Visvesvaraya Technological University

Jnana Sangama, Belagavi - 590018

A Project Work Phase-I (17CSP78)

Report on

"Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy"

Project Report submitted in partial fulfilment of the requirement for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

S.MONIKA	**1KS17CS067**
SUJANA.G.N	**1KS17CS085**
SUPRIYA.K	**1KS17CS087**
VARSHINI.N.PRAKASH	**1KS17CS094**

Under the guidance of

Mr. PRASHANTH.H.S
Assistant Professor
Department of Computer Science & Engineering
K.S.I.T, Bengaluru-560109

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

K. S. Institute of Technology

#14, Raghuvanahalli, Kanakapura Road, Bengaluru - 560109

2020 - 2021

K. S. Institute of Technology

#14, Raghuvanahalli, Kanakapura Road, Bengaluru - 560109

Department of Computer Science & Engineering

CERTIFICATE

Certified that the Project Work Phase-I (17CSP78) entitled **"Blockchain:A Panacea for Healthcare Cloud-Based Data Security and Privacy"** is a bonafide work carried out by:

S.MONIKA	**1KS17CS067**
SUJANA.G.N	**1KS17CS085**
SUPRIYA.K	**1KS17CS087**
VARSHINI.N.PRAKASH	**1KS17CS094**

in partial fulfilment for VII semester B.E., Project Work in the branch of Computer Science and Engineering prescribed by **Visvesvaraya Technological University, Belagavi** during the period of September 2020 to January 2021. It is certified that all the corrections and suggestions indicated for internal assessment have been incorporated. The Project Work Phase-I Report has been approved as it satisfies the academic requirements in report of project work prescribed for the Bachelor of Engineering degree.

……	……..……	……..……
Signature of the Guide	**Signature of the HOD**	**Signature of the Principal & CEO**
[Prashanth.H.S]	[Dr. Rekha B. Venkatapur]	[Dr. K.V.A. Balaji]

DECLARATION

We, the undersigned students of 7th semester, Computer Science & Engineering, KSIT, declare that our Project Work Phase-I entitled "**Blockchain:A Panacea for Healthcare Cloud-Based Data Security and Privacy**", is a bonafide work of ours. Our project is neither a copy nor by means a modification of any other engineering project.

We also declare that this project was not entitled for submission to any other university in the past and shall remain the only submission made and will not be submitted by us to any other university in the future.

Place:
Date:

Name and USN	**Signature**
S.MONIKA (1KS17CS067)	**…….**
SUJANA.G.N (1KS17CS085)	**…….**
SUPRIYA.K (1KS17CS087)	**…….**
VARSHINI.N.PRAKASH(1KS17CS094)	…….

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task will be incomplete without the mention of the individuals, we are greatly indebted to, who through guidance and providing facilities have served as a beacon of light and crowned our efforts with success.

First and foremost, our sincere prayer goes to almighty, whose grace made us realize our objective and conceive this project. We take pleasure in expressing our profound sense of gratitude to our parents for helping us complete our Project Work Phase-I successfully.

We take this opportunity to express our sincere gratitude to our college **K.S. Institute of Technology,** Bengaluru for providing the environment to work on our project.

We would like to express our gratitude to our **MANAGEMENT,** K.S. Institute of Technology, Bengaluru, for providing a very good infrastructure and all the kindness forwarded to us in carrying out this project work in college.

We would like to express our gratitude to **Dr. K.V.A Balaji, Principal & CEO**, K.S. Institute of Technology, Bengaluru, for his valuable guidance.

We like to extend our gratitude to **Dr. Rekha.B.Venkatapur**, **Professor and Head**, Department of Computer Science & Engineering, for providing a very good facilities and all the support forwarded to us in carrying out this Project Work Phase-I successfully.

We also like to thank our Project Coordinators, **Mr. K Venkata Rao, Associate Professor, Mrs. Vaneeta M, Associate Professor, Mr. Raghavendrachar S, Asst. Professor, Mr. Aditya Pai H, Asst. Professor, and Mrs. Sneha K, Asst. Professor, Department of Computer Science & Engineering** for their help and support provided to carry out the Project Work Phase-I successfully.

Also, we are thankful to **Prashanth.H.S, Asst.professor**, for being our Project Guide, under whose able guidance this project work has been carried out Project Work Phase-I successfully.

