the same program in C++.
- **Write better code**: practices and its garbage collection help you avoid memory leaks. Its object orientation, its JavaBeans component architecture, and its wide-ranging, easily extendible API let you reuse other people's tested code and introduce fewer bugs.
- **Avoid platform dependencies with100% Pure Java**: You can keep your program portable by avoiding the use of libraries written in other languages...
- **Distribute software more easily**: You can upgrade applets easily from central server. Applets take advantage of the feature of allowing new classes to be loaded "on the fly," without recompiling the entire program.

- **ODBC**

Microsoft Open Database Connectivity (ODBC) is a standard programming interface for application developers and database systems providers. Before ODBC became a *de fact* standard for Windows programs to interface with database systems, programmers had to use proprietary languages for each database they wanted to connect to.

Through the ODBC Administrator in Control Panel, you can specify the particular database that is associated with a data source that an ODBC application program is written tousle. Think of an ODBC data source as a door with a name on it. Each door will lead you to particular database. For example, the data source named Sales Figures might be a SQL Server database, whereas the Accounts Payable data source could refer to an Access database.

- **JDBC**

In an effort to set an independent database standard API for Java; Sun Microsystems developed Java Database Connectivity, or JDBC. JDBC offers a generic SQL database access mechanism that provides a consistent interface to a variety of RDBMSs.

The remainder of this section will cover enough information about JDBC for you to know what it is about and how to use it effectively. This is by no means a complete overview of JDBC. That would fill an entire book.

- **JDBC Goals**

Few software packages are designed without goals in mind. JDBC is one that, because fits many goals, drove the development of the API.

These goals, in conjunction with early reviewer feedback, have finalized the JDBC class library into a solid framework for building database applications in Java. The goals that were set for JDBC are important. They will give you some insight as to why certain classes and functionalities behave the way they do.

NETWORKING

- **TCP/IP stack**

The TCP/IP stack is shorter than the OSI one:

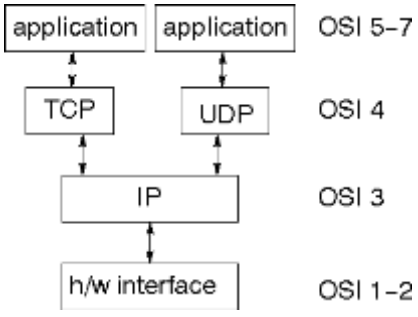


Fig:9TCP/IP Stack

TCP is a connection-oriented protocol; UDP (User Datagram Protocol) is a connection less protocol.

- **Network address**

Class A uses 8 bits for the network address with 24 bits left over for to hear dressing. Class B uses 16 bit network addressing. Class C uses 24 bit network addressing and class D uses all 32.

- **Time Series Chart Interactivity**

Implement a new (to J Free Chart) feature for interactive time series charts --- to display a separate control that shows a small version of ALL the time series data, with a sliding "view" rectangle that allows you to select the subset of the time series data to display in the main chart.

- **Dashboards**

There is currently a lot of interest in dashboard displays. Create a flexible dash board mechanism that supports a subset of JFree Chart types (dials, pies, thermometers, bars, and lines/time series) that can be delivered easily via both Java Web Start and an applet.

- **What is Java EE?**

Java EE (Enterprise Edition) is a widely used platform containing a set of coordinated technologies that significantly reduce the cost and complexity of developing, deploying, and managing multi-tier, server-centric applications. Java Eebuilds upon the Java SE platform and provides a set of APIs (application programming interfaces) for developing and running portable, robust, scalable, reliable and secure server-side applications.

Some of the fundamental components of Java EE include:

- **Java Persistence API (JPA)** : a frame work that allows developers to manage data using object- relational mapping (ORM)in applications built on the Java Platform.
- **Communication Support** – Container provides easy way of communication between web server and the servlets and JSPs. Because of container, we don't need to build a server socket to listen for any request from web server, parse the request and generate response. All these important and complex tasks are done by container and all wended to focus is on our business logic for our applications.
- **Multithreading Support** – Container creates new thread for every request to the servlet and when it's processed the thread dies. So servlet are not initialized for each request and saves time and memory.

