International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Enhancing Security of Data Exchange through Block Chain Technology

Pream Kumar[1], Ramesh.V[2]

[1]PG Student, Department Of CSE, Global Institute Of Engineering and Technology, Tamil Nadu, India

[2]Assistant Professor, Department Of CSE, Global Institute Of Engineering and Technology, Tamil Nadu, India

ABSTRACT

Electronic medical records (EMRs) square measure vital, sensitive personal data in aid, and wish to be often shared between peers. Blockchain Technology facilitates a shared, immutable and history of all the transactions creating software of trust,responsibility and transparency. This provides a novel chance to implement a secure and reliable EMR knowledge management and sharing, system victimization. In this paper, we gift our views on block chain primarily based aid knowledge management, specially, for EMR knowledge sharing between aid suppliers and for analysis studies. All World Health Organization work with health data— health information processing and management professionals, doctors, researchers, business directors have responsibility to accept that data. Confidentiality of patient medical records is of utmost importance. Access to patient medical records in hospital software package ought to be with the treating/admitting practician and therefore the team. Victimization digital signatures on Blockchain-based knowledge permits access for multiple folks may regulate the provision and maintain the security of health records.

Keywords: Searchable Encryption, Cloud Security, Privacy Preserving Scheme, Secure Hash Algorithm, Attribute Based Encryption; Anonymity.

I. INTRODUCTION

Electronic restorative statistics (EMRs) are basic but very responsive to innate information for finding and treat human services, which have to be as often as viable disseminated and shared amongst pals, as an example, medicinal services suppliers, insurance agencies, drug stores, analysts, sufferers families, amongst others. This represents a noteworthy take a look at on preserving a patient's medicinal history splendid.. A affected person, experiencing a real sickness, as an instance, malignant increase, or HIV, wishes to preserve up the lengthy history of the remedy procedure and submit-remedy recovery and checking. Approaching a complete history might be crucial for his remedy: as an example, knowing the conveyed radiation quantities or research facility consequences is crucial for proceeding with the treatment. A patient may visit diverse restorative institutions for a meeting, or might be exchanged starting with one clinical medical institution then onto the next. As in step with the legislation, a affected person is given a without delay over his well being records and may set tips and breaking factors on who can take a gander at and get his well-being records. On the off danger that a affected person desires to percentage his medical facts for the examination functions, or exchange them beginning with one clinical health facility then onto the following, he is probably required to sign an assent that determines what sort of statistics may be shared, the facts approximately the beneficiary, and the duration amid which the facts can be gotten to by means of the beneficiary. This might be very hard to facilitate, mainly whilst a patient is transferring to any other metropolis, district, or state and won't recognize in advance of time the parental parent or clinic where he'll get care in a while. Regardless of whether or not the assent is given, the manner closer to replacing the statistics is tedious, especially if sending them through put up. Sending the patients' statistics via e mail over the Internet isn't always taken into consideration in many medical clinics as this will pressure security risk while the patient's medicinal offerings records are in transit. Environments for well-being statistics trade (HIE, as an example, Common Well Health Alliance intend to guarantee that the statistics shape persistent electronic wellness record are effectively, proficiently and precisely shared across the state in US. This suggests as soon as suppliers receives an entrance to the affected person's well-being data it's far tough to make certain that a patient could get autonomous feelings from diverse medicinal offerings suppliers.

