A PRELIMINARY PROJECT REPORT ON

Block-chain Security for Cloud

SUBMITTED TO SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE

OF

BACHELOR OF ENGINEERING (COMPUTER ENGINEERING)

SUBMITTED BY

Chitte Priyanka R.	Exam No: B150134227
Bhalerao Pratiksha U.	Exam No: B150134216
Jadhav Manasi R.	Exam No: B150134250
Jadhav Shrijit S.	Exam No: B150134252

DEPARTMENT OF COMPUTER ENGINEERING
K. K. Wagh Institute of Engineering Education & Research

Hirabai Haridas Vidyanagari, Amrutdham, Panchavati, Nashik-422003

SAVITRIBAI PHULE PUNE UNIVERSITY

2018-19

K. K. Wagh Institute Of Engineering Education & Research

CERTIFICATE

This is to certify that the Project Entitled

Block-chain Security for Cloud

Submitted by

Chitte Priyanka R.	Exam No: B150134229
Bhalerao Pratiksha U.	Exam No: B150134216
Jadhav Manasi R.	Exam No: B150134250
Jadhav Shrijit S.	Exam No: B150134252

is a bonafide work carried out by Students under the supervision of Prof. C. R. Patil and it is approved for the partial fulfilment of the requirement of Savitribai Phule Pune University, for the award of Bachelor of Engineering (Computer Engineering).

Prof. C. R. Patil
Internal Guide
Dept. of Computer Engg.

Dr. S. S. Sane
H.O.D
Dept. of Computer Engg.

Dr. K. N. Nandurkar
Principal

Place: Nashik

Date:

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on ***'Blockchain Security for Cloud'****.*

We would like to take this opportunity to thank our internal guide ***Prof. C. R. Patil*** *for giving us all the help and guidance we needed. We are really grateful to her for the kind support. Her valuable suggestions were very helpful.*

We are also grateful to ***Prof. S. S. Sane****, Head of Computer Engineering Department, K.K.W.I.E.E.R. for his indispensable support, suggestions.*

In the end our special thanks to all staff members of computer engineering department for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for our Project.

Chitte Priyanka R.
Bhalerao Pratiksha U.
Jadhav Manasi S.
Jadhav Shrijit S.
(B.E. Computer Engg.)

ABSTRACT

In the internet world demand for data is increasing day by day. This has generated an issue of large data storage. To overcome this, cloud-based storage service was developed. Today there is vast involvement of cloud on business transaction and daily applications. This has raised the need for providing high end of security to the stored data, project helps to overcome this problem. The use of blockchain network as an interface to access the data which helps to overcome the problem of security of data on the cloud. The blockchain is a distributed public ledger and Internet-based computer network. This project works on the ERP data of a company, on a private cloud which is accessible through internet from any place. This system validates and secure the employee data of company. Smart phone and laptop security features like bio-metrics and password validation, can be to make this idea more robust and easier to use for end user. The local validation process of laptop and smart phones, acts as a user interface between the background process and the user. This also act as the next level of security for validation of user details. Thus, providing a more secure way of accessing the cloud service.

INDEX

List of Figures

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

Recent years have witnessed the trend of increasingly relying on distributed infrastructures. This increased the number of reported incidents of security breaches compromising user's privacy, where third parties massively collect, process and manage user's personal data.

The use of blockchain network as an interface to access the data can help to overcome the problem of security of data on the cloud. The blockchain is a distributed public ledger. Every computer on it is called a node and has to record every verified transaction or contract. Since there are many nodes in such a network, and every node has an entire record of all transactions constituting a blockchain, it is not possible to alter data on the network level, as it is required to do so, virtually on all nodes.

Smart phone and laptop security features like bio-metrics and password validation, has helped to make this idea more robust and easier to use for end user. The local validation process of laptop and smart phones, acts as a user interface between the background process and the user. This also act as the next level of security for validation of user details. Thus, providing a more secure way of accessing the cloud service.

1.2 PROBLEM DEFINITION

To provides high end security to the data on the cloud, which is accessible to the user through an easy interface.

1.3 PROJECT SCOPE AND LIMITATION

1.3.1 Project Scope

- The aim of this proposed system is to provide a easier and safer way to access the data on the cloud, than the traditional system.
- Provide high end of security to the stored data.This allows the user to save data on cloud without any worries.
- This will increase the trust of users to put high confidential data on the cloud,thus making the cloud technology safer and cheaper for all types of users.
- System will remove the dependency of access of third party companies to maintain the data on cloud.

1.3.2 Limitation

- This System as of now works only on the Windows OS and Android only.
- System could not work without internet connection, the continuous good speed network is essential.
- System attempts trillions of solutions per second in effort to validate transaction, so accuracy matters.

CHAPTER 2

LITERATURE SURVEY

- Block-chain based data provenance can enable the transparency of data accountability in the cloud, and help to enhance the privacy and availability of the provenance data. System make use of the cloud storage scenario and choose the cloud file as a data unit to detect user operations for collecting provenance data. System design and implement Prov-Chain, an architecture to collect and verify cloud data provenance, by embedding the provenance data into blockchain transactions. Prov-Chain operates mainly in three phases:
  1. provenance data collection.
  2. provenance data storage.
  3. provenance data validation.

- Blockchain may well be viewed as a public ledger and each submitted dealings is place during a list of blocks. This chain develops as new blocks are mounted to that incessantly. With an awfully designed data storage structure, transactions in Bitcoin system might occur with no any third party and therefore the core innovation to construct Bitcoin is blockchain, that was initial planned in 2008 and dead in 2009[11]

- System present eclipse attacks on bit-coins peer-to-peer network. Attack allows an adversary controlling a sufficient number of IP addresses to monopolize all connections to and from a victim bit-coin node. The attacker can then exploit the victim for attacks on bit-coins mining and consensus system, including confirmation double spending, selfish mining, and adversarial forks in the blockchain. System take a detailed look at bit-coins peer-to-peer network, and quantify the resources involved in attack via probabilistic analysis, Monte Carlo simulations, measurements and experiments with live bit-coin nodes[4].

- In standard centralized group action systems, every group action must be valid through the central trustworthy agency (e.g., the central bank), inevitably ensuing to the value and therefore the performance bottlenecks at the central servers. Distinction to the centralized mode, third party is not any longer required in blockchain. Accord algorithms in blockchain are accustomed main-

tain information consistency in distributed network. Bitcoin blockchain stores knowledge regarding user balances supported the unexpended dealings Output (UTXO) model. Any dealings must ask some previous unexpended transactions. Once this dealing is recorded into the blockchain, the state of these referred unexpended transactions switch from unexpended to spent. Therefore, transactions may well be simply verified and tracked.[12]

CHAPTER 3

SOFTWARE REQUIREMENT SPECIFICATION

3.1 INTRODUCTION

The purpose of this project is to provide security to distributed data saved on cloud so it can store high confidential data, using block-chain.

3.1.1 User Classes and Characteristics

The user of this system can be any person who needs to store his data on cloud. This user may vary from common person to business man and from single person to an entire organization.The user can either dump or retrieve data from cloud. To access the cloud user will have to verify himself using the bio-metric validation done on local system. According to user type the access of data will be offered by the system.

3.1.2 Assumptions and Dependencies

- Assumptions
  - The user specifies the user access of the data on the cloud.
  - The data uploaded should not be infected with virus.
- Dependencies
  - Consensus Algorithm.
  - Cloud connectivity.

3.2 FUNCTIONAL REQUIREMENT

- **A local verification system:-**
  A device which will verify that the only authorised user is accessing the data by using two step authentication. This device should be a personal device to the user e.g smartphone.
- **Data for storage:-** A data needs o be stored on to the cloud this data may vary from in size and type. Currently this system works on the ERP database of a company i.e BOM(Bill of Material).

- **Data request(query):-** Some task needs to be performed on the data,this can be done by using a data query. System performs task like data retrieval or uploading or modification depending on user query.

3.3 EXTERNAL INTERFACE REQUIREMENTS

3.3.1 Hardware Interfaces

- System should be compatible across difference platforms.
- System should have a local system to verify the user(bio-metric verification device).
- Cloud storage.

3.3.2 Communication Interfaces

- Minimum wireless or wired connection between the local system(mobile device) and the cloud server.
- Minimum wired connection between the cloud server and the cloud storage.

3.4 NON FUNCTIONAL REQUIREMENTS

3.4.1 Performance Requirements

- Request validation process should be minimum and accurate.
- The connection between the devices should be fast.
- Request should be accurate to locate data fast.

3.4.2 Software Quality Attributes

- System should easily execute on currently available minimum configuration of hardware and software.
- System should work correctly according to the valid input requirements.
- Proposed System should adapt easily to various software data patterns.
- System should integrate according to available local system.

3.5 SYSTEM REQUIREMENTS

3.5.1 Software Requirements

- IDE:Microsoft visual studio 2010.
- OS:Windows XP/2000/Vista/7/8/8.1/10.
- Framework: .Net Framework.
- IDE:Turbo C .

3.5.2 Hardware Requirements

- Local system
  - Bio-metric validation sensors.
  - Any processor(ARM or x86).
  - 256MB of storage.
- Cloud system
  - Linux system server.
  - Processing memory more than 256GB.
  - Large amount storage.

3.6 ANALYSIS MODELS : SDLC MODEL TO BE APPLIED

SDLC - Waterfall Model: In the first phase i.e Requirements Gathering all the requirements such as functional and non-functional requirements were gathered. The most important functional requirement was to study the distributed ledger. The next phase is ”Implementation phase” in which the actual coding is done in order make encryption and decryption algorithm.This phase also include validation coding for local system and data request generation from the local system. Third and the last phase is ”Deployment phase” where the trained model will be used to access data from the cloud.