We are also thankful to the teaching and non-teaching staff of Computer Science & Engineering, KSIT for helping us in completing the Project Work Phase-I work.

S.MONIKA
SUJANA.G.N
SUPRIYA.K
VARSHINI.N.PRAKASH

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The main objective of this project is securely store and maintain the patient records in the healthcare. Healthcare is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily. The blockchain technology is used to protect the healthcare data hosted within the cloud.

The block that contain the medical data and the timestamp. Cloud computing will connect different healthcare providers. It allows healthcare provider to access the patient details more securely from anywhere. It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud. The healthcare provider have to decrypt the data prior to download.

CHAPTER -1

INTRODUCTION

1.1 Overview:

Healthcare is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily.It is clear that technology can play a significant role in enhancing the quality of care for patients (e.g. leveraging data analytics to make informed medical decisions) and potentially reduce costs by more efficiently allocating resources in terms of personnel, equipment, etc.

Generally, Electronic Medical Records (EMRs) contain medical and clinical data related to a given patient and stored by the responsible healthcare provider. This facilitates the retrieval and analysis of healthcare data. To better support the management of EMRs, early generations of Health Information Systems (HIS) are designed with the capability to create new EMR instances, store them, and query and retrieve stored EMRs of interest.2 HIS can be relatively simple solutions, which can be schematically described as a graphical user interface or a web service. These are generally the front-end with a database at the back-end, in a centralized or distributed implementation. With patient mobility (both internally and externally to a given country) being increasingly the norm in today's society, it became evident that multiple stand-alone EMR solutions must be made interoperable to facilitate sharing of healthcare data among different providers, even across national borders, as needed. For example, in medical tourism hubs such as Singapore, the need for real-time healthcare data sharing between different providers and across nations becomes more pronounced.

To facilitate data sharing or even patient data portability, there is a need for EMRs to formalize their data structure and the design of HIS. Electronic Health Records (EHRs), for example, are designed to allow patient medical history to move with the patient or be made available to multiple healthcare providers (e.g. from a rural hospital to a hospital in the capital city of the country, before the patient seeks medical attention at another hospital in a different country).3 EHRs have a richer data structure than EMRs. There have also been initiatives to develop HIS and infrastructures that are able to scale and support future needs, as evidenced by the various national and international initiatives such as the FascicoloSanitarioElettronico (FSE) project in Italy, the epSOS project in Europe, and an ongoing project to standardize sharing of EHRs.

Blockchain was originally designed to record transaction data, which is relatively small in size and linear. Inother words, one only concerns itself about whether the current transaction can be traced backwards to the original "deal".

1.2 Purpose of the project:

1.2.1 Existing system:

Existing system doesn't maintain and process the data securely. It doesn't provides the more accurate search result. Incorrect and misleading of data will produce the wrong analysis result.Low search Efficiency. The search delay of the scheme is proportional to the size of the database. It is not suitable for the large scale databases.

1.2.2 Proposed System:

To overcome the security problems that are occurred in the existing system and effectively store the data over the cloud we introduce this system.

The data user outsources the encrypted documents to the cloud.

The Data user get the each result, the proof and the public verification key, they itself or others can verify the freshness, authenticity, and completeness of the search result even without decrypting them.

1.3 Definitions:

Java:

Java is a programming language originally developed by James Gosling at Sun Microsystems (now a subsidiary of Oracle Corporation) and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to byte code (class file) that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is a general-purpose, concurrent, class-based, object-oriented language that is specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere." Java is currently one of the most popular programming languages in use, particularly for client-server web applications.

Java Platform

One characteristic of Java is portability, which means that computer programs written in the Java language must run similarly on any hardware/operating-system platform. This is achieved by compiling the Java language code to an intermediate representation called Java byte code, instead of directly to platform-specific machine code. Java byte code instructions are analogous to machine code, but are intended to be interpreted by a virtual machine (VM) written specifically for the host hardware.

End-users commonly use a Java Runtime Environment (JRE) installed on their own machine for standalone Java applications, or in a Web browser for Java applets. Standardized libraries provide a generic way to access host-specific features such as graphics, threading, and networking.

A major benefit of using byte code is porting. However, the overhead of interpretation means that interpreted programs almost always run more slowly than programs compiled to native executables would. Just-in-Time compilers were introduced from an early stage that compiles byte codes to machine code during runtime.