- **My SQL databases are relational.**

A relational database stores data in separate tables rather than putting all the data in one big storeroom. The database structures are organized into physical files optimized for speed. The logical model, with objects such as databases, tables, views, rows, and columns, offers a flexible programming environment.

SQL is defined by the ANSI/ISO SQL Standard. The SQL standard has been evolving since 1986 and several versions exist. In this manual, "SQL-92" refers to the standard released in 1992, "SQL:1999" refers to the standard released in 1999, and"SQL:2003" refers to the current version of the standard. We use the phrase "the SQL standard" to mean the current version of the SQL Standard at any time.

- **MySQL software is Open Source.**

Open Source means that it is possible for anyone to use and modify the software. Anybody can download the MySQL software from the Internet and use it without paying anything. If you wish, you may study the source code and change it to suit your needs. The MySQL software uses the GPL (GNU General Public License), http://www.fsf.org/licenses/, to define what you may and may not do with the software in different situations.

See the MySQL Licensing Overview for more information (http://www.mysql.com/company/legal/licensing/).

- **The MySQL Database Server is very fast, reliable, scalable, and easy to use.**

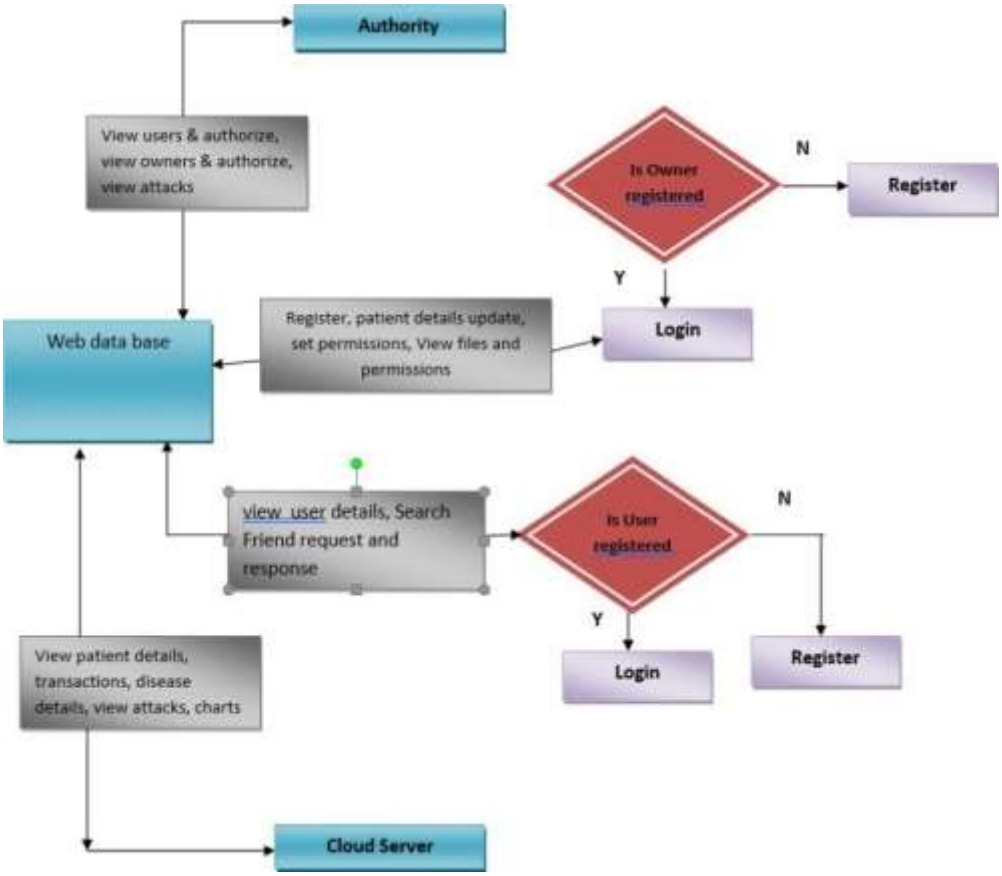
If that is what you are looking for, you should give it a try. MySQL Server can run comfortably on a desktop or laptop, alongside your other applications, web servers, and so on, requiring littler no attention.