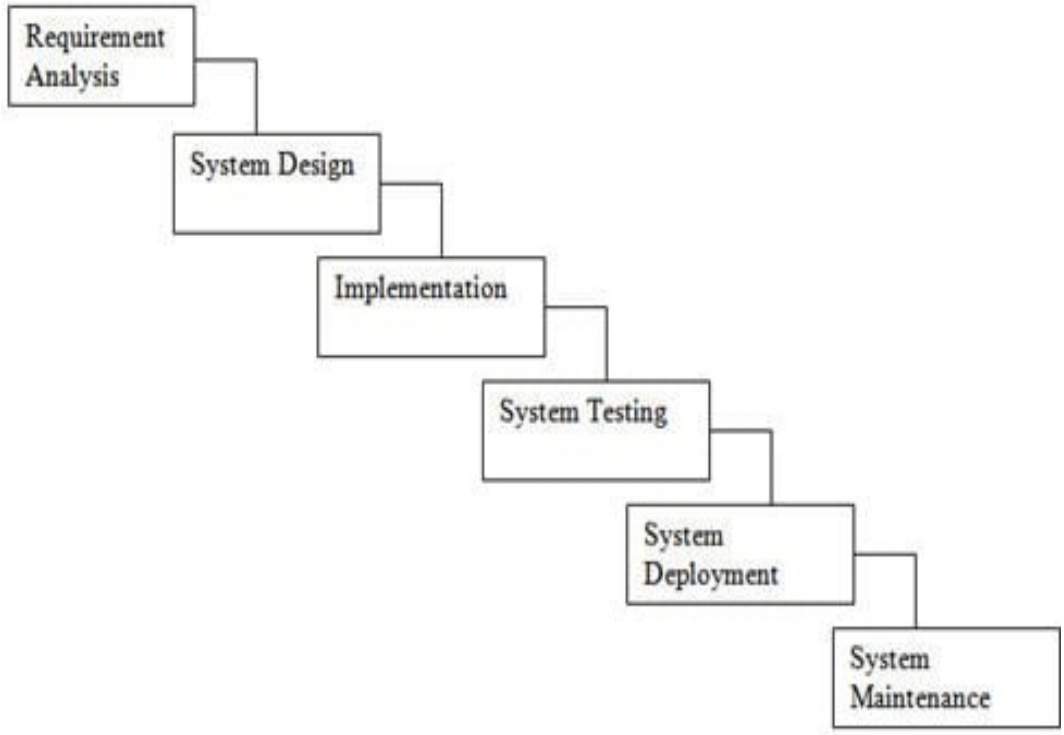

Figure 3.1: Waterfall Model

CHAPTER 4

SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

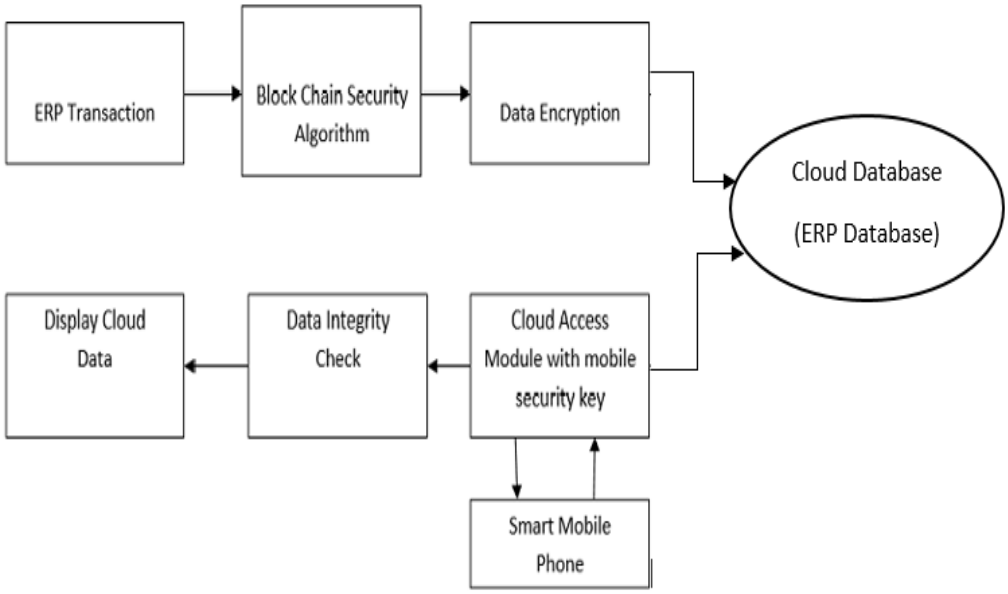

Figure 4.1: System Architecture

The user request is verified and processed by local system.This request is passed to the cloud server which processes the request based on retrieval or upload of data on cloud.In this process the blockchain algorithm either encrypts or decrypts the data based on the request.Further the data integrity is checked by the cloud server.The output of the retrieval request is passed to the local server and displayed to the user.In case of upload, after processing of algorithm, the data appears on cloud.

