DELICATE INFORMATION EXCHANGE AMONG REPRESENTATIVE AND AUTHORITY

A PROJECT REPORT

Submitted by

GAYATHRI. S [REGISTER NO:211418104062]
HYSHWARRYA. J.D [REGISTER NO:211414104088]
KEERTHANA. P.N [REGISTER NO:211414104117]

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE, CHENNAI-600123.

ANNA UNIVERSITY: CHENNAI 600 025

MAY 2022

BONAFIDE CERTIFICATE

Certified that this project report **" DELICATE INFORMATION EXCHANGE AMONG REPRESENTATIVE AND AUTHORITY "** is the bonafide work of "**GAYATHRI.S (211418104062), HYSHWARRYA.J.D (211418104088), KEERTHANA.P.N (211418104117)"** who carried out the project work under my supervision.

SIGNATURE

Dr.S.MURUGAVALLI,M.E.,Ph.D .,
HEAD OF THE DEPARTMENT

DEPARTMENT OF CSE,
PANIMALAR ENGINEERING COLLEGE,
NASARATHPETTAI,
POONAMALLEE,
CHENNAI-600 123.

SIGNATURE

Mrs. D.JENNIFER, M.E.,
SUPERVISOR
ASSISTANT PROFESSOR

DEPARTMENT OF CSE,
PANIMALAR ENGINEERING COLLEGE,
NASARATHPETTAI,
POONAMALLEE,
CHENNAI-600 123.

Certified that the above candidate(s) were examined in the Anna University Project Viva-Voce Examination held on..........................

INTERNAL EXAMINER

EXTERNAL EXAMINER

DECLARATION BY THE STUDENT

We, GAYATHRI.S (211418104062), HYSHWARRYA.J.D (211418104088), KEERTHANA.P.N (211418104117)_hereby declare that this project report titled "DELICATE INFORMATION EXCHANGE AMONG DELEGATE AND AUTHORITY" , under the guidance of **Mrs.D.JENNIFER.,M.E.,** is the original work done by us and we have not plagiarized or submitted to any other degree in any university by us.

GAYATHRI S

HYSHWARRYA J D

KEERTHANA P N

ACKNOWLEDGEMENT

We would like to express our deep gratitude to our respected Secretary and Correspondent **Dr.P.CHINNADURAI, M.A., Ph.D.** for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We express our sincere thanks to our Directors **Tmt.C.VIJAYARAJESWARI**, **Dr.C.SAKTHI KUMAR,M.E.,Ph.D** and **Dr.SARANYASREE SAKTHI KUMAR B.E.,M.B.A.,Ph.D.,** for providing us with the necessary facilities to undertake this project.

We also express our gratitude to our Principal **Dr.K.Mani, M.E., Ph.D.** who facilitated us in completing the project.

We thank the Head of the CSE Department, **Dr. S.MURUGAVALLI , M.E.,Ph.D.,** for the support extended throughout the project.

We would like to thank my **Project Guide Mrs. D. Jennifer** and all the faculty members of the Department of CSE for their advice and encouragement for the successful completion of the project.

GAYATHRI.S
HYSHWARRYA.J.D
KEERTHANA.P.N

ABSTRACT

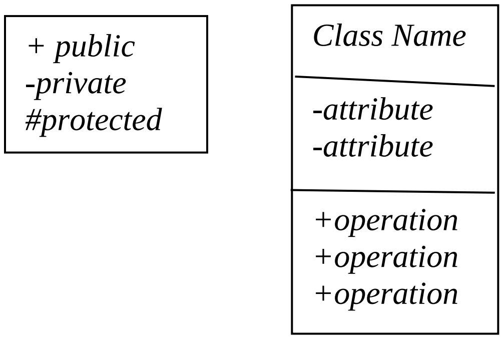
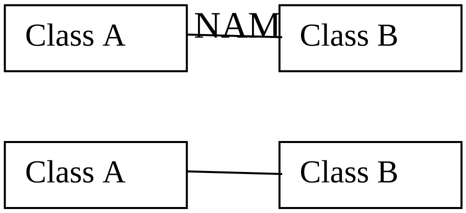
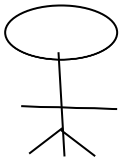
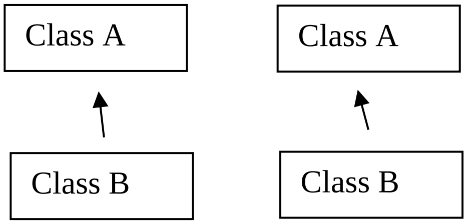
The principal point is to give a more secure climate to touchy information exchanges between the representative and position to forestall information spillage if any. This application gives a dispersed application administration and utilizations blockchain innovation to help it. The SaaS layer module offers a cloud stage administration that permits each party effectively participate in business correspondences by means of web-based interfaces. The proposed shrewd framework is utilized by each party engaging in the exchange of delicate information. Gathering staff data and guides their connections for a total image of client account association. We'll assist you with security plan while making clients, gatherings, and job based authorizations Encryption is an exceptionally nonexclusive term and there are numerous ways of encoding information. Organizations need to accurately execute and oversee encryption. The way in to a decent encryption technique is areas of strength for utilizing and legitimate key administration. Scramble touchy information before it is shared over untrusted networks (ex. Encoded document capacity).