1.1 Block chain (BC) Technology

Blockchain is a distributed ledger technology that is managed by different peers on a peer-to-peer network [11,12]. This technology operates without any central administrator or centralized data storage management [13]. Data is widely spread across several nodes and the quality of data is maintained by replication and encryption [14,15]. On 31st October 2008, the concept of blockchain came into existence via a white paper, written by Nakamoto [16]. He came up with the idea of bitcoin transactions on a platform where the online payments could be sent directly from one peer to another peer without going through a financial institution. His main idea was to develop a trustless [17] system that solves the double-spending problem using a peer-to-peer distributed ledger technology through a computational proof of the chronological order of transactions [18]. The term, blockchain refers to a chain of blocks where each block stores a group of information about its past, present and future [19,20]. Each block plays a key role in connecting with the previous block, and with the following block, as soon as it comes into the system to be a part of the chain [21]. The main role of each block is to record, validate and distribute the transactions among other blocks [22]. This means that a block in the chain cannot be removed or altered as this would change every subsequent block [23,24]. The blockchain network is, therefore, a decentralized information system [25,26] that contains information about all past transactions and operates on a pre-selected protocol which defines the direction of performing and validating the transactions, as well as the functioning of the entire network and its members [27]. Moreover, this network is usually referred to as a distributed registry, as data is stored on each node operating in each of the individual networks [28,29]. A transaction group in blockchain networks is combined into blocks of transactions connected in the chain using the hash of the previous block's record [30]. Therefore, as a property of immutability, the basic security feature of blockchain networks is enforced [31]. The further the block is along the chain (the older it is), the more the data included in it is protected from changes [32]. If an attacker tries to change any of the keys, the local register will immediately cease to be valid because the hash values inside the next blocks headers will be completely different depending on the hash function mechanism [33,34].

1.2 A Review on Blockchain Healthcare Applications

Legacy systems typically only share healthcare resources internally in the medical and healthcare field and are not fully compatible with external systems. Nonetheless, evidence indicates numerous benefits from integrating these networks for interconnected and better healthcare, calling for interconnection between different organizations for health informatics researchers [35]. One of the most critical issues is multi-organizational data exchange, which demands that medical dataobtained by a healthcare provider be easily available to other organizations, such as a physician or research institute. In many healthcare implementations, blockchain technology redefines data processing and governance. This is to its adaptability and unprecedented segmentation, secure and sharing of medical data and services. In the healthcare industry, blockchain technology is at the forefront of many current developments.

II. LITERATURE SURVEY

This work is based on providing security and privacy through cryptography based access control to store data in the cloud and encryption through attributes. The generic public key encryption (PKE) based techniques uses high key management mechanism, or require encrypting a file using different users keys of different sets for using fine-grained access control... However, there is a trend push towards patient-driven ability, during which health knowledge exchange is patient-driven. Patient-centered approach introduces new challenges and necessities for technology, privacy, security, incentives, and governance that has got to be taken up in this sort of knowledge sharing to succeed at a large scale. In this work, we look at on applying blockchain technology for facilitating this transition through 5 mechanisms: (1) digital access rules, (2) knowledge aggregation, (3) knowledge liquidity, (4) patient identity, and (5) knowledge immutableness. We have a tendency to verify barriers of blockchain-enabled patient-driven ability, specifically clinical knowledge dealings volume, privacy and security, patient engagement, and incentives. We have a tendency to conclude by noting that whereas patient-driving ability is associate exciting trend in care, given these challenges, it is required to be verified as to how blockchain will facilitate the change from hospital centric to patient-centric information knowledge sharing. [1]

Physicians have a different relationship with the electronic health record (EHR). On the one hand, doctors apprehend they cannot offer the most effective attainable treatment while not them. And on the opposite, today's EHR systems are cumbersome, gawky and slow physicians down. Indeed, there is a lot of to like and far to hate concerning today's EHRs, aboard a spread of the way to handle the issues they produce. One resolution might belong block chain, the technology presently powering the crypto currency Bit coin. [2]

The worth of those medical records is 10 to sixty times larger than a master card range on the black market, because the info on the records is also wont to pull alternative forms of fraud, like filing dishonest tax returns, creating these records a primary target for malicious hackers [3].

On-line form was improved by taking from literature with performance perspective, trust, and risk ideas. The feedback respondents were 149.. Trust issue has impact on acceptance and low risk having positive impact on the Blockchain technology[4].

Electronic medical records (EMRs) are crucial however sensitive non-public data for designation and treatment in aid, that has to be usually distributed and pooled among peers like aid suppliers, insurance firms, pharmacies, researchers, patient’s families’ et al. Storing and sharing knowledge between varied entities, maintaining a right to use management through varied consents solely obscures the method of a patient's treatment. Having access to a patients complete history is also essential for his treatment as an example, knowing the delivered radiation doses or laboratory results is critical for continued the treat is necessary for continuing the treat.[5]

III. SYSTEM STUDY

3.1 FEASIBILITY STUDY

The practical implementation of the project is analyzed during this part and business proposal is place forth with a really general arrange for the project and a few value estimates. This can be to confirm that the projected system isn't a burden to the corporate. For practical analysis, some understanding of the foremost necessities for the system is crucial. Three main considerations involved in the feasibility analysis are

- ❖ ECONOMICAL FEASIBILITY
- ❖ TECHNICAL FEASIBILITY
- ❖ SOCIAL FEASIBILITY

3.2 ECONOMICAL FEASIBILITY

This study is disbursed to examine the economic impact that the system can wear the organization. The number of fund that the corporate will pour into the analysis and development of the system is restricted. The expenditures should be even. Therefore the developed system also at intervals the budget and this was achieved as a result of most of the technologies used area unit freely out there. Solely the custom-built product had to be purchased.