Just as application servers such as Glass Fish provide lifecycle services to web applications, the Net Beans runtime container provides them to Swing applications. All new shortcuts should be registered in "Key maps/Net Beans" folder. Shortcuts installed INS Shortcuts folder will be added to all key maps, if there is no conflict. It means that if the same shortcut is mapped to different actions in Shortcut folder and current key map folder (like Key map/Net Beans), the Shortcuts folder mapping will be ignored.

- ✓ Database Explorer Layer API in Database Explorer
- ✓ Loaders-text-dB schema-Actions in Database Explorer
- ✓ Loaders-text-sq.-Actions in Database Explorer
- ✓ Plug-in Registration in Java EE Server Registry

The keyword public denotes that a method can be called from code in other classes, or that a class may be used by classes outside the class hierarchy. The class hierarchy is related to the name of the directory in which the .java file is located.

The keyword static in front of a method indicates a static method, which is associated only with the class and not with any specific instance of that class. Only static methods can be invoked without a reference to an object. Static methods cannot access any class members that are not also static. The keyword void indicates that the main method does not return any value to the caller. If a Java program is to exit with an error code, it must call System. Exit () explicitly.

The method name "main" is not a keyword in the Java language. It is simply the name of the method the Java launcher calls to pass control to the program. Java classes that run in managed environments such as applets and Enterprise JavaBeans do not use or need a main () method. A Java program may contain multiple classes that have main methods, which means that the VM needs to be explicitly told which class to launch from.

The Java launcher launches Java by loading a given class (specified on the command line or as an attribute in a JAR) and starting its public static void main(String[]) method. Stand-alone programs must declare this method explicitly. The String [] rags parameter is an array of String objects containing any arguments passed to the class. The parameters to main are often passed by means of a command line.

Net Beans

The **Net Beans Platform** is a reusable framework for simplifying the development of Java Swing desktop applications. The Net Beans IDE bundle for Java SE contains what is needed to start developing Net Beans plug-in and Net Beans Platform based applications; no additional SDK is required.

Applications can install modules dynamically. Any application can include the Update Center module to allow users of the application to download digitally-signed upgrades and new features directly into the running application.

The platform offers reusable services common to desktop applications, allowing developers to focus on the logic specific to their application. Among the features of the platform are:

- User interface management (e.g. menus and toolbars)
- User settings management
- Storage management (saving and loading any kind of data)
- Window management
- Wizard framework (supports step-by-step dialogs)
- Net Beans Visual Library
- Integrated Development Tools

J2EE

A **Java EE application** or a **Java Platform, Enterprise Edition application** is any deployable unit of Java EE functionality. This can be a single Java EE module or a group of modules packaged into an EAR file along with a Java EE application deployment descriptor.

Enterprise applications can consist of the following:

- EJB modules (packaged in JAR files)
- Web modules (packaged in WAR files)
- connector modules or resource adapters (packaged in RAR files)
- Session Initiation Protocol (SIP) modules (packaged in SAR files)
- application client modules
- Additional JAR files containing dependent classes or other components required by the application

Wamp Server:

WAMPs are packages of independently-created programs installed on computers that use a Microsoft Windows operating system.

Apache is a web server. MySQL is an open-source database. PHP is a scripting language that can manipulate information held in a database and generate web pages dynamically each time content is requested by a browser. Other programs may also be included in a package, such as phpMyAdmin which provides a graphical user interface for the MySQL database manager, or the alternative scripting languages Python or Perl.

MySQL

The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation.

Free-software-open source projects that require a full-featured database management system often use MySQL. Applications which use MySQL databases include: TYPO3, Joomla, WordPress, hob, Drupal and other software built on the LAMP software stack.

CHAPTER-2

LITERATURE SURVEY

2.1 Outsourced symmetric private information retrieval
S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner

Outsourcing is the process of contracting an existing business process which an organization previously performed internally to an independent organization, where the process is purchased as a service. The data owner enables SSE Scheme and outsources a document or collection of files to a remote server in encrypted form. And also the data owner authorizes clients (third parties) to search the database to learn. The remote server still does not learn about the data or queried values as in the basic SSE setting. We extend the OXT protocol of Cash et al. to support arbitrary Boolean queries in all of the above models while withstanding adversarial non-colluding servers (Data owner and remote server) and arbitrarily malicious clients to preserve the remarkable performance of the protocol.