TABLE OF CONTENTS

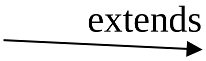
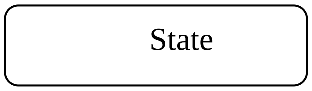
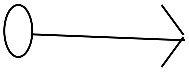
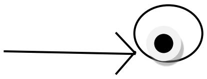
LIST OF TABLES:

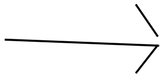
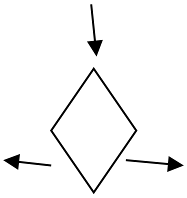
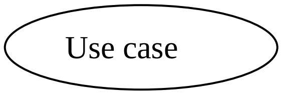
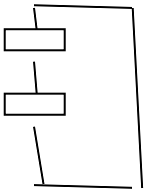
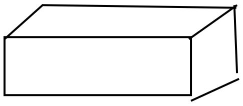
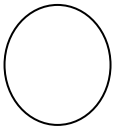
LIST OF FIGURES:

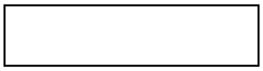
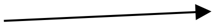
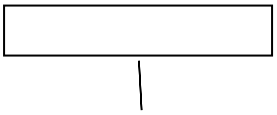
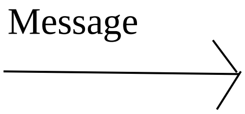
LIST OF SYMBOLS:

S.NO	NOTATION NAME	NOTATION	DESCRIPTION
1.	Class	 + public -private #protected Class Name -attribute -attribute +operation +operation +operation	Represents a collection of similar entities grouped together.
2.	Association		Associations represents static relationships between classes. Roles represents the way the two classes see each other.
3.	Actor		It aggregates several classes into a single classes.
4.	Aggregation		Interaction between the system and

			external environment

5.	**Relation** (uses)	**uses**	Used for additional process communication.
6.	Relation (extends)		Extends relationship is used when one use case is similar to another use case but does a bit more.
7.	Communication		Communication between various use cases.
8.	State		State of the process.
9.	Initial State		Initial state of the object
10.	Final state		Final state of the object

11.	Control flow		Represents various control flow between the states.
12.	Decision box		Represents decision making process from a constraint
13.	Use case		Interact ion between the system and external environment.
14.	Component		Represents physical modules which is a collection of components.
15.	Node		Represents physical modules which are a collection of components.
16.	Data Process/State		A circle in DFD represents a state or process which has been triggered due to some event or action.

17.	External entity		Represents external entities such as keyboard, sensors, etc.
18.	Transition		Represents communication that occurs between processes.
19.	Object Lifeline		Represents the vertical dimensions that the object communications.
20.	Message		Represents the message exchanged.

LIST OF ABBREVIATIONS:

Sl.no	Abbreviation	Expansion
1	HTML	Hypertext Markup Language
2	CSS	Cascading Style Sheets
3	Js	Java script
4	IDE	Integrated Development Environment
5	SQL	Structured Query Language

6	AWS	Amazon Web Server
8	RDS	Relational Database Service
9	RSA	Rivest Shamir Adleman
10	AES	Advanced Encryption Standard
11	SHA	Secure Hash Algorithm
12	OS	Operating System
13	QR Code	Quick Response Code
14	RAM	Random Access Memory
15	UML	Unified Modelling Language
16	JSP	Java Server Pages
17	SMC	Secure Multiparty Computation
18	JVM	Java Virtual Machine

INTRODUCTION

1.1 OBJECTIVES

Collecting staff information and maps their relationships for a complete picture of user account organization. We'll help you with privacy design when creating users, groups, and role-based permissions Encryption is a very generic term and there are many ways to encrypt data. Companies need to implement and manage encryption correctly. The key to a good encryption strategy is using strong encryption and proper key management. Encrypt sensitive data before it is shared over untrusted networks (ex. Encrypted file storage).

1.2 PROBLEM DEFINITION:

Touchy information exchange is private data that should be remained careful and far away from all untouchables except if they have consent to get to it. Admittance to touchy information ought to be restricted through adequate information security and data security rehearses intended to forestall information holes and information breaks. Delicate information can be any kind of data that should be shielded from unapproved admittance to protect the security or security of an individual or association. It can incorporate any data relating to: Passwords. Encryption keys.

LITERATURE SURVEY

1.TITLE: "A Survey on Secured Data Sharing using Ciphertext Policy Attribute Based Encryption in Cloud”

AUTHOR: G. A. Thushara and S. M. S. Bhanu

YEAR: 2021

PAPER EXPLANATION:

"Cloud based data sharing" is a procedure that permits scientists to convey and team up, that prompts major new improvements in the field. It additionally empowers clients to "access information" over the cloud effectively and advantageously. Protection, realness and privacy are the three principal challenges while sharing information in cloud. "Characteristic Based Encryption(ABE), Role Based Encryption, Hierarchical Based Encryption, and Identity Based Encryption", are sorts of encryption.

2.TITLE: A systematic literature review of blockchain cyber security

AUTHOR: Paul J. Taylor, Tooska Dargahi , Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo.

YEAR: 2020

PAPER EXPLANATION:

Since the distribution of Satoshi Nakamoto's white paper on Bitcoin in 2008, blockchain has (gradually) become perhaps the most often talked about strategy for getting information stockpiling and move through decentralized, trustless, shared frameworks. This exploration recognizes peer-looked into writing that tries to use blockchain for digital protection purposes and presents a deliberate examination of the most often taken on blockchain security applications. Our discoveries show that the Internet of Things (IoT) loans itself well to novel blockchain applications, as do organizations and machine perception, public key cryptography, web applications, certificate plans and the solid stockpiling of Personally Identifiable Information (PII). This convenient efficient audit additionally reveals insight into future bearings of exploration, schooling and practices in the blockchain and network protection space, for example, security of blockchain in IoT, security of blockchain for AI information, and sidechain security, and so forth.