3.3 TECHNICAL FEASIBILITY

This study is allotted to see the technical practicability, that is, the technical needs of the system. Any system developed should not have a high demand on the available technical resources. This may result in high demands on the obtainable technical resources. The developed system should have a modest demand, as solely marginal or null changes square measure needed for implementing this method.

3.4 SOCIAL FEASIBILITY

The facet of study is to observe the extent of system acceptance by the user. This includes the method of training the user to use the system efficiently and effective The extent of acceptance by the users depends on the strategies that are used to train the user regarding the system and create awareness on it. His level of confidence should be raised so that he is ready to take up defects associated with the system,as he's the ultimate user of the system.

3.5 EXISTING SYSTEM

Electronic medical records area unit important however sensitive non-public info for diagnosing and treatment in attention, which require to be oftentimes distributed and shared among peers like attention suppliers, insurance corporations, pharmacies, researchers, patients, their family, among others. Storing and sharing information between entities for maintaining access management through varied consents solely complicate the method of a patient's treatment..

DISADVANTAGES:

- Less efficiency
- Decision creating is a smaller amount

3.6 PROPOSED SYSTEM

A framework for administering and EMR sharing information for cancer patient care. In collaboration with a Hospital, a framework is enforced during a paradigm that ensures privacy, security, availableness, and fine-grained access management over EMR information. The pro-posed work will considerably cut back the turnaround for EMR sharing, improve deciding for treatment, and cut back the value.

ADVANTAGES:

- More efficiency
- Improve deciding
- Less time consuming

IV. SYSTEM REQUIREMENTS

4.1 H/W System Configuration:-

- Processor I3/Intel Processor
- RAM 4GB (min)
- Hard Disk 160GB
- Key Board Standard Windows Keyboard
- Mouse Two or Three Button Mouse
- Monitor SVGA

4.2 S/W System Configuration:-

- Operating System Windows 7/8/10
- Application Server Tomcat 7.0
- Front End HTML, JSP
- Scripts JavaScript.
- Server side Script Java Server Pages.
- Database My SQL 6.0

V. SOFTWARE DESCRIPTION

JAVA TECHNOLOGY

Object Oriented Programming popularly called OOPS is one of the buzzwords in the software industry. Object Oriented Programming is designed around the data being operated upon as opposed to the operations themselves. Instead of making certain types of specific & rigid computer operations these operations are designed to fit to the data.

OOP enables one to remain close to the conceptual, higher level model of real-world problem that he is trying to solve. Besides he can take advantage of the modularity of objects and implement the program in relatively independent units that are easier to maintain and extend. So sharing of code among objects can be made possible through inheritance.

1. Class

Defines the abstract characteristics of a thing (object), including the thing's characteristics (its attributes, fields or properties) and the thing's behaviors (the things it can do, or methods, operations or features). One might say that a class is a blueprint or factory that describes the nature of something.

2. Object

A particular instance of a class. The class of Dog defines all possible dogs by listing the characteristics and behaviors they can have; the object Lassie is one particular dog, with particular versions of the characteristics. A Dog has fur; Lassie has brown-and-white fur. In programmer jargon, the Lassie object is an instance of the Dog class.

Method

An object's abilities. Lassie, being a Dog, has the ability to bark. So bark () is one of Lassie's methods. Object may have other methods as well, for example sit () or eat () or walk ().particular object; all Dogs can bark, but only one particular dog to do the barking.

3. Characteristics of OOPs

The following are the characteristics of OOPS:

- Message passing
- Data abstraction
- Encapsulation
- Inheritance
- Polymorphism
- Dynamic binding

1) Inheritance

When one object acquires all the properties and behaviours of a parent object, it is known as inheritance. It provides code reusability. It is used to achieve runtime polymorphism.