Advantages

- ✓ Implementing digital signatures.
- ✓ Cryptographic protocols with different security and privacy features.
- ✓ Supporting various signature schemes without adding additional hardware complexity compared to a hardware implementation of a conventional signature scheme.

Disadvantages

- ✓ Encryption keys aren't simple strings of text like passwords
- ✓ **Damage** is massive when you lost your symmetric key

2.2 Dynamic search-able symmetric encryption
S. Kamara, C. Papamanthou, and T. Roeder

Searchable symmetric encryption (SSE) allows a client to encrypt data in such a way that it can later generate search tokens to send as queries to a storage serve. We propose the first SSE scheme to satisfy all the properties like sub-linear search time and so-on. Extends the inverted index approach in several non-trivial ways and introduces new techniques for the design of SSE. We implement our schemeand conduct a performance evaluation, showing that our approach ishighlyefficient and ready fordeployment.

Advantages

- ✓ Security against adaptive chosen-keyword attacks.
- ✓ Compact indexes.
- ✓ Ability to add and delete files efficiently.

Disadvantages

- ✓ Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

2.3 Highly-scalable searchable symmetric encryption with support for Boolean queries

D. Cash, S. Jarecki, C. Jutla, H. Krawczyk,

M. Rosu, andM. Steiner

The design, analysis and implementationof the first searchable symmetric encryption (SSE) protocol that supports conjunctive search and general Boolean queries on outsourced symmetrically-encrypted data and that scales to very large databases and arbitrarily-structured data including free text search. Our solution provides a realistic and practical trade-off between performance and privacy by efficiently supporting very large databases at the cost of moderate and well-defined leakage to the outsourced serve.

Advantages

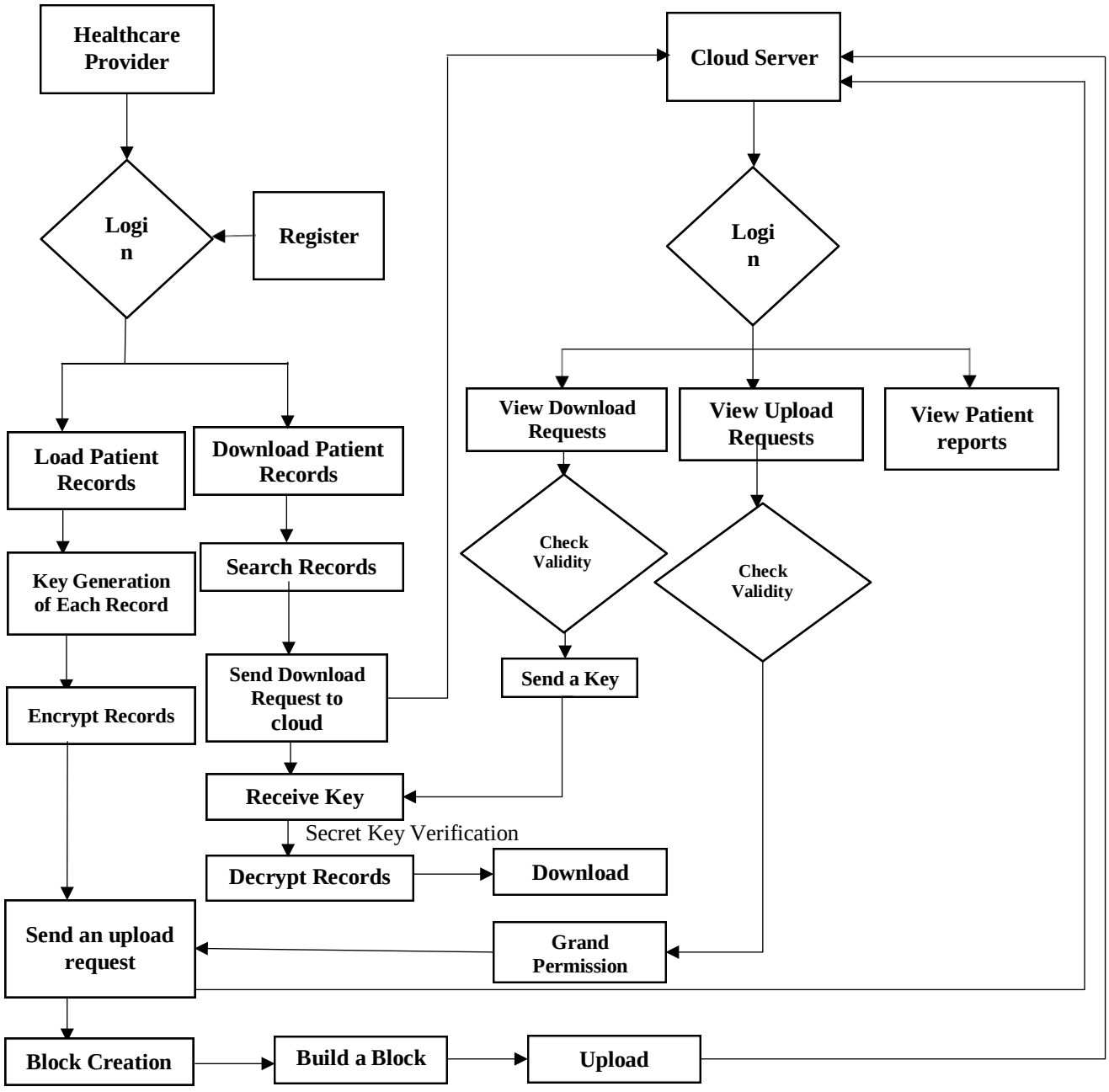
- ✓ Providing performance results of a prototype applied to several large representative data sets, including encrypted search over the whole English Wikipedia.
- ✓ Load Balancing