3.TITLE: “Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism “

AUTHOR: Sanjeev Kumar Dwivedi, Ruhul Amin, Satyanarayana Vollala

YEAR: 2020

PAPER EXPLANATION:

This paper depicts how the blockchain instrument consolidates with the conventional drug inventory network framework and to accomplish a superior SCM framework, we present a "blockchain-based plot" for data sharing safely in the drug inventory network framework with shrewd agreements and agreement system. The proposed plot additionally gives a system to "appropriate required cryptographic keys" to every one of the members safely utilizing the shrewd agreement strategy.

4.TITLE: Secure Secret Sharing Using Homomorphic Encryption

AUTHOR: Nileshkumar Kakade; Utpalkumar Patel

YEAR: 2020

PAPER EXPLANATION:

Secret sharing is a significant means to accomplish classification and information security. Secret imparting arrangements to parting a restricted data with different players. The objective of the mystery sharing is security of mystery, protection and concealing data. There are various methods accessible for secret sharing for example polynomial, Chinese leftover portion hypothesis, vector space, network projection. Methods have attributes like edge, proactive, obvious. Proactive mystery sharing plan permit client to change share in the event of uncertainty of burglary. In this work we propose the proactive mystery sharing plan in view of homomorphic methods. Our plan comprises of three periods of offer development, share reestablishment, share recreation. Focal power parts a scrambled mystery with each gatherings utilizing homomorphic property of paillier encryption for example deduction. In recharging process at least two gatherings relate share with one another for to produced restored share. In remaking process all gatherings offer will be add to focal power then, at that point, scrambled mystery will be produced. Focal power will unscramble encoded secret utilizing secret key then unique mystery will be created. Our plans interesting elements is offer can be reestablished any time, Each party can pick mysterious voluntarily, If any two gatherings have same substance share then likewise scrambled offer will be different because of non-deterministic property of paillier encryption.

5.TITLE: Secure Computation by Secret Sharing using Input Encrypted with Random Number

AUTHOR: Keiic Keiichi Iwamura and Ahmad Akmal Aminuddin Mohd Kamalhi Iwamura and Ahmad Akmal Aminuddin Mohd Kamal

YEAR: 2019

PAPER EXPLANATION:

Regularly, genuinely secure calculation utilizing a (k, n) limit secret sharing is viewed as incomprehensible when $n < 2k - 1$. In this manner, in our past work, we originally adopted the strategy of finding the circumstances expected for secure calculation under the setting of $n < 2k - 1$ and showed that safe calculation utilizing a (k, n) limit secret sharing can be acknowledged with a semi-legitimate enemy under the accompanying three preconditions: (1) the aftereffect of secure calculation does exclude 0; (2) irregular numbers remade by every server are fixed; and (3) every server holds arbitrary numbers obscure to the foe and holds portions of irregular numbers that make up the irregular numbers obscure to the foe. In this paper, we show that by leaving condition (3), secure calculation with data hypothetical protection from a semi-fair enemy is conceivable with $k \leq n < 2k - 1$. Furthermore, we explain the upside of utilizing privileged intel that has been scrambled with an arbitrary number as contribution to get calculation. One of the benefits is the speed increase of the calculation time. Specifically, we partition the calculation cycle into a preprocessing stage and a web-based stage and shift the expense of correspondence to the preprocessing stage. Accordingly, for calculations, for example, internal item activities, we understand a quicker online stage, contrasted and ordinary techniques.

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

The vast majority of the current homomorphic secret sharing and secure multi-party processing advances have the issues of gigantic correspondence adjusts and an excessive amount of traffic load. If the plaintext is utilized, the framework face the gamble of uncovering information security. In any case, if the ciphertext is utilized, despite the fact that information security is safeguarded, it is hard to help homomorphic figuring. Likewise, the peculiarity of DE dissemination in present day enterprises experience the accompanying issues: There is a gamble of spillage of touchy information in the flow.

Methodology: Different hash function models, DSA Algorithm

Disadvantages:

- It takes long time to process various hash function methods.
- DSA algorithm requires lot of time to authenticate.
- Data is not encrypted in DSA.

3.2 PROPOSED SYSTEM:

The proposed brilliant framework is utilized by administrator or authority engage in the creation of delicate information. The last delicate information are delivered by the last information chairman or authority individual, and different modules associated with the course of information total know nothing about the last information. We have involved SHA calculation for producing hash codes, for secure information base administration and square chain innovation for secure information exchange. The age of two different access codes, one from private key and the other from QR Code makes it extraordinary from the current framework. Subsequently, Improving the respectability of the information.

Methodology: SHA Algorithm, AES Algorithm, Block-Chain Technology

Advantages:

- It gives standard and valid solution to process the data with hash function.
- Data is encrypted using AES and stored in the cloud.
- Block chain is used to connect the hash values.
- QR Code generation.

3.3 FEASIBILITY STUDY:

Practicality concentrates on expect to unbiasedly and normally uncover the qualities and shortcomings of the current business or proposed adventure, open doors and dangers as introduced by the climate, the assets expected to bring through, and eventually the possibilities for progress.

In its easiest term, the two rules to pass judgment on plausibility are cost expected and worth to be accomplished. Thusly, a very much planned achievability study ought to give an authentic foundation of the business or task, depiction of the item or administration, bookkeeping proclamations, subtleties of the activities and the board, advertising examination and approaches, monetary information, lawful prerequisites and assessment commitments. For the most part, achievability studies go before specialized advancement and task execution.