4.2 DATA FLOW DIAGRAM

4.2.1 DFD-0

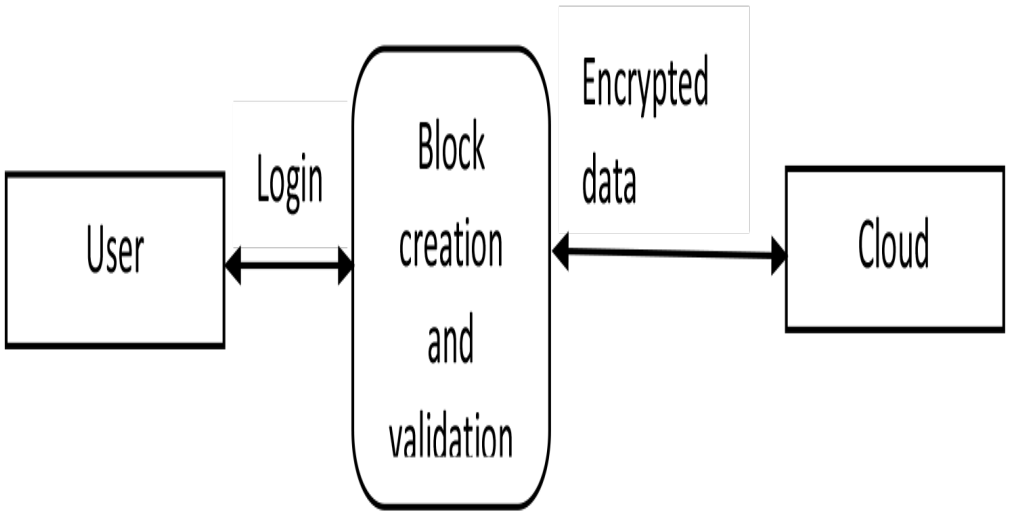

Figure 4.2: DFD0

4.2.2 DFD-1

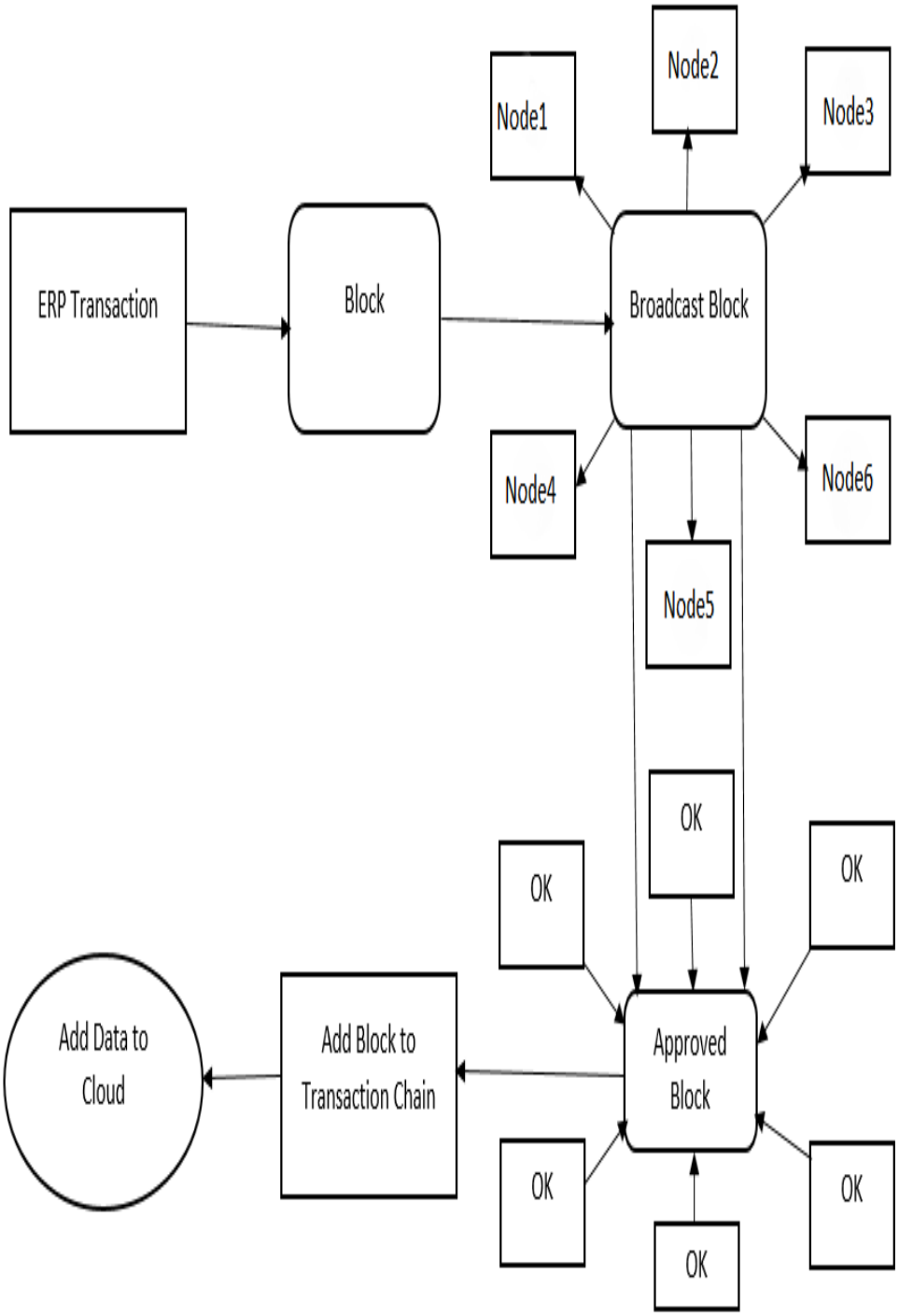

Figure 4.3: DFD1

4.2.3 DFD-2

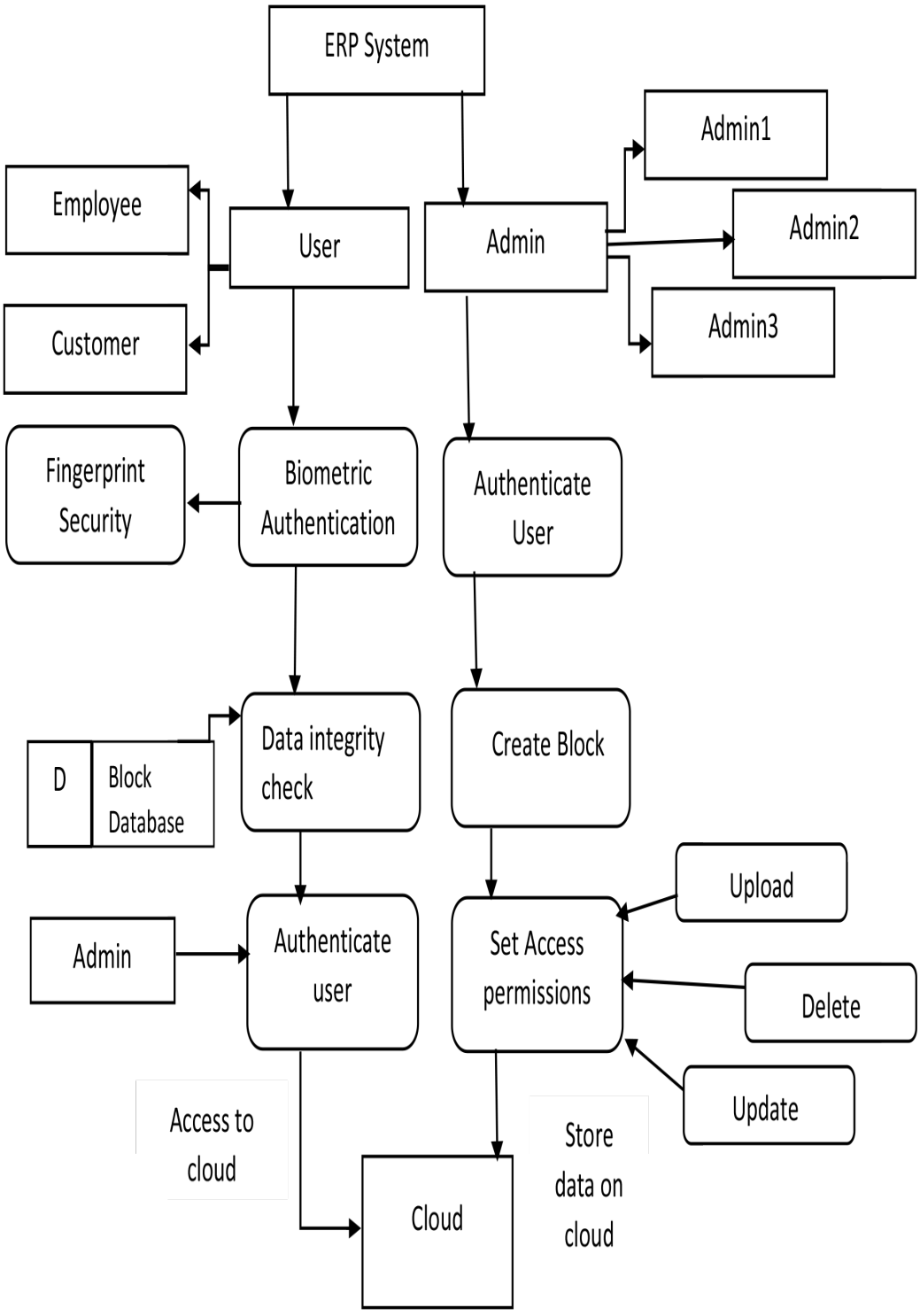

Figure 4.4: DFD2

4.3 UML DIAGRAM

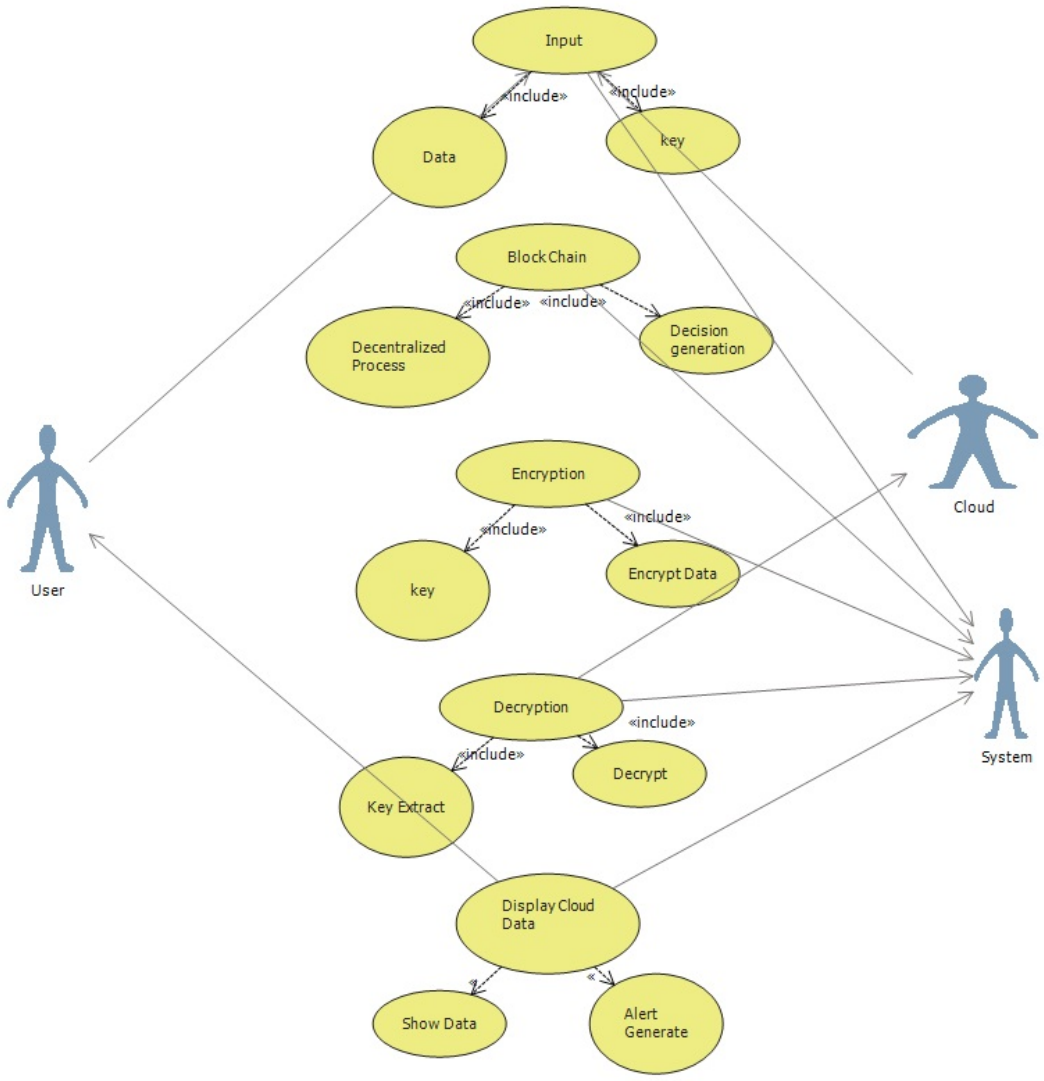

Figure 4.5: UML Diagram

4.4 SEQUENCE DIAGRAM

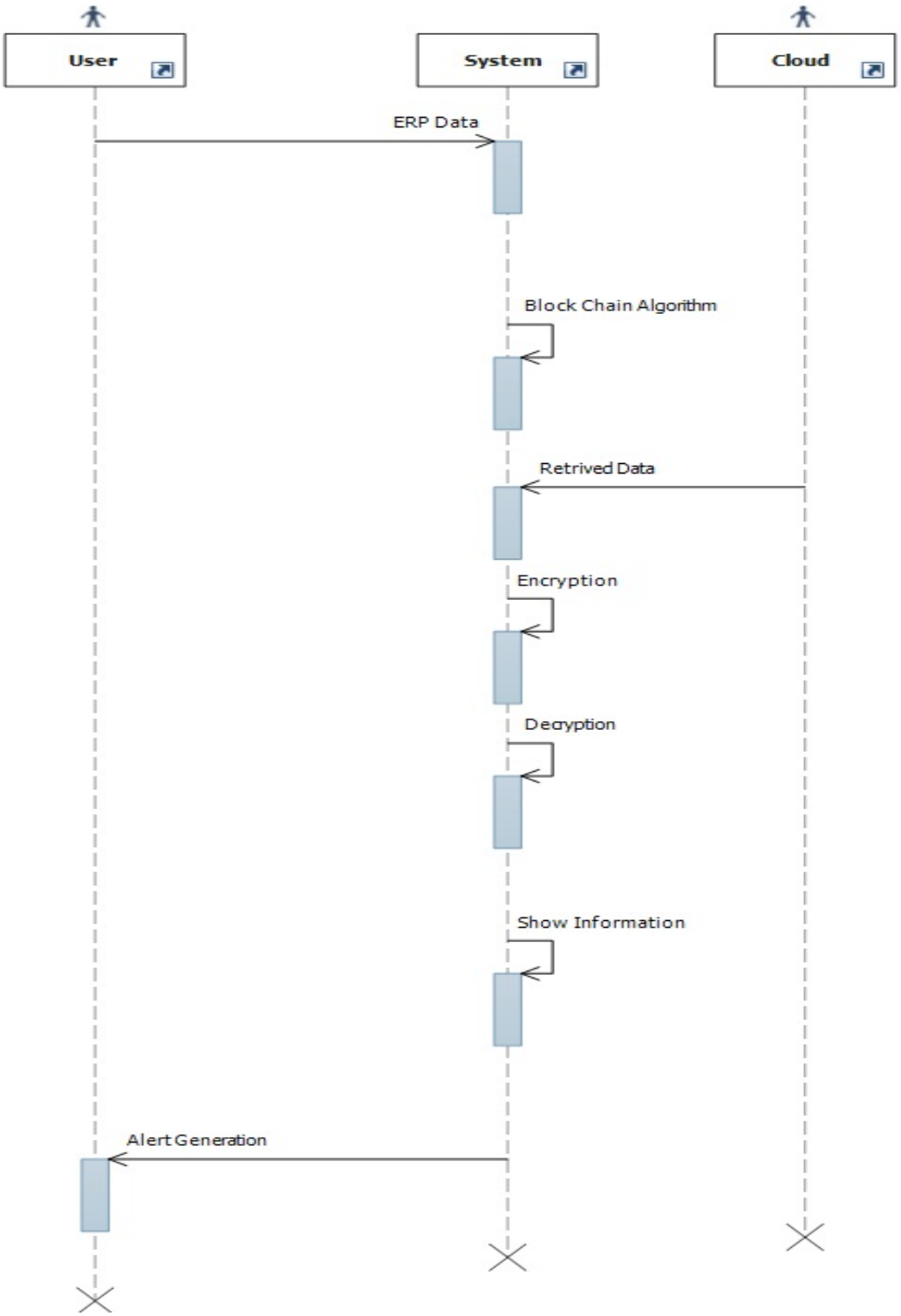

Figure 4.6: sequence Diagram

4.5 CLASS DIAGRAM

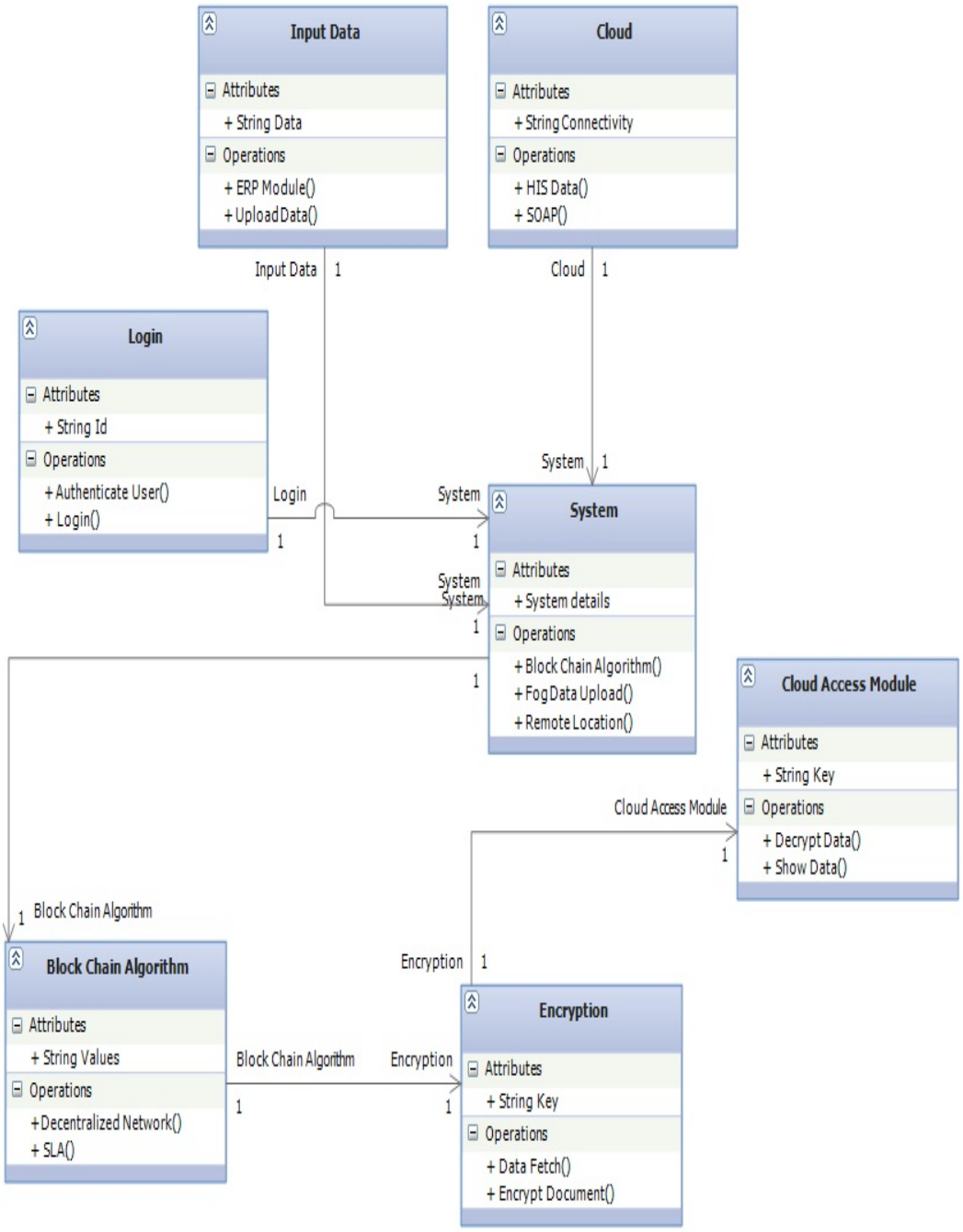

Figure 4.7: Class Diagram

CHAPTER 5

PROJECT PLAN

5.1 PROJECT ESTIMATION

5.1.1 Reconciled Estimate

TThe model followed is the Constructive Cost Model (COCOMO) for estimating the effort required in completing the project. Like all the estimation models, the COCOMO model requires sizing information. This information can be specified in the form of:

- Object Point
- Function Point(FP)
- Lines of Source Code(KLOC)(For this project, we use the sizing information in the form of Lines of Source Code.)
- Total Lines of Code for our project , KLOC=4k(approx).
- Cost of each person per month, Cp=Rs.150 /- (per person-hour)

Equation:

The initial effort (Ei) in man months is calculated using the equation:

E=a*(KLOC)^b

Where,

a=3.0,b=1.12, for a semi-detached project

E=Efforts in person-hour

D=a*(E)^b

Where,

a=2.5 ,b=0.32, for a semi-detached project.

D=Duration of project in months

Semi-detached project:

Project of moderate size and complexity, where teams with mixed experience levels must meet a mixed rigid and less than rigid requirements (project midway between embedded and organic types).

- Equation for calculation of Number of people required for completion of project, using the COCOMO model is:

  N=E/D

  Where,

  N=Number of people required

  E=Efforts in person-month

  D=Duration of project in months

- **Equation for calculation of Cost of Project, using the COCOMO model is:**

  C=D*Cp*hrs

  Where,

  C=Cost of project

  D=Duration in hours

  Cp=Cost incurred per person-hour

  Hrs=hours

- **Efforts:**

  $E=3.0*(5.2)^{1.12}$

  E=22.31 person-months

  Total of **22.31 person-months** are required to complete the project successfully.

- **Duration of project:**

  $D=2.0*(E)^{0.32}$

  D=4.75 months

  The approximate duration of project is **5 months**

- **Number of people required for the project:**

  N=22.31/7

  N=3.83

  N=4 people

  Therefore **4 people** are required to successfully complete the project on schedule.

- **Cost of project:**

  C=4*40*150=24000/-

  Therefore, the cost of project is 24000/-(approx.)

5.1.2 Project Resources

- People: Four students and one internal guide.
- Hardware:

  1. Processor - Core i5-7th generation
  2. Speed - 2.4 GHz
  3. RAM - 2GB(min)
  4. Hard Disk - 500 GB