Disadvantages

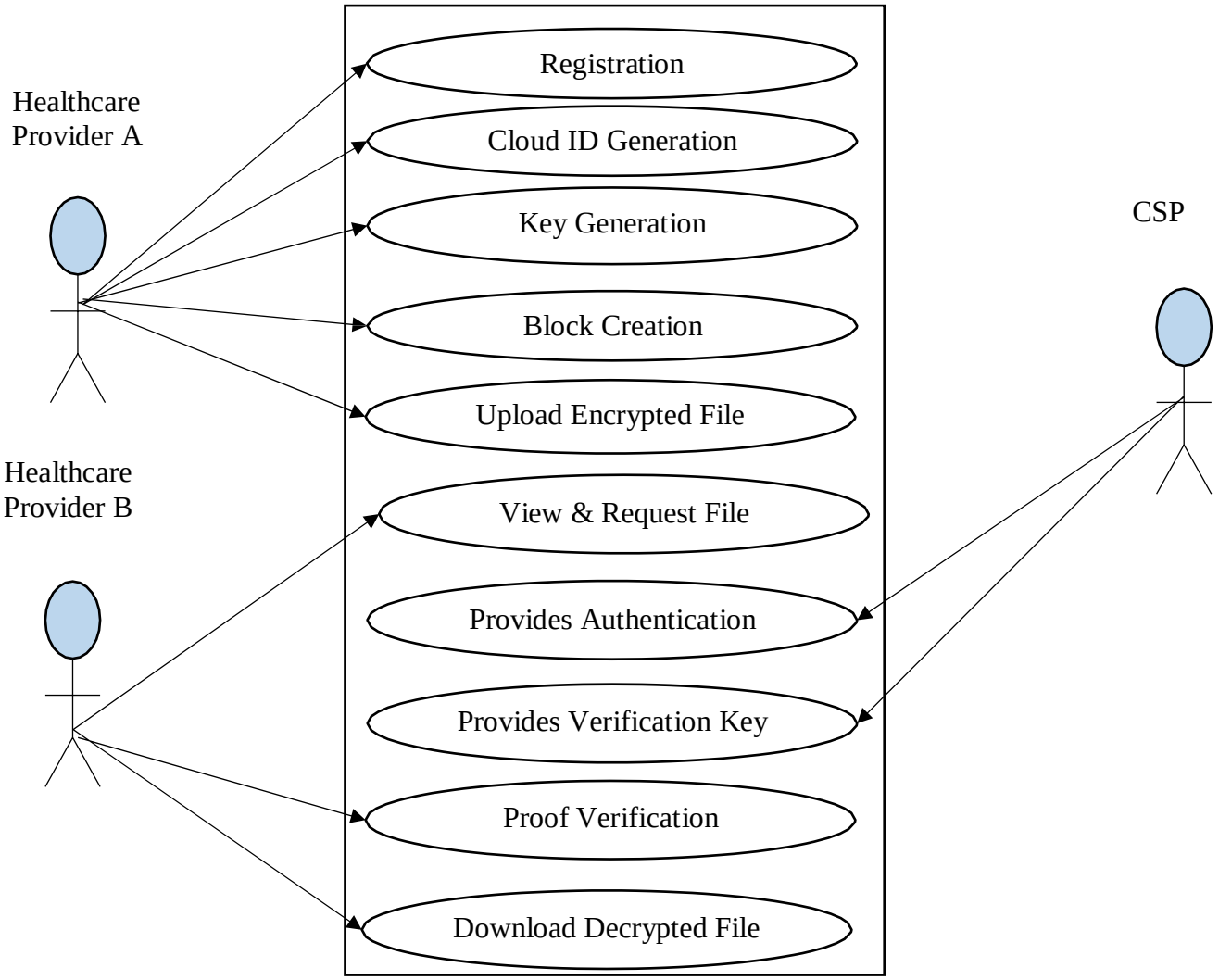
- ✓ Exact matching may retrieve too few or too many documents.