They are 3 types of Feasibility

- Technical feasibility
- Economical feasibility
- Social feasibility

Technical Feasibility:

It incorporates figuring out advancements for the undertaking, both equipment and programming. Here, the base equipment prerequisite is 2GB RAM and Dual-port processor and the product necessities incorporate Windows OS, MySQL data set and Eclipse IDE. The backend innovation utilized is JAVA. Since, it is stage free and can be utilized in assortment of uses.

Economic Feasibility:

Here, we track down the absolute expense and advantage of the proposed framework over current framework. For this venture, the primary expense is data set administration cost. This fills in as a straightforward web application which is cost productive. Additionally, it is basic in activity and doesn't cost preparing or fixes.

Social Feasibility:

Our necessities picked are not all that complex. It requires a straightforward OS and programming. It includes no mind boggling computations. Information partook in this framework is more private, with the goal that any individual this framework need not stress over the information breaks.

3.4 HARDWARE REQUIREMENTS

Microsoft Windows 7/8/10 (32 or 64 bit).

Dual Core Processor

4 GB RAM recommended

250 GB disk space

3.5 SOFTWARE REQUIREMENTS:

Front end -> HTML, CSS, Js, JQuery

Back end -> JAVA

DBMS -> MySQL

IDE -> Eclipse

Frontend + Backend hosted in AWS Server

SYSTEM DESIGN

4.1 E-R DIAGRAM:

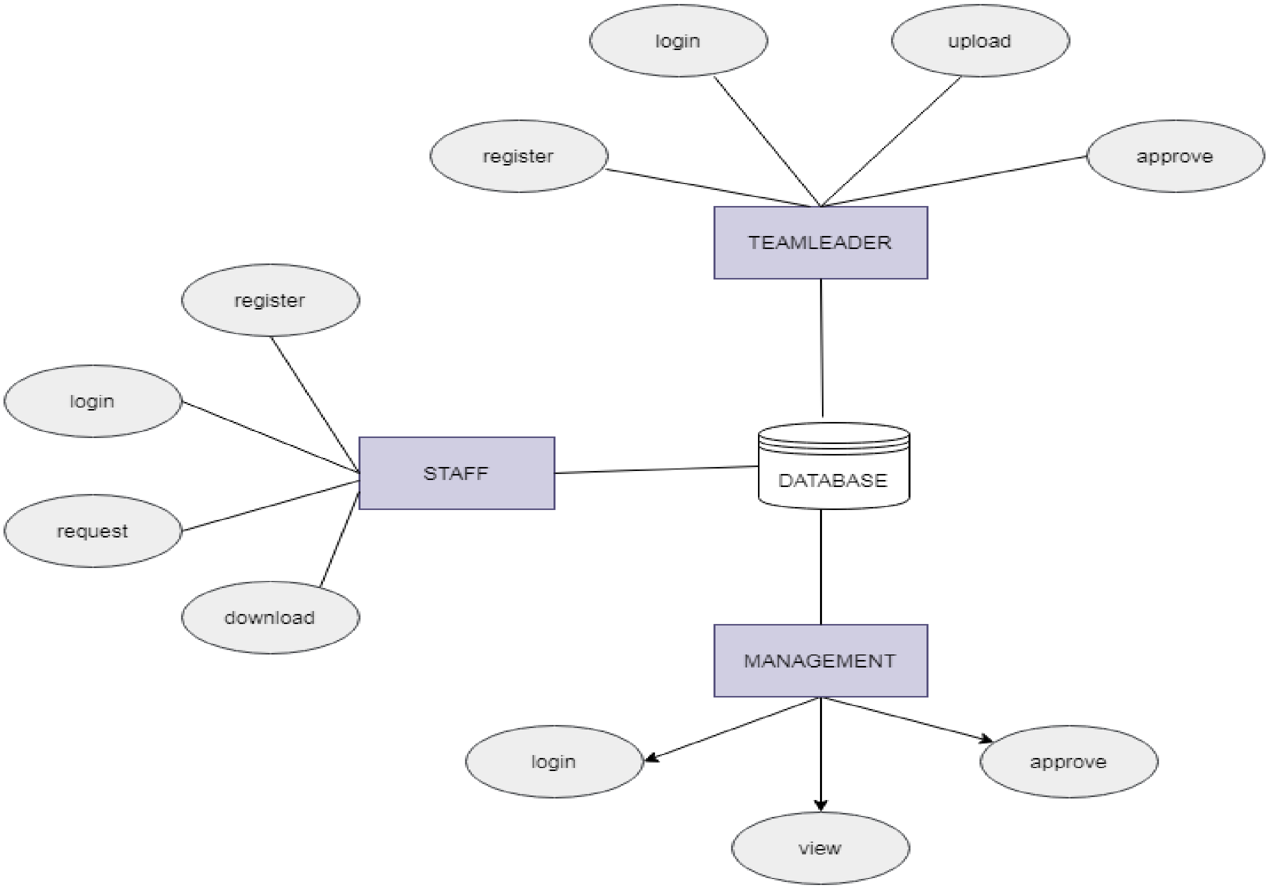


Fig 4.1 E-R diagram of Modules

Explanation:

An Entity Relationship (ER) Diagram is a form of flowchart that shows how "entities" within a system, such as people, things, or concepts, interact with one another.

4.2 DATA FLOW DIAGRAM:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. It differs from the flowchart as it shows the data flow instead of the control flow of the program. A data flow diagram can also be used for the visualization of data processing. The DFD is designed to show how a system is divided into smaller portions and to highlight the flow of data between those parts.