  5. Linux cloud server
  6. OS-Windows Vista/7/8/10
  7. Software:
     (a) Pg Admin 4- tool for Postgres
     (b) Spring IDE

5.2 RISK MANAGEMENT

Project risk management is an important aspect of project management. Project risk is defined as, ”an uncertain event or condition that, if it occurs, has a positive or negative effect on a projects objectives”. The concepts of risk, risk management and individual risks are nearly interchangeable, being either personnel or monetary impacts respectively. Impacts in project risk management are more diverse, overlapping monetary, schedule, capability, quality and engineering disciplines. For this reason, in project risk management, it is necessary to specify the differences:-

- **Risk Management**: Organizational policy for optimizing investments and (individual) risks to minimize the possibility of failure.
- **Risk**: The likelihood that a project will fail to meet its objectives.
- **A risk**: A single action, event or hardware component that contributes to an effort’s ”Risk.”

There are different types of risks:-

- **Personnel risks:** Personnel risks caused by a lack of Knowledge about technology and training to perform functions. There is a possibility that errors are intentional, this is the result of the dubious conduct. The main risks from personal issues are:
  - Unintentional
  - Cannot perform task because lack of ability.
  - Lack of time management.
- **Process Risks**: The occurrence of internal process deciencies like inadequate performance indicators, inefcient controls, modeling failures and an inability to abide by the current laws.

- **Systems risks**: Arising from inadequate, poorly structured or defective IT systems. Some examples:-
  - Intermittent networks
  - Server crash
  - Physical damage to data storage components
  - System obsolescence
  - Improper maintenance
  - Power outage from internal causes
  - System slowdown

5.2.1 Risk identification

Risk identification is the process of finding out the possible pot-holes in a software application and minimizing it. This process is done to reduce the cost of running the software. The major type of Risk that is identified in the system are the System risks-network failures,server crash,power outage from internal causes,low processing speed of servers.

5.2.2 Risk Analysis

The risks for the Project can be analysed within the constraints of time and quality.

Table 5.1: Your first table.

Risk Discription α	**Probability** β
Real Time User Interface Design	Good
Decentarlized Data Management	Good

5.2.3 Overview of Risk Mitigation,Monitoring,Management

The primary goal of risk analysis is to identify as many potential risks as possible.For this project, care was taken to mitigate as many risks as possible.