BLOCK DIAGRAM

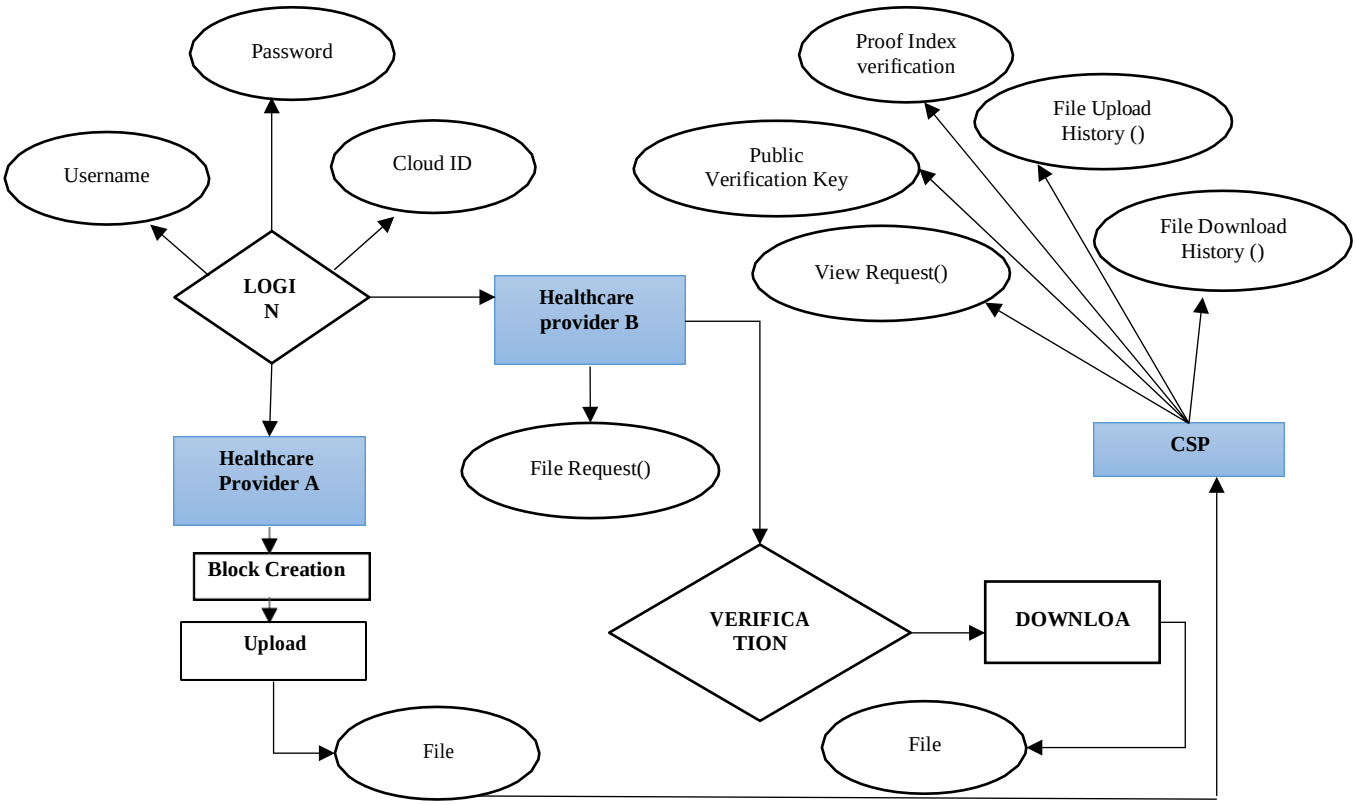
2.2.1FLOW DIAGRAM :