Level – 1:

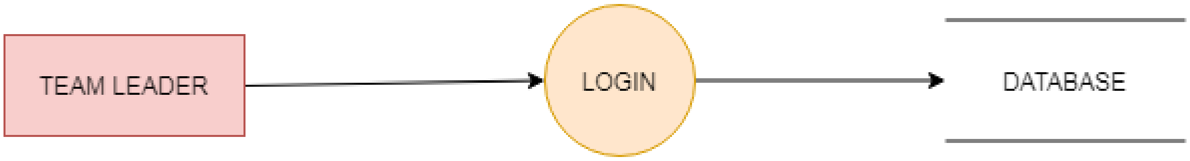


Fig 4.2 DFD – Team Leader Login

Level – 2:

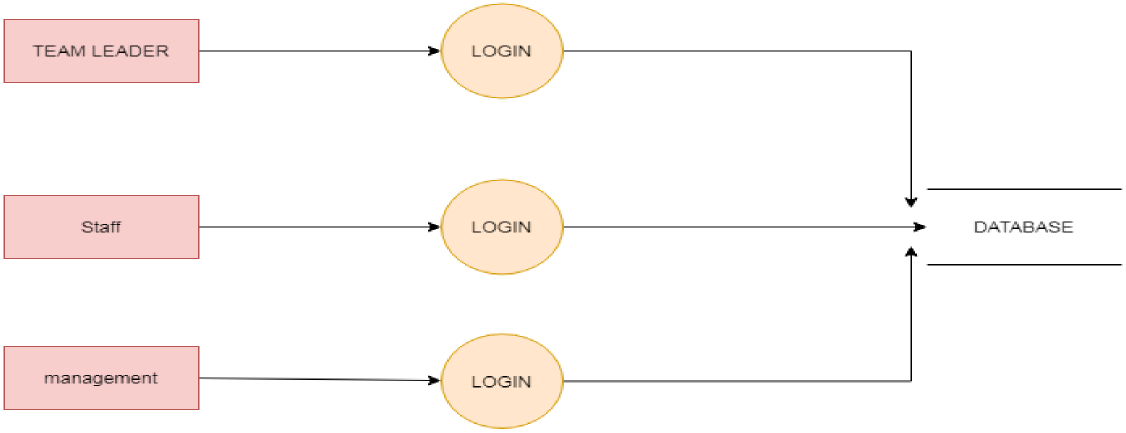


Fig 4.3 DFD – All sectors Login

Level – 3:

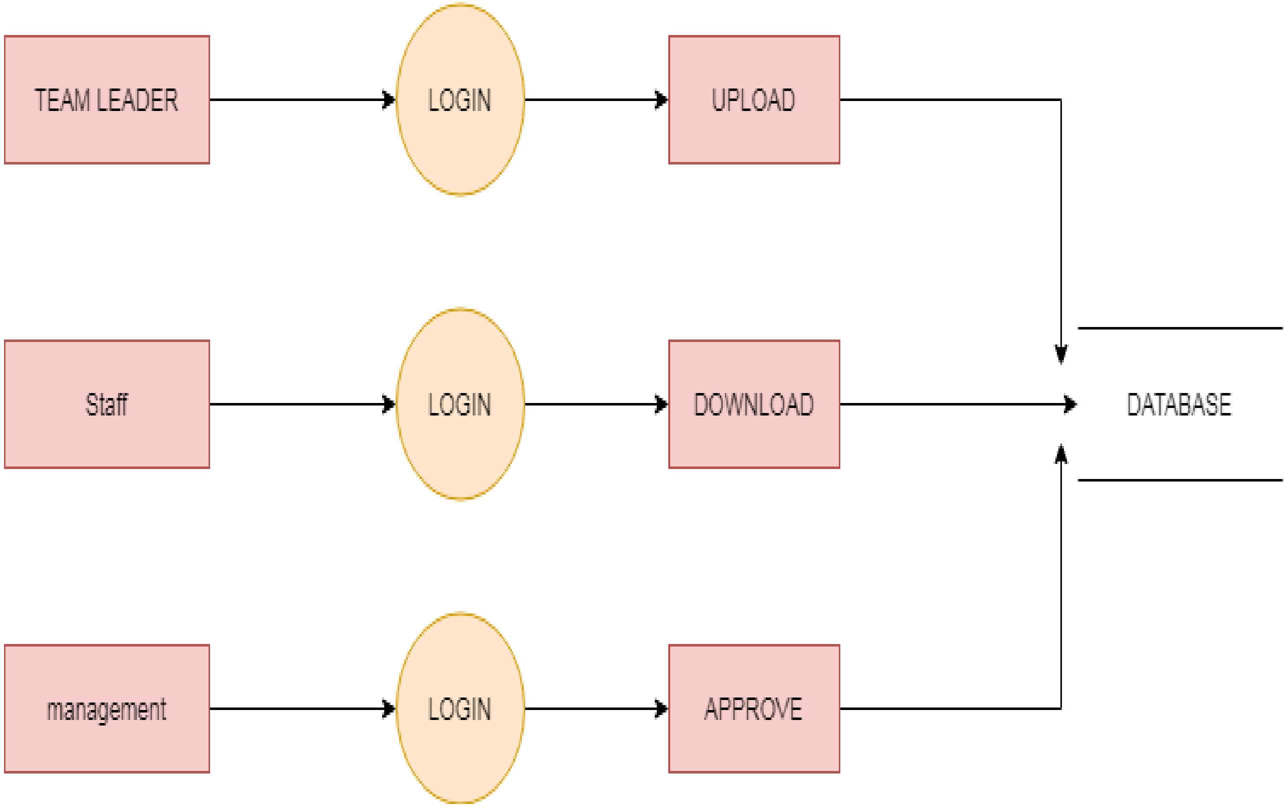


Fig 4.4 DFD – Decryption Process

4.3 UML DIAGRAMS:

4.3.1 Use-Case Diagram:

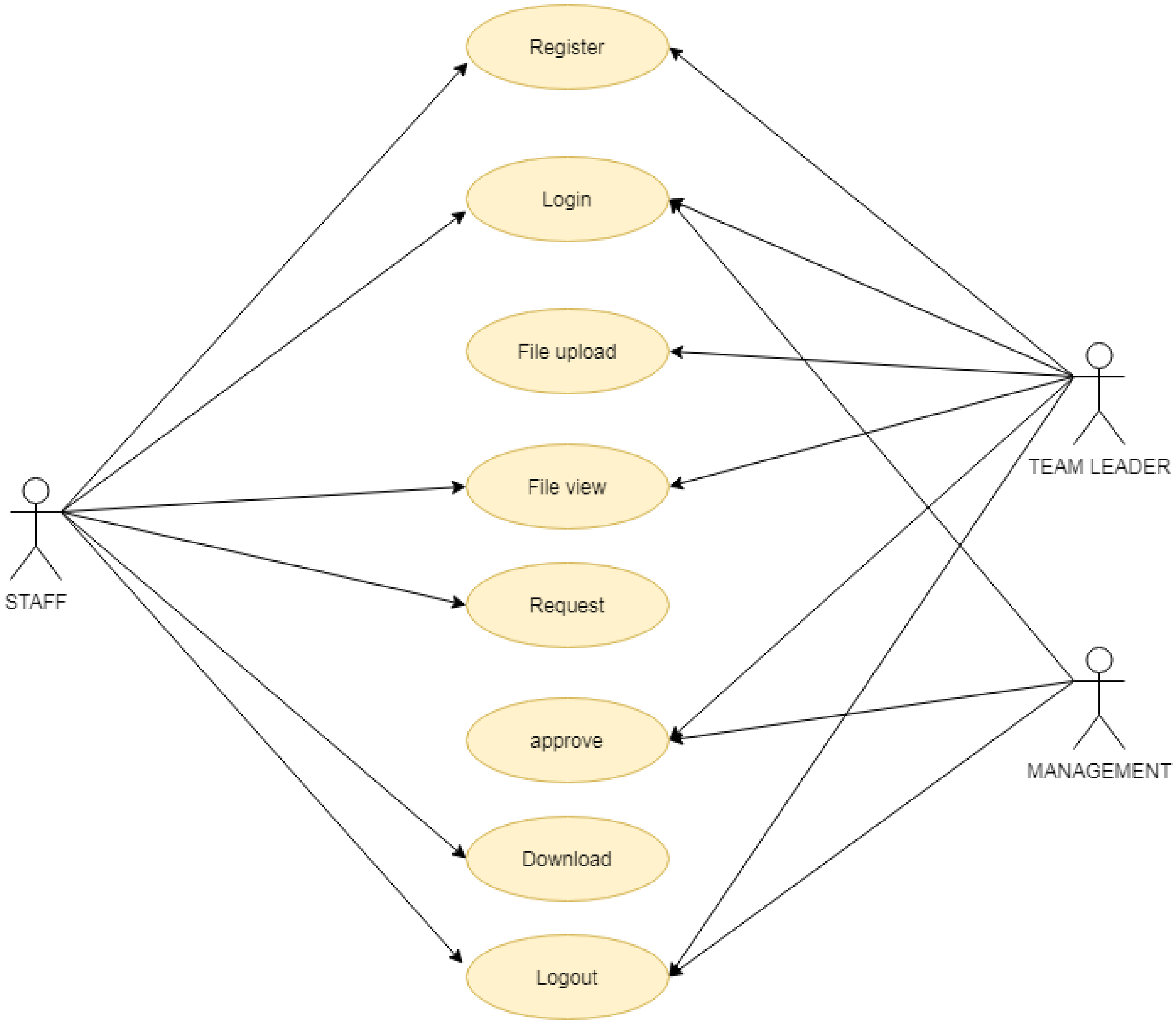


Fig 4.5 Use Case diagram of Encryption Process

EXPLANATION:

The use case diagram is the main building block of object oriented modeling. It is used both for general conceptual modeling of the systematic of the application, and for detailed modeling translating the models into programming code. For this in our component diagram first propose a data. In this proposed method we are using Hash-Solomon Code Algorithm to encrypt the data.

4.3.2 State Diagram:

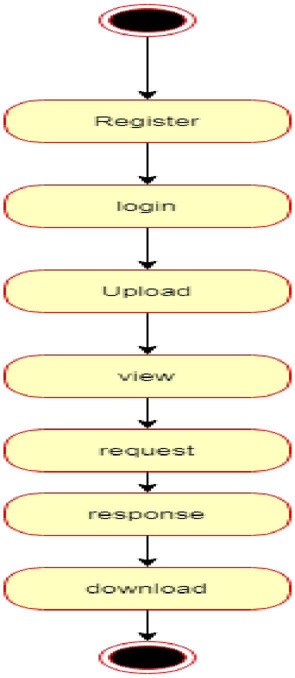


Fig 4.6 State Diagram of Request process

EXPLANATION:

State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction. Many forms of state diagrams exist, which differ slightly and have different semantics. In our state diagram first propose a. For this in our component diagram first propose a data. In this proposed method we are using Hash-Solomon Code Algorithm to encrypt the data.