2) Polymorphism

If one task is performed in different ways, it is known as polymorphism. For example: to convince the customer differently, to draw something, for example, shape, triangle, rectangle, etc.

In Java, we use method overloading and method overriding to achieve polymorphism.

Another example can be to speak something; for example, a cat speaks meow, dog barks woof, etc.

3) Abstraction

Hiding internal details and showing functionality is known as abstraction. For example phone call, we don't know the internal processing.

In Java, we use abstract class and interface to achieve abstraction.

4) Encapsulation

Binding (or wrapping) code and data together into a single unit are known as encapsulation. For example, a capsule, it is wrapped with different medicines.

A java class is the example of encapsulation. Java bean is the fully encapsulated class because all the data members are private here.

5) Coupling

Coupling refers to the knowledge or information or dependency of another class. It arises when classes are aware of each other. If a class has the details information of another class, there is strong coupling. In Java, we use private, protected, and public modifiers to display the visibility level of a class, method, and field. Cohesion

Cohesion refers to the level of a component which performs a single well-defined task. A single well-defined task is done by a highly cohesive method. The weakly cohesive method will split the task into separate parts. The java.io package is a highly cohesive package because it has I/O related classes and interface. However, the java.util package is a weakly cohesive package because it has unrelated classes and interfaces.

6) Association

Association represents the relationship between the objects. Here, one object can be associated with one object or many objects. There can be four types of association between the objects:

- One to One
- One to Many
- Many to One, and
- Many to Many

Let's understand the relationship with real-time examples. For example, One country can have one prime minister (one to one), and a prime minister can have many ministers (one to many). Also, many MP's can have one prime minister (many to one), and many ministers can have many departments (many to many). Association can be unidirectional or bidirectional.

7) Aggregation

Aggregation is a way to achieve Association. Aggregation represents the relationship where one object contains other objects as a part of its state. It represents the weak relationship between objects. It is also termed as a has-a relationship in Java. Like, inheritance represents the is-a relationship. It is another way to reuse objects.

8) Composition

The composition is also a way to achieve Association. The composition represents the relationship where one object contains other objects as a part of its state. There is a strong relationship between the containing object and the dependent object. It is the state where containing objects do not have an independent existence. If you delete the parent object, all the child objects will be deleted automatically.

4. Benefits of OOP

OOP offers several benefits to both the program designer and the user. Object Orientation contributes to the solution of many problems associated with the development and quality of software products.

5. Applications of Java Programming

The latest release of the Java Standard Edition is Java SE 8. With the advancement of Java and its widespread popularity, multiple configurations were built to suit various types of platforms. For example: J2EE for Enterprise Applications, J2ME for Mobile Applications.

- ❖ **Multithreaded** – With Java's multithreaded feature it is possible to write programs that can perform many tasks simultaneously. This design feature allows the developers to construct interactive applications that can run smoothly.
- ❖ **Interpreted** – Java byte code is translated on the fly to native machine instructions and is not stored anywhere. The development process is more rapid and analytical since the linking is an incremental and light-weight process.
- ❖ **High Performance** – With the use of Just-In-Time compilers, Java enables high performance.
- ❖ **Distributed** – Java is designed for the distributed environment of the internet.
- ❖ **Dynamic** – Java is considered to be more dynamic than C or C++ since it is designed to adapt to an evolving environment. Java programs can carry extensive amount of run-time information that can be used to verify and resolve accesses to objects on run-time.

JAVA PROGRAMMING LANGUAGE

Java is a fully Object Oriented Programming Language. Java supports all the features of the OOPS. Java can be used to create 2 types of programs: 1. Application and 2. Applet. An application is a program that runs on your computer, under the operating system of that computer. That is, an application created by java is more or less like one created using C or C++. When used to create application, java is not much different from any other computer language. Rather, it is java's ability to create applets that makes it important.

JAVA SWING

Swing was developed to provide a more sophisticated set of GUI components than the earlier Abstract Window Toolkit (AWT). Swing provides a native look and feel that emulates the look and feel of several platforms, and also supports a pluggable look and feel that allows applications to have a look and feel unrelated to the underlying platform.