2.2.2 USE CASE DIAGRAM:



2.2.3 ER DIAGRAM:



CHAPTER-3

PROBLEM IDENTIFICATION

3.1 Problem Statement

- In the electronic medical record-based system, security and privacy of patient's data are the primary concern. Patient's data need to be stored in a secure manner such that unauthorized users are not performed malicious activity on it. Existing EMRs system tries to handle, this issue with the use of different cryptographic methodologies. we can solve the above-mentioned problem, with the adoption of blockchain technology in the EMRs system.

- Authentication and key-management are the second type of problem, which exist in the EMRs system. we can adopt a cryptographic mechanism to provide secure and reliable sharing of patient's data.

3.2 Project scope

Healthcare Manager: Supervision is the main task of a healthcare manager. A healthcare manager has to look upon the tasks of maintaining budgets, dealing with the operations of the organization, implementing various policies and communicating with staffs and subordinates.

Healthcare Planner: Healthcare planner optimizes the existing facilities and seeks operational solutions. Making assumptions, trying out new processes and future plans, developing new contracts and maintaining the old ones, dealing with new challenges, all are the part of a healthcare planner’s work profile.

Administrator: Managing hospitals, treatment centers, hospices and support staffs are the major tasks of a healthcare administrator. Efficient operation of the hospital and providing satisfactory service to the patients is the responsibility of an administrator. The administrators are the bridge between the medical staff and the hospital board. Recruitment, hiring and even training new staffs and members of the organization come under the tasks of health care administrator. Activities of all the departments are monitored and integrated by the administrator so that the whole organization works excellently.

CHAPTER-4

GOALS AND OBJECTIVES

4.1 Project Goals

- The main Goal is to ensure the data security
- To achieve forward and backward security of the data with revocation scheme.
- To enable access control that is cryptographically enhanced.
- To ensure the protection of cloud database.
- To perform secure and efficient query processing.

4.2 Project Objectives

- The main objective is to ensure the data security.
- To achieve forward and backward security of the data with revocation scheme.
- To enable access control that is cryptographically enhanced.
- To ensure the protection of cloud database.
- To perform secure and efficient query processing.