4.3.3 Activity Diagram:

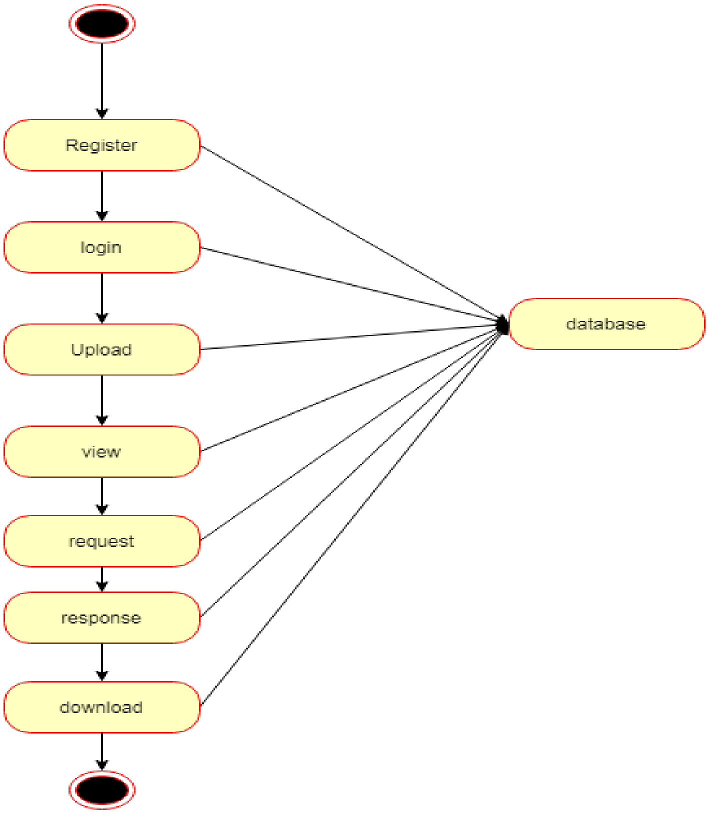


Fig 4.7 Activity Diagram of Database Storage

EXPLANATION:

Activity diagram are a loosely defined diagram to show workflows of stepwise activities and actions, with support for choice, iteration and concurrency. UML, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. UML activity diagrams could potentially model the internal logic of a complex operation. In many ways UML activity diagrams are the object-oriented equivalent of flow charts and data flow diagrams (DFDs)from structural development.

4.3.4 Class Diagram:

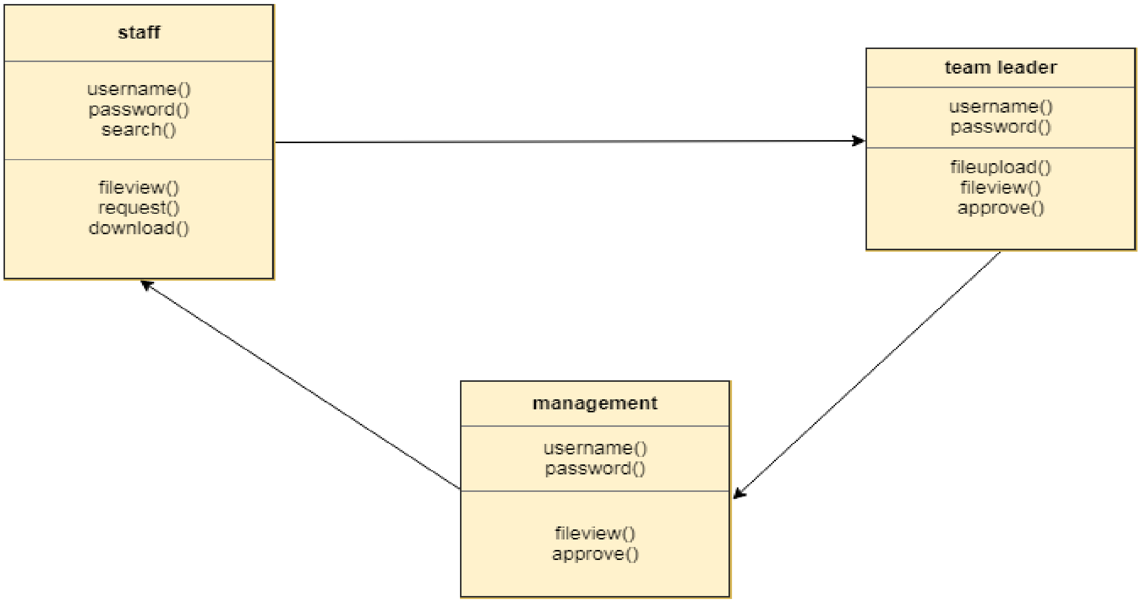


Fig 4.8 Class Diagram of Functions

EXPLANATION:

Class diagram is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, and the relationships between the classes. The classes in a class diagram represent both the main objects and or interactions in the application and the objects.