VI. MICROSOFT SQL SERVER 2005

Microsoft SQL Server 2005 is a full-featured relational database management system (RDBMS) that offers a variety of administrative tools to ease the burdens of database development, maintenance and administration.

A. SQL

- SQL stands for Structured Query Language
- SQL allows you to access a database
- SQL is an ANSI standard computer language
- SQL can execute queries against a database
- SQL can retrieve data from a database
- SQL can insert new records in a database
- SQL can delete records from a database
- SQL can update records in a database
- SQL is easy to learn

There are five more frequently used tools in SQL2005. They are as follows:

1. Enterprise Manager is the main administrative console for SQL Server installations. It provides you with a graphical "birds-eye" view of all of the SQL Server installations on your network.
2. Query Analyzer offers a quick and dirty method for performing queries against any of your SQL Server databases.

3. SQL Profiler provides a window into the inner workings of your Database.
4. Service Manager is used to control the MS SQL Server (the main SQL Server process), MSDTC (Microsoft Distributed Transaction Coordinator) and SQL Server Agent processes.
5. Data Transformation Services (DTS) provide an extremely flexible method for importing and exporting data between a Microsoft SQL Server installation and a large variety of other formats.

JSP

Java Server Pages (JSP) is a server-side programming technology that enables the creation of dynamic, platform-independent method for building Web-based applications. JSP have access to the entire family of Java APIs, including the JDBC API to access enterprise databases.

A Java Server Pages component is a type of Java servlet that is designed to fulfill the role of a user interface for a Java web application. Web developers write JSPs as text files that combine HTML or XHTML code, XML elements, and embedded JSP actions and commands.

JSP tags can be used for a variety of purposes, such as retrieving information from a database or registering user preferences, accessing JavaBeans components, passing control between pages, and sharing information between requests, pages etc.

Why Use JSP?

JavaServer Pages often serve the same purpose as programs implemented using the Common Gateway Interface (CGI). But JSP offers several advantages in comparison with the CGI.

- Performance is significantly better because JSP allows embedding Dynamic Elements in HTML Pages itself instead of having separate CGI files.
- JSP are always compiled before they are processed by the server unlike CGI/Perl which requires the server to load an interpreter and the target script each time the page is requested.
- JavaServer Pages are built on top of the Java Servlets API, so like Servlets, JSP also has access to all the powerful Enterprise Java APIs, including JDBC, JNDI, EJB, JAXP, etc.
- JSP pages can be used in combination with servlets that handle the business logic, the model supported by Java servlet template engines.

Finally, JSP is an integral part of Java EE, a complete platform for enterprise class applications. This means that JSP can play a part in the simplest applications to the most complex and demanding.

Advantages of JSP

Following table lists out the other advantages of using JSP over other technologies –

1) vs. Active Server Pages (ASP)

The advantages of JSP are twofold. First, the dynamic part is written in Java, not Visual Basic or other MS specific language, so it is more powerful and easier to use. Second, it is portable to other operating systems and non-Microsoft Web servers.

2) vs. Pure Servlets

It is more convenient to write (and to modify!) regular HTML than to have plenty of println statements that generate the HTML.

3) vs. Server-Side Includes (SSI)

SSI is really only intended for simple inclusions, not for "real" programs that use form data, make database connections, and the like.

4) vs. JavaScript

JavaScript can generate HTML dynamically on the client but can hardly interact with the web server to perform complex tasks like database access and image processing etc.

5) vs. Static HTML

Regular HTML, of course, cannot contain dynamic information

MYSQL

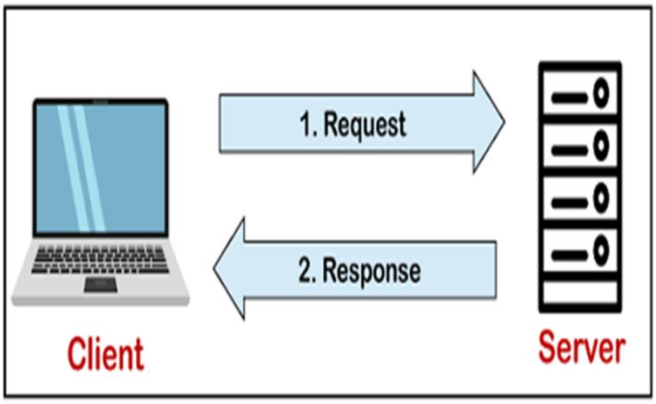
MySQL is currently the most popular database management system software used for managing the relational database. It is open-source database software, which is supported by Oracle Company. It is fast, scalable, and easy to use database management system in comparison with Microsoft SQL Server and Oracle Database. It is developed, marketed, and supported by MySQL AB, a Swedish company, and written in C programming language and C++ programming language. The official pronunciation of MySQL is not the My Sequel; it is My Ess Que Ell. However, you can pronounce it in your way. Many small and big companies use MySQL. MySQL supports many Operating Systems like Windows, Linux, MacOS, etc. with C, C++, and Java languages.