If you dedicate an entire machine to MySQL, you can adjust the settings to take advantage of all the memory, CPU power, and I/O capacity available. MySQL canals scale up to networked together.

You can find a performance comparison of MySQL Server with managers on our benchmark page. MySQL Server was originally developed to handle large databases much faster than existing solutions

Although under constant development, MySQL Server today offers a rich and useful set of functions. Its connectivity, speed, and security make MySQL Server highly suited for accessing databases on the Internet.

5. DESGIN



ARCHITECTURE

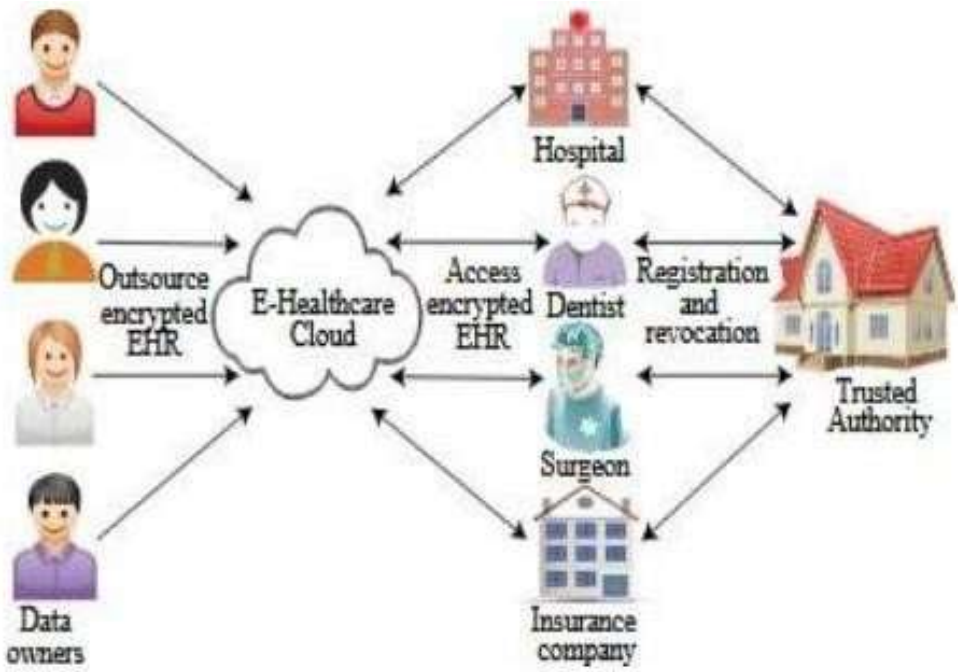
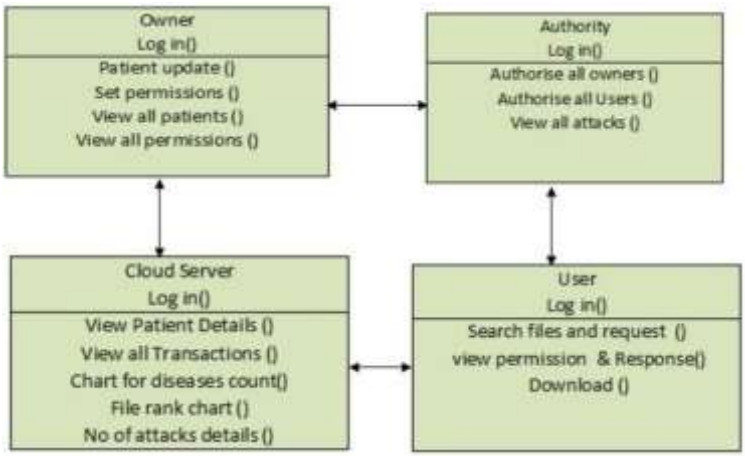


Fig: 11Architecture



UMLDIAGRAM

Flowchart

A flowchart is a diagram that shows an overview of a program. Flowcharts normally use standard symbols to represent the different types of instructions.