Following are the details for each risk:

Risk ID	**1**
Risk Description	Real time user management
category	Requirement
Source	Software design Documentation review
Software design Documentation review	Low
Impact	High
Response	Medium
Strategy	Better accuracy can resolve problem
Risk Status	Identied

Table 5.2: Risk Identication 1.

Risk ID	**2**
Risk Description	Unrealistic Expectations
category	Requirement
Source	Identied during early development
Software design Documentation review	Medium
Impact	High
Response	Mitigate
Strategy	User need the impact of external factor.
Risk Status	Identied

Table 5.3: Risk Identication 2.

Risk ID	**3**
Risk Description	Centralized Database Management
category	Requirement
Source	Software Requirement specication document
Software design Documentation review	Low
Impact	High
Response	Mitigate
Risk Status	Identified

Table 5.4: Risk Identication 3.

5.3 PROJECT SCHEDULE

5.3.1 Project Task set

Major task in project are

Task 1: New User Block Creation.

Task 2: Admin Block Creation

Task 3: Cloud Connectivity

Task 4: Server Encoding

Task 5: Two Step Authentication

Task 6: GUI Creation

Task 7: Making Connection between the modules

Task 8: Testing integrity of the modules

Task 9: Finalizing the system

5.4 TIME LINE CHART

BLOCHAIN SECURITY FOR CLOUD

Project Start: Mon, 6-18-2018

TASK DESCRIPTION	PROGRESS	PLAN START	PLAN END	PLAN DAYS
Project Topic Discussion	5%	18 June 2018	01 July 2018	14
Project Domain Discussion	5%	02 July 2018	29 July 2018	28
Literature survey	7%	30 July 2018	16 August 2018	18
Design stratergy	5%	17 August 2018	07 September 2018	22
Data avaliability	6%	30 July 2018	03 September 2018	36
Sysnopsis report	10%	24 August 2018	05 October 2018	43
Hardware arangement	8%	06 October 2018	08 November 2018	34
Coding the Server system	20%	01 January 2019	25 February 2019	55
Coding the local system	15%	08 January 2019	05 March 2019	56
Testing	9%	10 March 2019	21 March 2019	11
Model evaluation	10%	25 March 2019	02 April 2019	8
TOTAL	100%			

Figure 5.1: Weekly Planner

5.5 TEAM ORGANIZATION

5.5.1 Team Structure

Team Members:

- Priyanka Chitte:
  - To study and analyse existing system and justify the feasibility of the problem.
  - Gathering the requirements for the software. Identifying the model
  - Preparing the draft for the paper.
- Pratiksha Bhalerao:
  - Exploiting functional dependencies and feasibility of the problem.
  - Contributing in designing the system and creating the flow of project by documentation of the system and performing testing by generating the test cases for the system.
  - Risk analysis and design block diagram.
- Manasi Jadhav:
  - Designing of the convolutional Blockchain network.
  - Implementation of the model.
  - Designing relevant UML diagram.
- Shrijit Jadhav:
  - Designing of the convolutional cloud system.
  - Implementation of the model.
  - Literature survey and contributing in documentation of system.

5.5.2 Management Reporting and Communication

- A document containing working of each week is maintained.
- In each week progress of work is discussed in meetings and record is maintained.
- Meeting was conducted on Tuesday or Friday of every week.

CHAPTER 6

PROJECT IMPLEMENTATION

6.1 OVERVIEW OF PROJECT MODULES

The Project was dived into 4 modules:-

1. **Server side definition:**connecting the user system with cloud system.
2. **Block-chain creation,verification,validation**
3. **Android application:**2 step verification system
4. **Cloud module:**Data storage

6.2 TOOLS AND TECHNOLOGY USED

6.2.1 MS-Visual studios

hspace*10exMicrosoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.

Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both as a source-level debugger and a machine-level debugger. Other built-in tools include a code profiler, forms designer for building GUI applications, web designer, class designer, and database schema designer. ˜

6.2.2 C#

C# is a general-purpose, modern and object-oriented programming language pronounced as C sharp. It was developed by Microsoft led by Anders Hejlsberg and his team within the .Net initiative and was approved by the European Computer Manufacturers Association (ECMA) and International Standards Organization (ISO). C# is among the languages for Common Language Infrastructure. C# is a lot

similar to Java syntactically and is easy for users who have knowledge of C, C++ or Java.

6.2.3 Andriod Studios

Android Studio is the official integrated development environment (IDE) for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for download on Windows, macOS and Linux based operating systems.[9][10] It is a replacement for the Eclipse Android Development Tools (ADT) as the primary IDE for native Android application development.

6.3 ALGORITHM DETAILS

- AES Algorithm-

  AES is a block cipher, that means encryption happens on fixed-length groups of bits. In our case the algorithm defines 128 bit blocks. AES supports key lengths of 128, 192 and 256 bit.Every block goes through many cycles of transformation rounds. The important part is that the key length does not affect the block size but the number of repetitions of transformation rounds (128 bit key is 10 cycles, 256 bit is 14).So AES will only encrypt 128 bit of data, but if the system want to encrypt whole to a single cipher text one can use GCM block mode.

  - Confidentiality: The ability to prevent eavesdroppers from discovering the plaintext message, or information about the plaintext message.
  - Integrity: The ability to prevent an active attacker from modifying the message without the legitimate users noticing.
  - Authenticity: The ability to prove that a message was generated by a particular party, and prevent forgery of new messages. This is usually provided via a Message Authentication Code (MAC). Note that authenticity automatically implies integrity.

AES with Galois/Counter Mode (GCM) block mode provides all those properties and our system uses this block mode for encryption.

- Public Key cryptography-

  Rather than using a single key for encryption and decryption, as is the case with symmetric key cryptography, separate keys (a public key and a private key) are used. A combination of a users public key and private key encrypt the information, whereas the recipients private key and sender's public key decrypt it. It is impossible to work out what the private key is based on the public key. Therefore, a user can send their public key to anyone without worrying that someone will gain access to their private key. The sender can encrypt files that they can be sure will only be decrypted by the intended party. Furthermore, through public-key cryptography a digital signature is produced, securing the integrity of the data.

- Digital signature-

  they provide validation and authentication in the same way signatures do, in digital form. Digital signatures are one of the main aspects of ensuring the security and integrity of the data that is recorded onto a blockchain. They are a standard part a blockchain protocols, mainly used for securing transactions and blocks of transactions, transferal of information, contract management and any other cases where detecting and preventing any external tampering is important. Digital signatures utilize asymmetric cryptography, meaning that information can be shared with anyone, through the use of a public key.

- RSA Algorithm-

  Hashing is the process of taking an input of any length and turning it into a cryptographic fixed output through a mathematical algorithm like RSA. The RSA algorithm can be used for both public key encryption and digital signatures. Key Generation Algorithm-

  1. Generate two large random primes, p and q, of approximately equal size such that their product n=pq is of the required bit length, e.g. 1024 bits.
  2. Compute n=pq and =(p1)(q1).
  3. Choose an integer e, 1¡e¡, such that gcd(e,)=1.
  4. Compute the secret exponent d, 1¡d¡, such that ed1mod.
  5. The public key is (n,e) and the private key (d,p,q). Keep all the values d, p, q and secret.
     - n is known as the modulus.
     - e is known as the public exponent or encryption exponent or just the exponent.
     - d is known as the secret exponent or decryption exponent.

- CONSENSUS ALGORITHMS:-

  Pow: (Proof of work) could be a accord strategy employed in the Bitcoin network . In PoW, every node of the network is shrewd a hash worth of the block header. The block header contains a nowadays and miners would modification the nowadays often to induce completely different hash values. The accord needs that the calculated worth should be adequate to or smaller than a specific given worth. PoS: (Proof of stake) is a vitality sparing option in contrast to PoW. Diggers in PoS need to demonstrate the responsibility for measure of money. Specifically, Blackcoin utilizes randomization to anticipate the next generator. It utilizes an equation that searches for the most minimal hash an incentive in blend with the span of the stake. Numerous blockchains embrace PoW toward the start and change to PoS bit by bit.

  PBFT: (Practical byzantine fault tolerance) is a replication calculation to endure byzantine issues. Hyperledger Fabric uses the PBFT as its

accord calculation since PBFT could deal with up to 1/3 malignant byzantine reproductions. DPOS: (Delegated proof of stake) is agent fair. Partners choose their agents to produce and approve squares. casted a ballot out effectively. DPOS is the foundation of Bitshares. Ripple: Ripple is an accord calculation that uses by and large confided in subnetworks inside the bigger system. In the system, hubs are separated into two kinds: server for taking an interest accord process and customer for just exchanging assets.

- Consensus Protocol Rules-

  Consensus rules are a specific set of rules that nodes on the network will ensure a block follows when validating that block and the transactions within it. The key requirement to achieve a consensus is a unanimous acceptance between nodes on the network for a single data value, even in the event of some of the nodes failing or being unreliable in any way.

CHAPTER 7

SOFTWARE TESTING

7.1 TYPES OF TESTING

1. Unit Testing: The register unit is tested for the registering new user and modifying the privileges of old user by admins. The admin validate the clients.

2. Integration testing: The validation process starts and personalised data access is granted to user.

3. GUI Testing: In this we test the performance and compatibility of GUI. We can conduct this by varieties of test cases.

4. System Testing: The system works properly independent of the platform or operating system.

5. Performance testing: The system provide effectiveness and speed under the performance testing

7.2 TEST CASES AND TEST RESULTS

Test case ID	Test Cases	Expected output	Actual output
1.	All fields are mandatory for the registration of the new users	The new users request should be granted if all fields are filled	The new users request is granted when all fields are successfully filled
2.	At least two admins should deactivate user to freeze user access	User access should be freeze.	The User access is freeze.
3.	At least two admins(out of 3) should approve block creation request of user	New block of user should be created	New block of user is created
4.	Access privileges of new users are setup by admin	User should access the data according to privileges assigned	User access the data according to privileges.
5.	Only the admin can update the user privileges	The user privileges should be updated by admin only.	The user privileges are updated by the admin only.