MySQL is a Relational Database Management System (RDBMS) software that provides many things, which are as follows:

- It allows us to implement database operations on tables, rows, columns, and indexes.
- It defines the database relationship in the form of tables (collection of rows and columns), also known as relations.
- It provides the Referential Integrity between rows or columns of various tables.
- It allows us to updates the table indexes automatically.
- It uses many SQL queries and combines useful information from multiple tables for the end-users.

How MySQL Works?

MySQL follows the working of Client-Server Architecture. This model is designed for the end-users called clients to access the resources from a central computer known as a server using network services.



The core of the MySQL database is the MySQL Server. This server is available as a separate program and responsible for handling all the database instructions, statements, or commands. MySQL creates a database that allows you to build many tables to store and manipulate data and defining the relationship between each table.

1. Clients make requests through the GUI screen or command prompt by using specific SQL expressions on MySQL.
2. Finally, the server application will respond with the requested expressions and produce the desired result on the client-side.

VII. SYSTEM DESIGN

INPUT DESIGN

The input coming up with is that the link between the entropy system and therefore the user.It includes the developing stipulation and operation for knowledge preparation and people steps area unit necessary to place dealing knowledge in to a usable kind for process is achieved by inspecting the pc to browse knowledge from a written or written document or it will occur by having mass keying the info directly into the system. The planning of input focuses on controller the number of input needed, dominant the wrongdoing, avoiding delay, avoiding duplicate steps and keeping the method person. The input is meant in such how in order that it provides security and remainder of use with retentive the secrecy. Input Design considered the following things:

- What information ought to run as input?
- However the information need to be organized or coded?
- The dialog to guide the operational personnel in providing input.
- Methods for making ready input validations and steps to follow once error occur.

OUTPUT DESIGN

A quality output is one that is essential to meet the needs of the end user and showcases the knowledge. In a given system results of a process aresent to the users and also toother system through outputs.

1. Planning pc output is for proceeding in a well thought out manner; the correct output should be improved whereas making certain that every output part is meant so the system will use it effectively. Once analysis is done on pc output, they must establish the precise output that's required to satisfy the requirement.
2. Choose ways for representing data.
3. Produce document, report, or alternative formats that contain data created by the system.

The output data system must satisfy one or more of the subsequent objectives.

- Convey past data of activities, current standing or projections of theFuture.
- Warn for Signal vital events, opportunities and problems.
- Trigger Associate in supportive action.
- Confirm Associate in supportive action.

UML DIAGRAMS:

UML represents Unified Modeling Language. UML is an institutionalized universally showing dialect in the subject of program designing. The goal is for UML to become a regular dialect for design of item in PC programming. In its gift frame UML is contained two noteworthy components: a Meta-show and documentation. Later on, a few type of method or system can also likewise be brought to; or related with, UML. The Unified Modeling Language is a popular dialect for indicating, Visualization, Constructing and archiving the curios of programming framework, and for business demonstration and different non-programming frameworks. The UML discusses on accumulation of first-rate building practices which have areuseful in the demonstration of fullsize and complicated frameworks. The UML is a essential piece of creating gadgets located programming and the product development method. The UML makes use of commonly graphical documentations to for programming platforms or systems.

USE CASE DIAGRAM:

A use case diagram (UML) is a behavioral diagram defined and created from a Use-case analysis. Its purpose is to represent a graphical overview of the functionality provided by a system in terms of actors and any dependencies. The main purpose of a use case diagram is to show how system functions are performed for which actor. Roles of the actors in the system can be depicted as below.