Sequence Diagram

Sequence Diagrams are interaction diagrams that detail how operations are carried out. They capture the interaction between objects in the context to collaboration. Sequence Diagrams are time focus and they show the order of the inter action visually by using the vertical axis of the diagram to represent time what messages are sent and when.

Class Diagram

In software engineering, a class diagram in the Unified Modelling Language(UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects

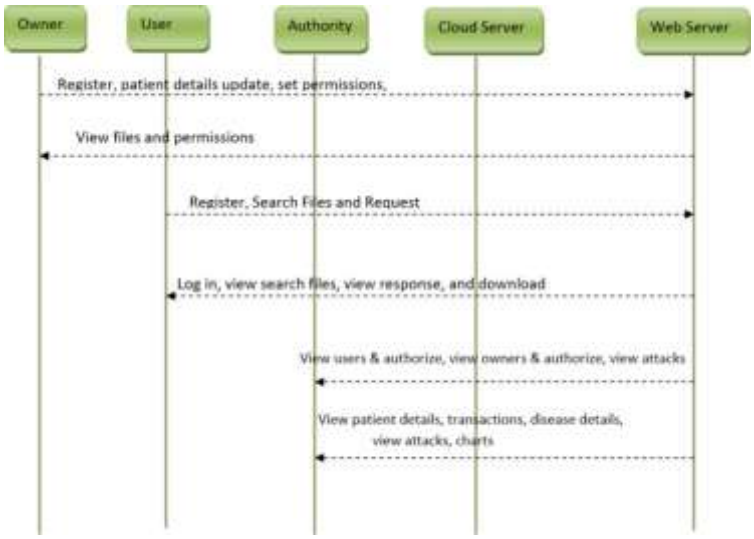


Fig: 14 Class Diagram

Dataflow Diagram

A data-flow diagram is a way of representing a flow of data through a process or system. The DFD also provides information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow — there are no decision rules and no loops.

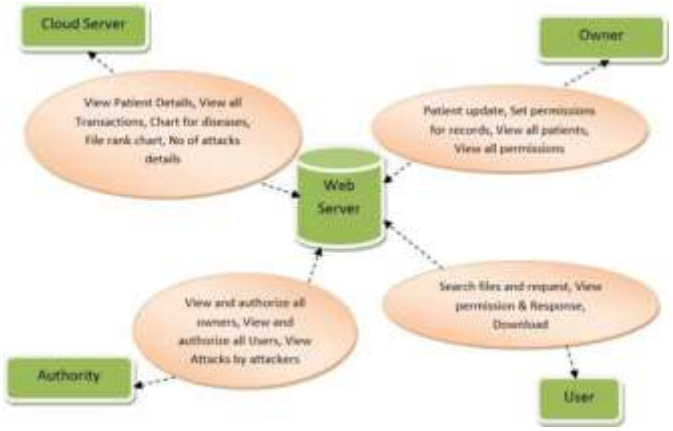


Fig: 15 Data Flow Diagram

6. IMPLEMENTATION

❖ SYSTEMARCHITECTURE

In proposed system four entities are involved, as shown in Fig. 2: they are the trusted authority, the data owners, the users, and the cloud.

❖ TRUSTEDAUTHORITY

The trusted authority is responsible for user registration and revocation. The trusted authority (TA) is responsible for distributing keys and parameters. TA is also responsible for distributing public parameters for the system data owners are those who will outsource their EHR data to the cloud.To guarantee a fine- grained access control(Data owners should specify the access policy for each data attribute in the EHR, so that the data user can only access and decrypt his authorized data attribute.) while preserving data privacy, the data owners encrypt their EHR data before outsourcing. The fundamental reason is that, once the sensitive EHR data are outsourced to the cloud, data owners would lose their control.