CHAPTER-5

SYSTEM REQUIREMENTS

5.1 Software Requirements

- O/S : Windows XP.
- Language : Java.
- IDE : Net Beans 8.2
- Data Base : MySQL

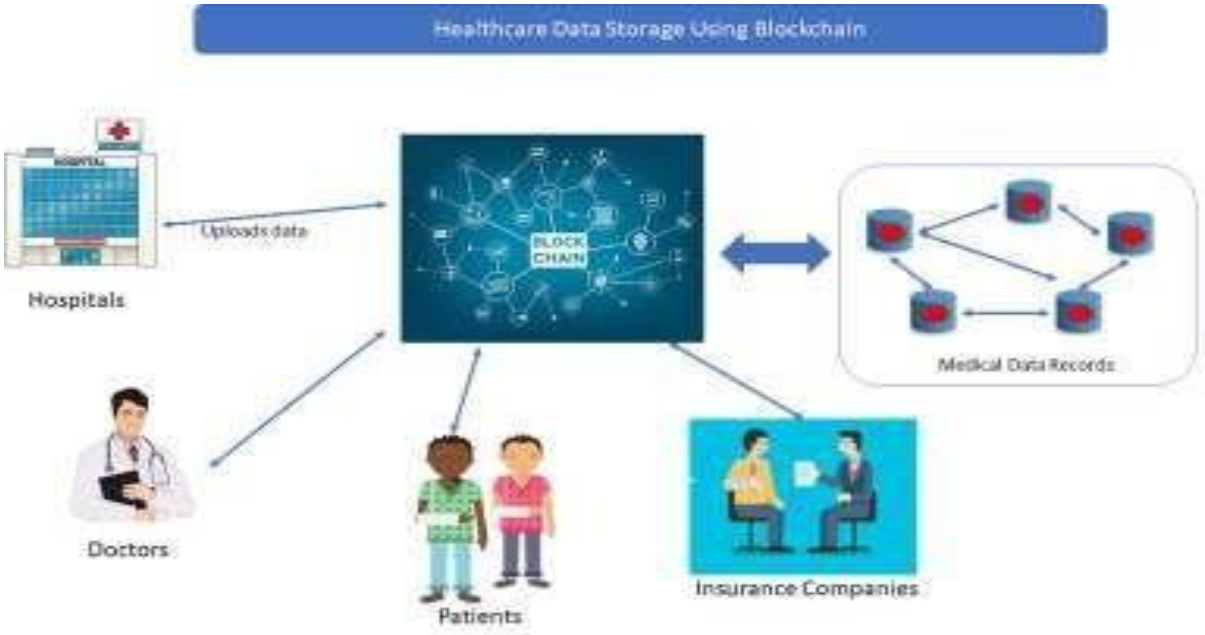
5.2 Hardware Requirements

- System : Pentium IV 2.4 GHz
- Hard Disk : 160 GB
- Monitor : 15 VGA color
- Mouse : Logitech.
- Keyboard : 110 keys enhanced
- Ram : 2GB

CHAPTER-6

METHODOLOGY

- We are developing a system "Healthcare Data Storage Using Blockchain" which provides the top-level security to all healthcare-related data records which remove cost, time, and other resources required for managing all this information. Figure gives the structural design of the proposed system, followed by the system description.



1. **Patient Account:** The user will add their personal information for creating their new account. It also contains their health records and medical history.

2. **Report Submission:** Hospital authority will submit the patient medical report. Submitted report will append with the patient existing history. Submission of one report generates one transaction.

3. **Generate Transaction:** From report submission to the billing process activity generates a number of transactions. All transactions are connected sequentially to each other like linked list.

4. **Block Generation:** A block contains more than 500 transactions on average. In this phase the generated block contains all transaction of the particular user/patients. The newly generated block is added into the existing blockchain. A block is composed of a header and a long list of transactions.
   - **Block Header:** It contains metadata about a block i.e . Previous block hash, mining competition, merkle tree root etc.
   - **Transaction List:** It contains long transaction list.

5. **Transaction Verification:** Insurance Company Officer will act as a validator. After raising insurance claim to the insurance company, the office will validate the patient transaction history.

6. **Final Outcome:** After validating the patient transaction officer will approve or reject the claim. And transfer claim money to the patient account

CHAPTER-8

APPLICATIONS

1. To secure the data of patients.
2. To maintain the standard privacy of patients.
3. Health information Exchange.
4. Medical Imaging.
5. retrieve an information from cloud storage
6. Increase the accuracy of the result.
7. The data's are highly secured.

CHAPTER-8

CONTRIBUTION TO SOCIETY AND ENVIRONMENT

- **Data analytics:** The healthcare industry constantly produces data. Health information systems help gather, compile and analyze health data to help manage population health and reduce healthcare costs. Then the healthcare data analysis can improve patient care.
- **Collaborative care:** Patients often need to treatments from different healthcare providers. Health information systems — such as health information exchanges (HIEs) — allow healthcare facilities to access common health records.
- **Cost control:** Using digital networks to exchange healthcare data creates efficiencies and cost savings. When regional markets use health information exchanges to share data, healthcare providers see reduced costs. On a smaller scale, hospitals aim for the same efficiencies with electronic health records.
- **Population health management:** Health information systems can aggregate patient data, analyze it and identify trends in populations. The technology also works in reverse. Clinical decision support systems can use big data to help diagnose individual patients and treat them.

REFERENCES

- M. Ciampi et al., "A Federated Interoperability Architecture for Health Information Systems," Int'l Journal of Internet Protocol Technology, vol. 7, no. 4, 2013.

- M. Moharra et al., "Implementation of a Cross-Border Health Service: Physician and Pharmacists' Opinions from the epSOS Project," Family Practice, 2015.

- D. He et al., "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms- Matching for Mobile Healthcare Social Network," IEEE Transactions on Dependable and Secure Computing, 2016.

- F.Y. Leu et al., "A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data," Computers and Electrical Engineering, 2017.

- G.S. Poh et al., "Searchable Symmetric Encryption: Designs and Challenges," ACM Computing Surveys, 2017.