Table 7.1: Unit Testing

case Id	Test Cases	Expected output	Actual output
1.	sub-forms are visible as per user privileges	sub-forms should be updated accordingly	sub-forms are updated.
2.	Hidden password field	Password should be encapsulated in asterisk form .	password is encapsulated with asterisk
3.	User id and password incorrect	Error message pop up window should appear.	Error message pop up arrives.
4.	Validating user using fingerprint	user access should be granted	user access is granted.

Table 7.2: GUI Testing

Test case Id	Test Cases	Expected output	Actual output
1.	User System and cloud server connection	validation process should start	validation process is started
2.	cloud server and cloud database connection	personalized data should be accessed	personalized data is accessed.

Table 7.3: Integration Testing

Test case Id	Test Cases	Expected output	Actual output
1.	Higher accuracy algorithm	Accurate	Accurate
2.	System should be stable	System is stable	system is stable

Table 7.4: Performance Testing

CHAPTER 8

RESULTS

8.1 OUTCOMES

Following outcomes were observed:-

1. User are able to access the data and the ERP system.
2. Admin are able to authenticate the user request.
3. Admin are able to set permission to users.
4. Admin are able to monitor all data transaction done by all users.
5. User is able to authenticate his access using 2-step authentications(Bio-metrics).

8.2 SCREEN SHOTS

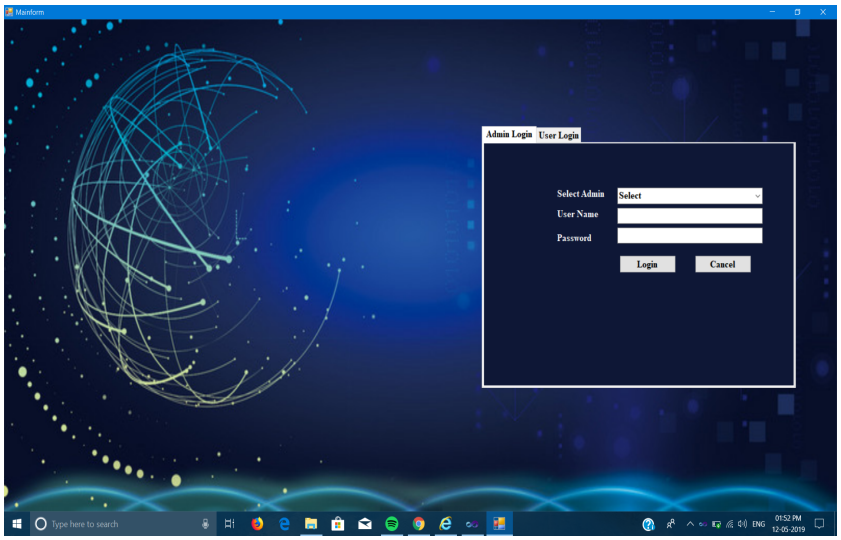

Figure 8.1: Login Page

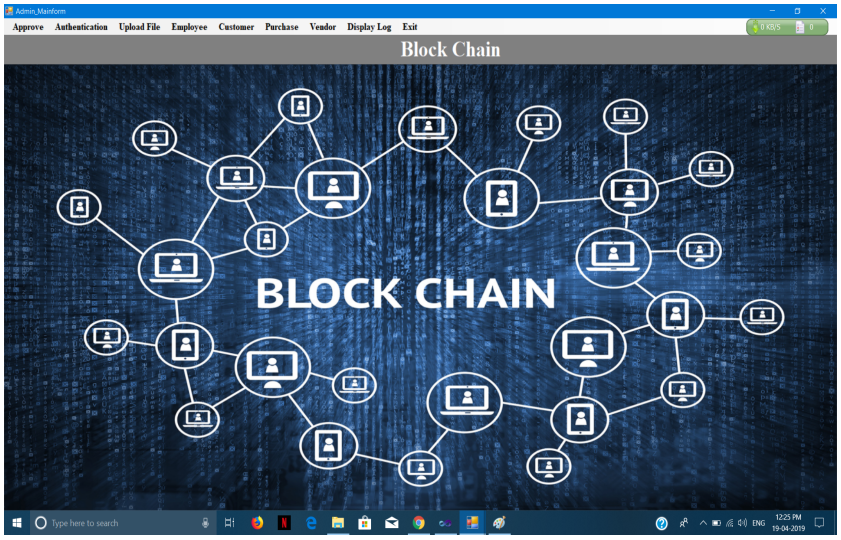

Figure 8.2: Admin Page

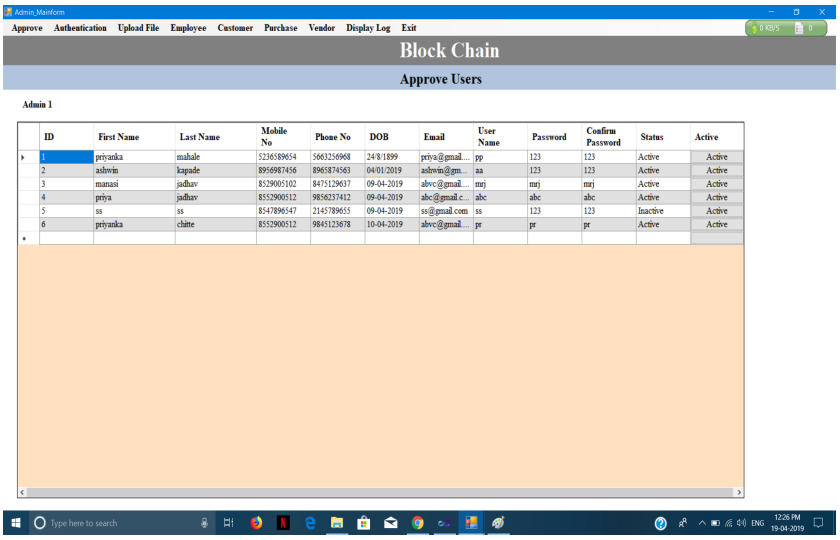

Figure 8.3: Adimin Approval

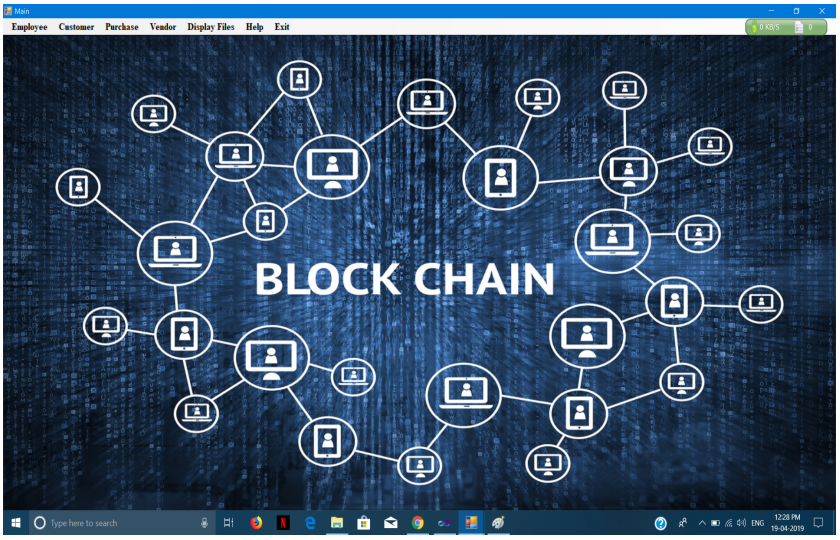

Figure 8.4: User Page

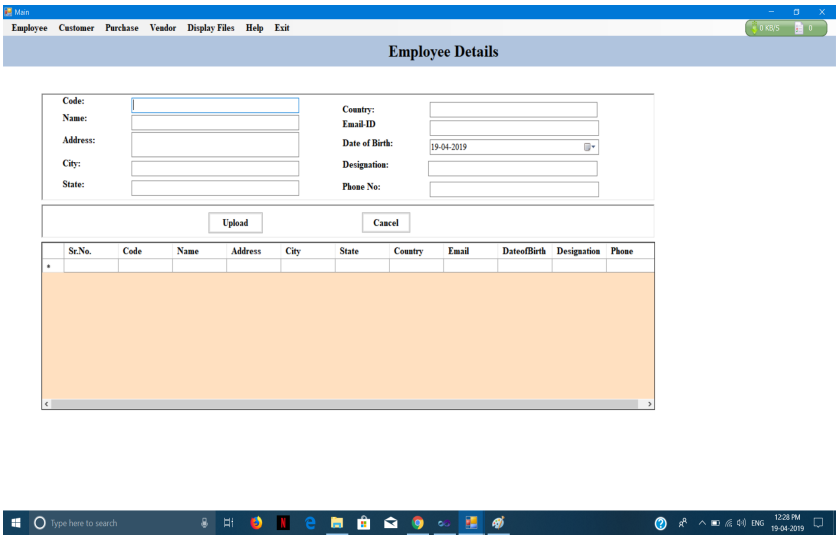

Figure 8.5: ERP Page

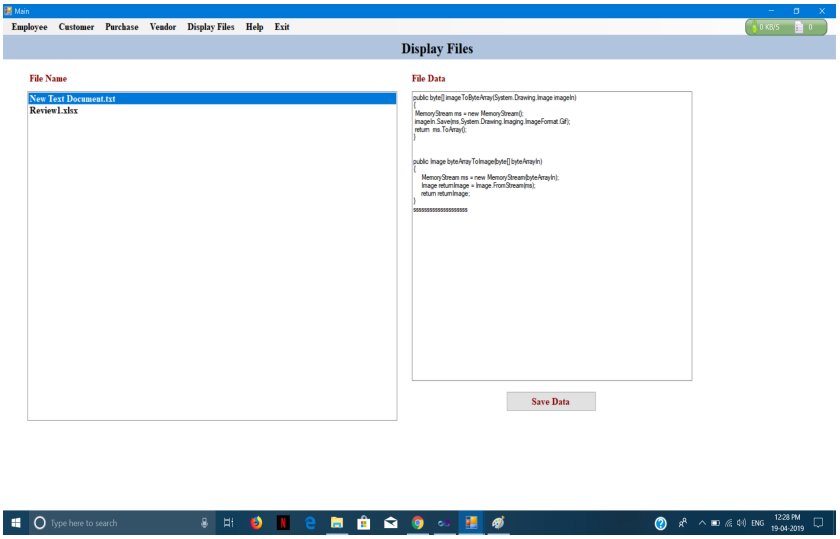

Figure 8.6: Document Page

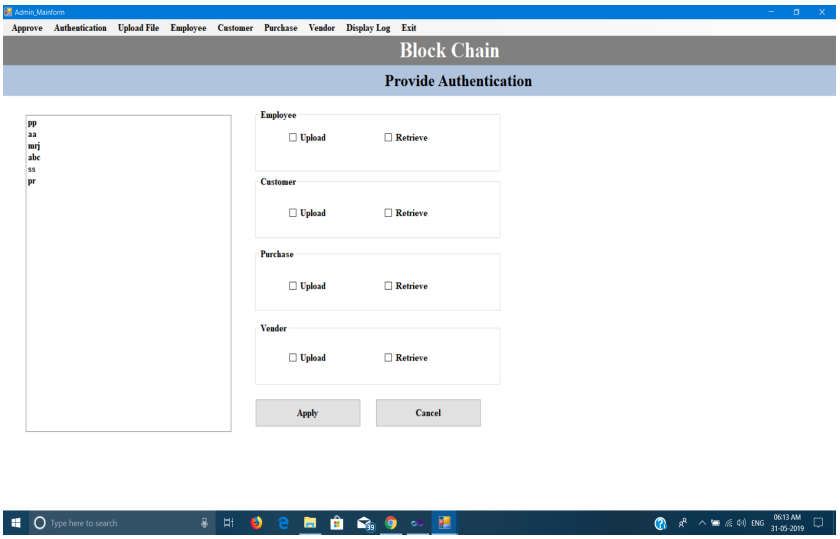

Figure 8.7: Admin Privilege set Page

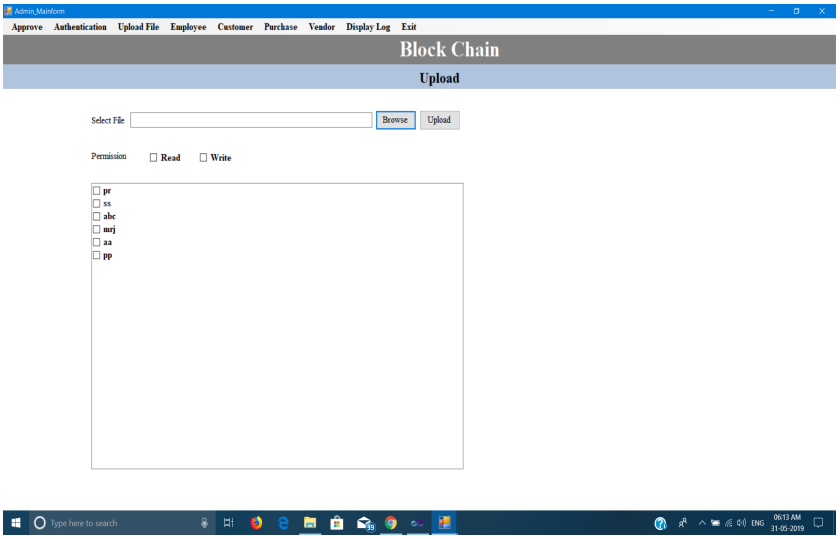

Figure 8.8: Admin file upload Page

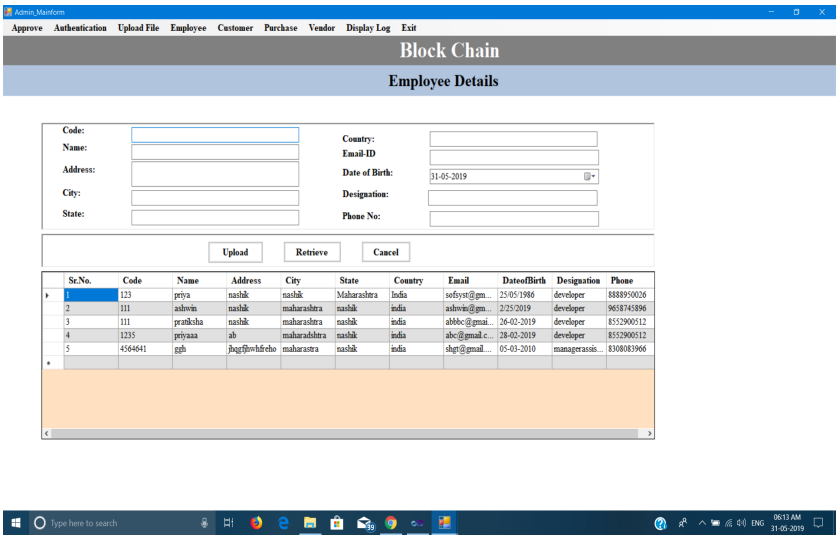

Figure 8.9: Admin ERP page

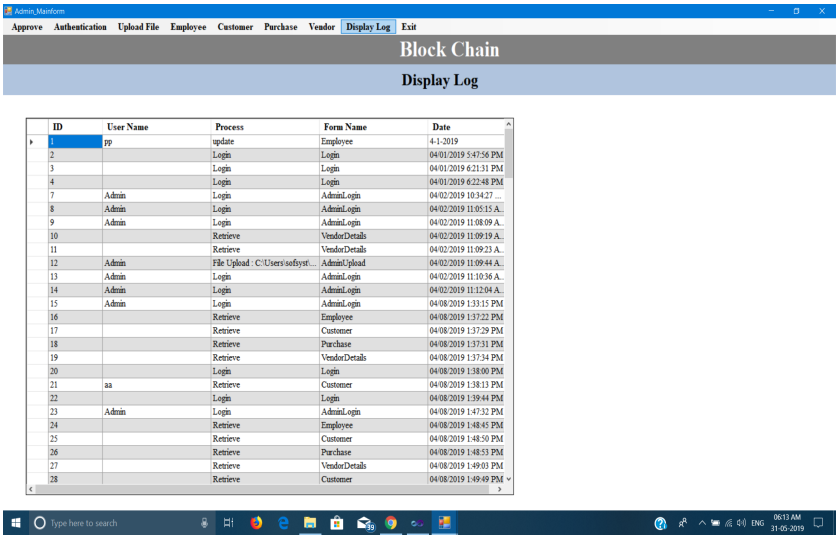

Figure 8.10: Admin Log Page

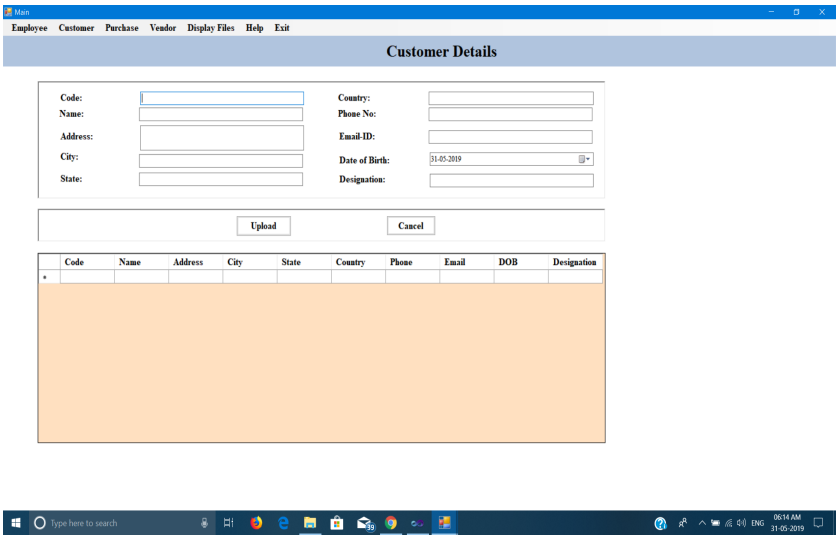

Figure 8.11: user ERP

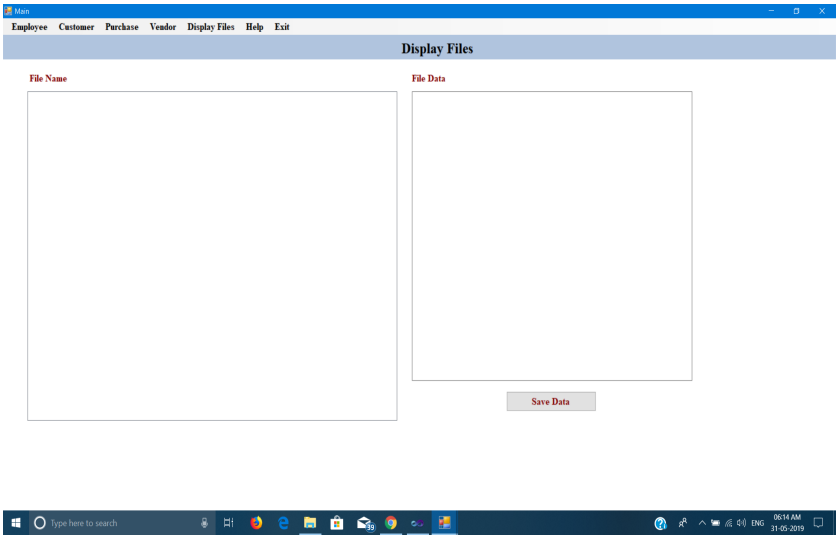

Figure 8.12: User file editing page

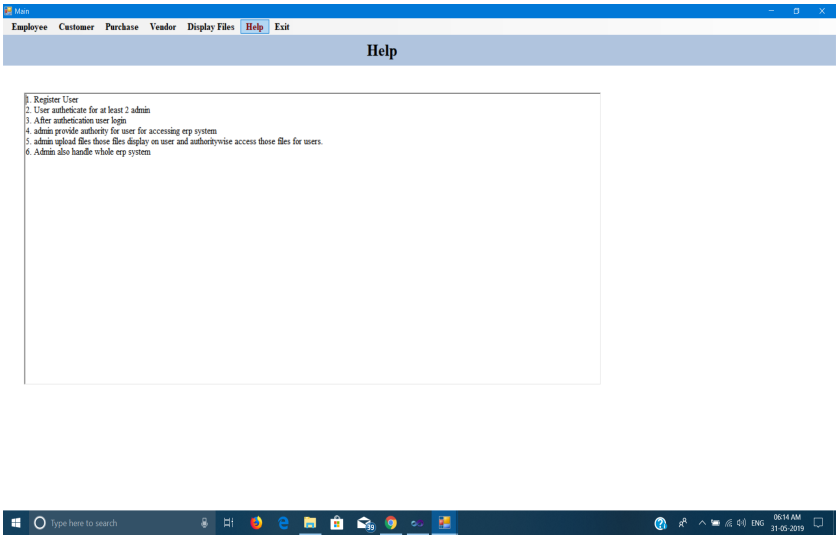

Figure 8.13: User Help

CHAPTER 9

CONCLUSION AND FUTURE WORK

9.1 CONCLUSION

Implemented a new blockchain-based solution for data usage auditing relying on the use of hierarchical ID-based mechanisms. Acting as a delegated PKG, each data owner is able to provide consent on his data usage and to control data collection and processing activities, in a privacy preserving manner based on smart-contract approach. In addition, our solution enables service providers to have a proof of receiving the data owners consent before processing his personal data, as the blockchain architecture is considered to be computationally tamper-proof.

9.2 FUTURE SCOPE

- System currently works on only a prescribed combination system OS,it can be designed to work on any combination of OS.
- Currently the System handles only one type of data, it can be designed to work with any type of data.
- System can be made more affordable depending on use of user.

9.3 APPLICATIONS

- Big Data Industry: System can be used in big data industries as a service purpose i.e. companies can provide this service to their client.
- Institutes: Vital information of institute like employee data, project report can be stored on the cloud using this system.
- Web applications: In web applications where only a specific amount of data is to be displayed out of entire data, this application can be used.

ANNEXURE A

System Description :

- Input: Request of user(send data to cloud or retrieve data from the cloud).
- Output: Requested data of user.
- A simple algorithm that aim towards reaching consensus .
- Mathematical Model:

  S={ I, O, F }

  I= User Details(local system verification)

  I= I1, I2, ..., In

  F= F1, F2, F3

  F1: Encryption of data

  F2: Decryption of data

  F3: Block Validation

  O= O1, O2

  O1: Retrieved data

  O2: Data uploaded

- xi(t) = $\sum_{jNi} aij(xj(t)xi(t))$,t>0

  Where, xi(t) is the information state of node i at time t with xi(0) being the initial state of node i.

  I= The algorithm can be interpreted as the change of agent is information being the difference between its own information and the agent connected to agents is information.