❖ CLOUD

To improve the efficiency of the whole system, the cloud is expected to execute computationally intensive works on behalf of the data users. The cloud is not trusted; we treat it as 'curious but honest'. the cloud can deduce sensitive data from the EHR with some background information.

❖ METHODOLOGY

At the beginning, the data owner conducts the first-layer encryption on each data attribute in the EHR

with the attribute-based encryption algorithms. Then, to prevent the attacker from knowing the access policies used in the first-layer encryption, the data owner conceals this access policy, and conducts the second-layer encryption. After that, the data owner outsources the encrypted EHR data, the encrypted first-layer access policy, and this condo-layer access policy to the cloud.

OUTPUTSCREENS

❖ Welcome Screen

Screen1: Welcome screen

❖ **Main Homepage**

7. SYSTEMTESTING

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 anun acceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TESTINGMETHODOLOGIES

The following are the Testing Methodologies:

- **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 asquint. 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 paths are tested for the expected results. All error handling paths are also tested.

❖ **Integration Testing**

Integration testing addresses the issues associated with the dual problem soft 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 program structure that has been dictated by design.

- **Top Down Integration**

This method is an incremental approach to the construction of program structure. Modules are integrated by moving downward through the control hierarchy, beginning with the main program module. The module subordinate stop the main program module are incorporated into the structure in either a depth first or breadth first manner.

In this method, the software is tested from main module and individual stubs are replaced when the test proceeds downwards.

8. CONCLUSION

Out of the blue, we structure adduction assaults fee-social insurance cloud framework with fine-grained get to control. We initially propose a two-layer encryption conspire. In the principal layer encryption, we propose to characterize a specific access arrangement for every datum characteristic in the EHR, create a mystery share for each particular job quality, and reproduce the key to encode every datum trait, which guarantees affine-grained get to control, spares much encryption time, and disguises the recurrence of job properties happen ring in the EHR.

In the second layer encryption, we propose to protect the security of job properties and access arrangements utilized in the principal layer encryption. Furthermore, to exploit the cloud server, we propose to give the cloud a chance to execute computationally escalated takes shoat benefit of the information client without knowing any touchy data.

In the principal layer encryption, we propose to characterize a specific access arrangement forever datum characteristic in the EHR, create a mystery share for each particular job quality, and reproduce the key to encode every datum trait, which guarantees a fine-grained get to control, spares much encryption time, and disguises the recurrence of job properties happening in the EHR

9. REFERENCES

[1]. Google fit. [Online]. Available: https://developers.google.com/fit

[2]. Healthkit. [Online]. Available: https://developer.apple.com/healthkit

[3]. Ibm Watson health cloud [Online].Available :http://www.ibm.com/smarterplanet/us/en/ibmwatson/health

[4]. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J.Hu,"Dynamicaudit services for out sourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 2,pp. 227–238, 2013.

[5]. H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based publicauditing for securec loud storage," IEEE Transactions on Services Computing, pp.1–10, 2015.

[6]. W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, "Secure distributed keyword search in multiple clouds," in Proc. IEEE/ACMIWQOS'14. Hongkong: IEEE/ACM, May2014, pp.370–379.

[7]. W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014). Atlanta, USA:IEEE, jun 2014,pp. 276–286.

[8]. D. Nascimentoand M. Correia, "Shuttle: Intrusion recovery for paas," in Proc. IEEED is tribute Computing Systems (ICDCS'15), Ohio, USA, Jun.2015, pp. 10–20.

[9]. At risk of exposure -in the push for electronic medical records, concern is growing about how well privacy can be safeguarded. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[10]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114.

[11]. M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient- centric and fine-grained data access control in multi-owner settings," in Security and Privacy in Communication Networks. Springer, 2010, pp. 89–106.

[12]. J. Sun, X. Zhu, C. Zhang, and Y. Fang, "Hcpp: Cryptography based secure ehr system for patient privacy and emergency health care," in Distributed Computing Systems (ICDCS), 201131stInternational Conference on. IEEE, 2011, pp. 373–382.