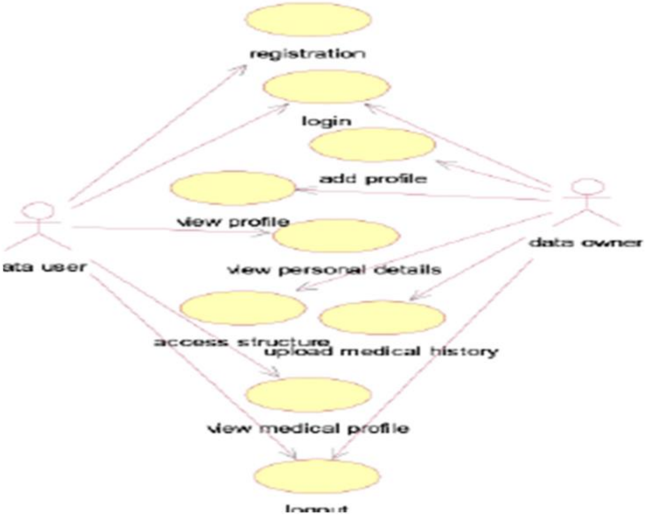


Fig 6.1 use case Diagram

CLASS DIAGRAM:

A class diagram in UML is a static structure diagram for describing the structure of a system. It shows the system's classes, their attributes, methods, and the relationships among them. It explains class information.

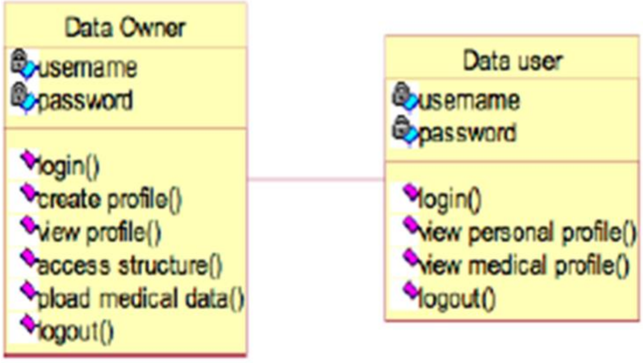


Fig 6.2 Class Diagram

ACTIVITY DIAGRAM:

Activity diagrams are the representations of workflow in form of step-wise activities. In Unified Model-ing Language, the activity diagrams are used to present the business and operating step-wise workflows of individual system component or items in a system. Flow control can be seen in activity diagrams

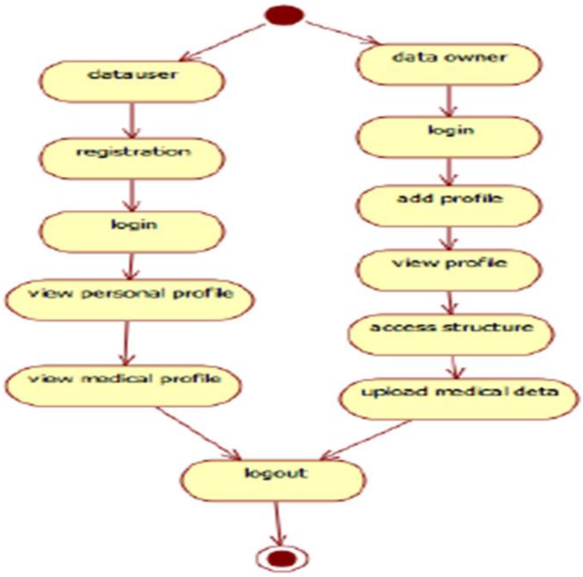


Fig 6.3 Activity Diagram

Architecture Diagram:

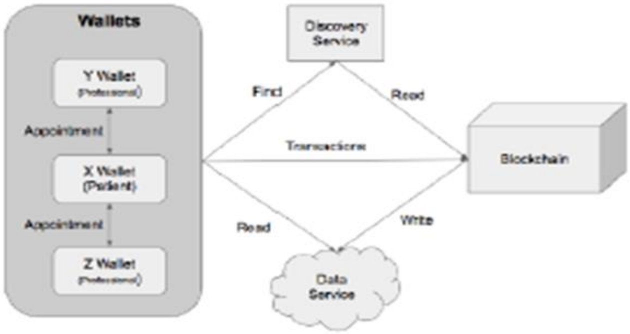


Fig 6.4 Architecture Diagram

Description on components:

Blockchain: A distributed ledger can execute smart contract. They record references for health transactions like examination, appointment and medications. It is described in cryptocurrency system. In block of a privacy layer, it contains a pointer to health information of patient. If a patient X is observed by doctor in a hospital Y, then a transaction is appended to Y as if transaction is accessible to information of X.