  With The Laplacian L from one can rewrite the consensus algorithm for all agents in a more compact form. x = -Lx

- Hash Function

  xi(t) = $\sum P(k) = 1/mj = 0, 1...m-1$

ANNEXURE B

PLAGIARISM REPORT

SmallSEOTools

PLAGIARISM SCAN REPORT

Words	989	Date	May 12,2019
Characters	6310	Exclude Url	

7%	93%	3	42
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

In the internet world demand for data is increasing day by day. This has gen-erated an issue of large data storage. To overcome this, cloud-based storage service was developed. Today there is vast involvement of cloud on business transaction and daily applications. This has raised the need for providing high end of security to the stored data, project helps to overcome this problem. The use of blockchain network as an interface to access the data which helps to overcome the problem of security of data on the cloud. The blockchain is a distributed public ledger and Internet-based computer network. This project works on the ERP data of a company, on a private cloud which is accessible through internet from any place. This system validates and secure the employee data of company. Smart phone and laptop security features like bio-metrics and password validation, can be to make this idea more robust and easier to use for end user. The local validation process of laptop and smart phones, acts as a user interface between the background process and the user. This also act as the next level of security for validation of user details. Thus, providing a more secure way of accessing the cloud service. CHAPTER 1 INTRODUCTION 1.1 MOTIVATION Recent years have witnessed the trend of increasingly relying on dis-tributed infrastructures. This increased the number of reported incidents of security breaches compromising user's privacy, where third parties massively collect, process and manage user's personal data. The use of blockchain network as an interface to access the data can help to overcome the problem of security of data on the cloud. The blockchain is a dis-tributed public ledger. Every computer on it is called a node and has to record every verified transaction or contract. Since there are many nodes in such a network, and every node has an entire record of all transactions constituting a blockchain, it is not possible to alter data on the network level, as it is required to do so, virtually on all nodes. Smart phone and laptop security features like bio-metrics and password validation, has helped to make this idea more robust and easier to use for end user. The local validation process of laptop and smart phones, acts as a user interface be-tween the background process and the user. This also act as the next level of security for validation of user details. Thus, providing a more secure way of accessing the cloud service. 1.2 PROBLEM DEFINITION To provides high end security to the data on the cloud, which is accessible to the user through an easy interface. 1.3 PROJECT SCOPE AND LIMITATION 1.3.1 Project Scope The proposed system can support Multi-objective i.e the system can be imple-mented on any device or data. Detection of alteration of data on cloud. Due to use of blockchain the data stored on cloud gets highly secured and any miscellaneous activity to alter the data will be detected and stopped and the data will return to the previous state. Provide high end of security to the stored data.This allows the user to save data on cloud without any worries. 1.3.2 Limitation This System system as of now works only on the Windows OS and Andriod only. System could not work without internet connection, the continuous good speed network is essential need of network. System attempts trillions of solutions per second in effort to validate transac-tion, so accuracy matters. CHAPTER 2 LITERATURE SURVEY Block-chain based data provenance can enable the transparency of data accountability in the cloud, and help to enhance the privacy and availability of the provenance data. System make use of the cloud storage scenario and choose the cloud file as a data unit to detect user operations for collecting provenance data. Sys-tem design and implement Prov-Chain, an architecture to collect and verify cloud data provenance, by embedding the provenance data into blockchain transactions. Prov-Chain operates mainly in three phases: provenance data collection. provenance data storage. provenance data validation. System present an evolutionary game theoretic framework to investigate the economic benefits of cyber