Data Service: It can store necessary information about health records. They can be implemented using cloud services like Drobox, Google Drive etc.… Wallets: It has the capability to store user's private and public keys. Email and other credentials are stored with the wallet. It serves as an interface to access the entire system.

Discovery Service: Non-mandatory and other credentials are stored in discovery service. Information stored in Blockchain is indexed using this. This is capable of listing all the services offered to patient X in the listing format. NOSQL can be used for implementing this.

Services offered by ledger includes the following: Storing a transaction, Accessing and processing requests and Registration of all transactions for which access is granted.

Transactions: It is the basic unit of information stored in the system as per the above architecture. The following are the transaction types: A New transaction creates an entry in the ledger. It contains transitive closures, timestamp information of transaction, link, public profile etc…

Request Access is the record entry listing the request to access the content of patient record X and also lists for those who were granted access.

Notification, these are special information stored along with a transaction.

Smart contracts: It is a program stored in the blockchain and run on virtual system. They actually manage transactions.

VIII. SYSTEM MODELS

Blockchain technology is an effective way to provide security to the medical records where it is also known as distributed ledger technology, where it requires no third party to organize, maintain, manage data in the records the implementation is done in the following modules:

1. Building a record structure and how patients and physicians can access the data.
2. Platform Creation
3. Data owner and User module
4. Block chain Security model

Module 1:

Here patients information must be keep secured and how data users can access the data is also important the structure is built how data is inserted and how data is retrieved. Here, the structure is built with two users data owner and data user and how there profile creations and problem description for data owner and tests, results, other information is added and how the data owner can access that information is built.

Module 2 :

Creating Ethereum which is a decentralized platformsoftware platform that has functionality like smart contract and distributed applications to be built without any downtime,error, fraud or third party interference. it possess smart contract functionality, it is a computer code where we can write what kind of operations we want to perform and also errors can be easily identified it can be installed from the official ethereum platform with an windows/mac version and geth is installed which is a multipurpose command line tool which serves as a ethereum full node in blockchain. Ethereum is better than other bock chain platforms

The other modules are yet to be processed and it will be implemented in phase – II of this project.

IX. 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 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.

TYPES OF TESTING

UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produces valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application.

INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

FUNCTIONAL TESTING

Functional testing ensures that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals. Functional testing is centered on the following items:

- Valid Input: identified classes of valid input must be accepted.

- Invalid Input: identified classes of invalid input must be rejected.
- Functions: identified functions must be exercised.
- Output: identified classes of application outputs must be exercised
- Systems / Procedures: interfacing systems or procedures must be invoked. must be considered for testing.

WHITE BOX TESTING

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

BLACK BOX TESTING

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box.

ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

X. CONCLUSION

The number of public and private healthcare service providers has grown significantly in recent times due to the advancement in EHSs. Given their numerous benefits, they also suffer from challenges, such as sharing of information, national-level regulation and oversight, and security and privacy of information. In this paper, we proposed situations of blockchain innovation utility in numerous social insurance settings: critical attention, restorative data inquire about, and associated wellness. We talked about how keeping up a permanent and easy document, which video display units every one of the occasions took place over the device, may want to improve and inspire the administration of restorative records. In view of the compels diagnosed with the social insurance placing, we defended the decision of the permissioned block chain innovation for the use of the proposed situations.

XI. REFERENCES

[1]. Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.

[2]. IEEE 2012 paper on "Improving the interoperability of healthcare information system through HL7 CDA and CCD standards".

[3]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and WJonker, —Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attribute 2009.

[4]. "Privacy-preserving personal health record system using attributebased encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

[5]. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[6]. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving phr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[7]. 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 SecureComm'10, Sept. 2010, pp. 89– 106.

[8]. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in IEEE INFOCOM’10, 2010

[9]. C. Dong, G. Russell, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in Journal of Computer Security, 2010.