security information sharing and analyze the impacts and consequences of not participating in the game. By using micro-economic the-ory as substrate, System model this framework as human-society inspired evolution-ary game among the organizations and investigate the implications of information sharing. Using proposed dynamic cost adaptation scheme and distributed learning heuristic, organizations are induced toward adopting the evolutionary stable strategy of participating in the sharing framework[2]. System present eclipse attacks on bit-coins peer-to-peer network. Attack allows an adversary controlling a sufficient number of IP addresses to monopolize all connections to and from a victim bit-coin node. The attacker can then exploit the victim for attacks on bit-coins mining and consensus system, including confirmation double spending, selfish mining, and adversarial forks in the blockchain. System take a detailed look at bit-coins peer-to-peer network, and quantify the resources in-volved in attack via probabilistic analysis, Monte Carlo simulations, measurements and experiments with live bit-coin nodes[4]. CHAPTER 3 SOFTWARE REQUIREMENT SPECIFICATION 3.1 INTRODUCTION The purpose of this project is to provide security to distributed data saved on cloud so it can store high confidential data, using block-chain. 3.1.1 User Classes and Characteristics The user of this system can be any person who needs to store his data on cloud. This user may vary from common person to business man and from single person to an entire organization.The user can either dump or retrieve data from cloud. To access the cloud user will have to verify himself using the bio-metric validation done on local system. According to user type the access of data will be offered by the system. 3.1.2 Assumptions and Dependencies Assumptions – The user specifies the user access of the data on the cloud. – The data uploaded should not be infected with virus. Dependencies – Consensus Algorithm. – Cloud connectivity. 3.2 FUNCTIONAL REQUIREMENT A local verification system. Data for storage(ERP data-BOM(bill of material)). Data request(querey).

Sources	Similarity
Blockchain Technology Aiming to Improve Cloud Security and CapacityCompare text every computer on it is called a node and has to record every verified transaction or contract. since there are many nodes in such a network, and every node has an entire record of all transactions constituting a blockchain, it is not possible to alter data on the network level, as it is required to do so... https://www.thesagenext.com/blog/blockchain-technology-aiming-improve-cloud-security-capacity/	5%
Sharing Information on Computer Systems Security: An Economic...Compare text	

ANNEXURE C

REFERENCES

1 X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: International Symposium on Cluster, Cloud and Grid Computing, IEEE/ACM, 2017

2 D. Tosh, S. Sengupta, C. A. Kamhoua, K. A. Kwiat, Establishing evolutionary game models for cyber security information exchange (cybex), Elsevier Journal of Computer and System Sciences. URL http://dx.doi.org/10.1016/j.jcss.2016.08.005

3 D. K. Tosh, M. Molloy, S. Sengupta, C. A. Kamhoua, K. A. Kwiat, Cyber-investment and cyber-information exchange decision modeling, in: IEEE 7th International Symposium on Cyberspace Safety and Security,2015, pp.12191224

4 E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoins peer-to-peer network, in: 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 129144

5 A. Biryukov, D. Khovratovich, I. Pustogarov, Deanonymisation of clients in bitcoin p2p network, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 1529.

6 X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: International Symposium on Cluster, Cloud and Grid Computing, IEEE/ACM, 2017.

7 C. Europe. Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In General Data Protection Regulation, January 2016, 2016.

8 M. Swan. Blockchain: Blueprint for a new economy. OReilly Media, Inc., 2015.

9 G. Zyskind, O. Nathan, and A. Pantland. Decentralizing privacy: Using blockchain to protect personal data. In IEEE Security and Privacy Workshops (SPW), 2015.

10 GSA, Cloud Computing Initiative Vision and Strategy Document (DRAFT), http://info.apps.gov/sites/default/files/ Cloud-Computing-Strategy-0.ppt.

11 S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

12 State of blockchain q1 2016: Blockchain funding overtakes bitcoin, 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/

REFERENCES