4.3.5 Sequence Diagram:

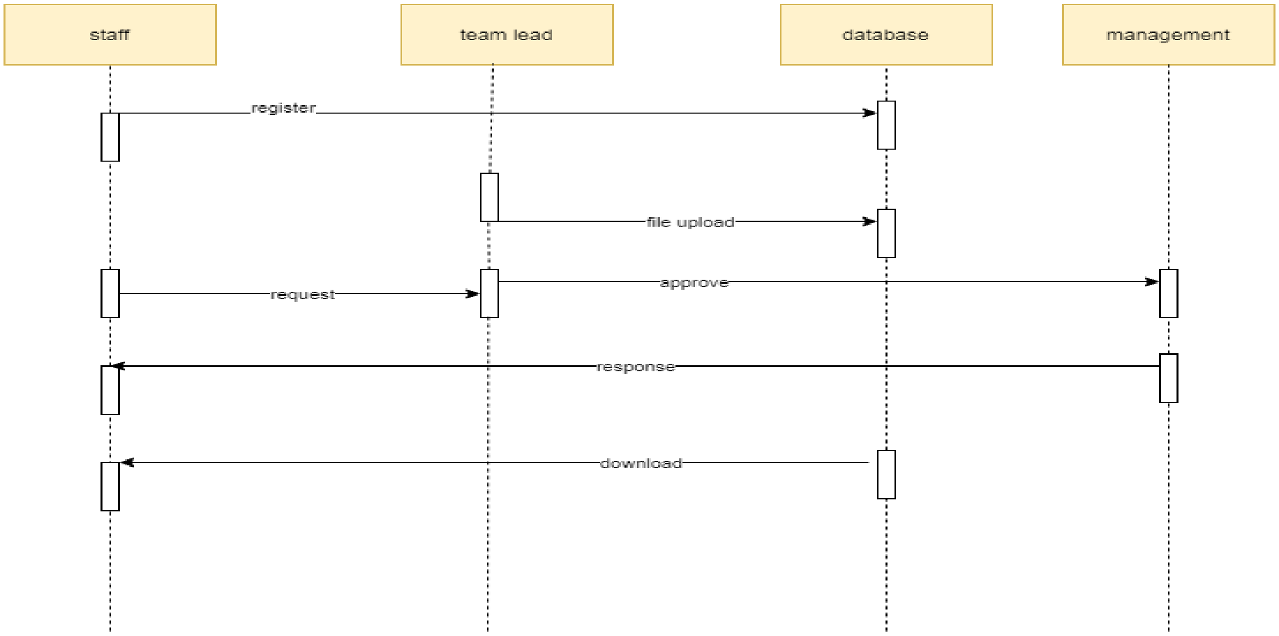


Fig 4.9 Sequence Diagram of Request and Grant Permission

EXPLANATION:

In our sequence diagram specifying processes operate with one another and in order. In our sequence diagram first propose. For this in our component diagram first propose a data. In this proposed method we are using Hash-Solomon Code Algorithm to encrypt the data.

4.3.6 Collaboration Diagram:

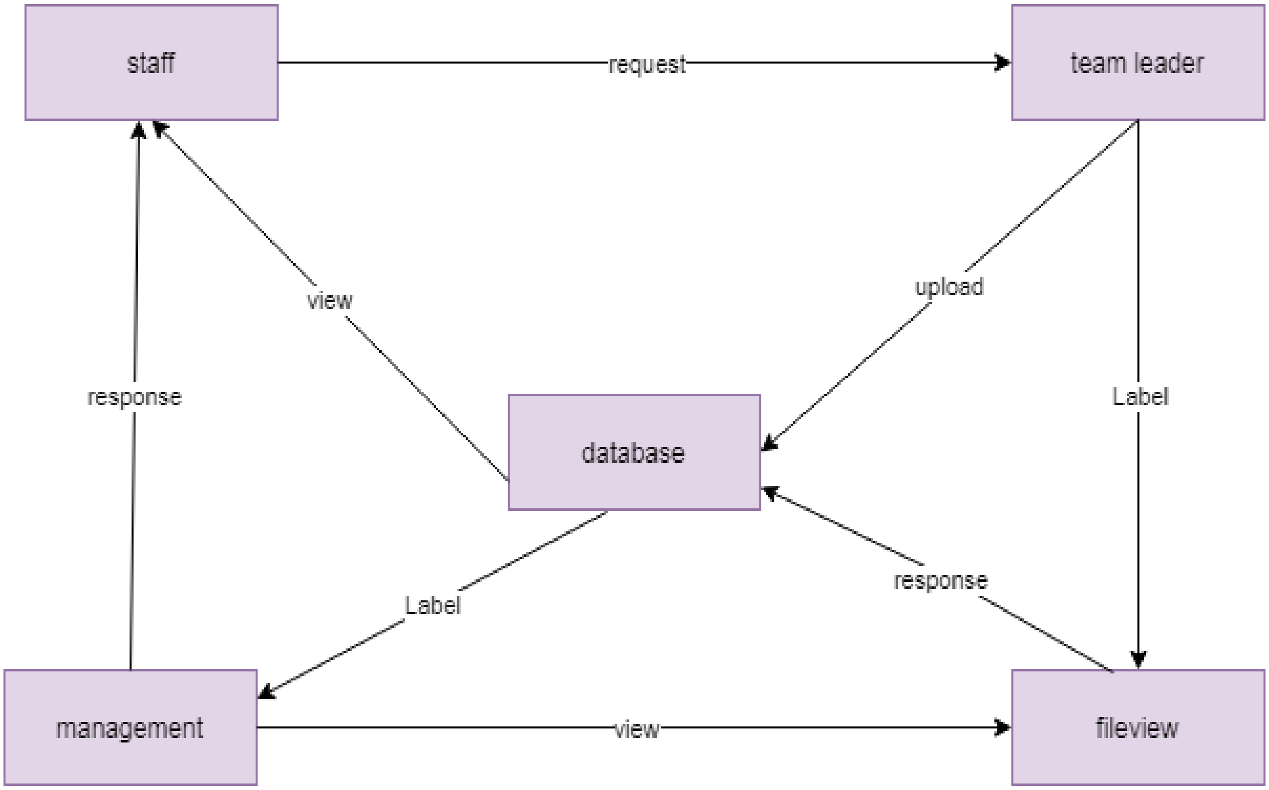


Fig 4.10 Collaboration diagram of responses

Explanation:

A collaboration is a structured classifier in which roles and attributes work together to define the classifier's internal structure. When you wish to define only the roles and connections that are essential to achieve a certain collaboration goal, you utilise a collaboration.

SYSTEM ARCHITECTURE

5.1 SYSTEM ARCHITECTURE

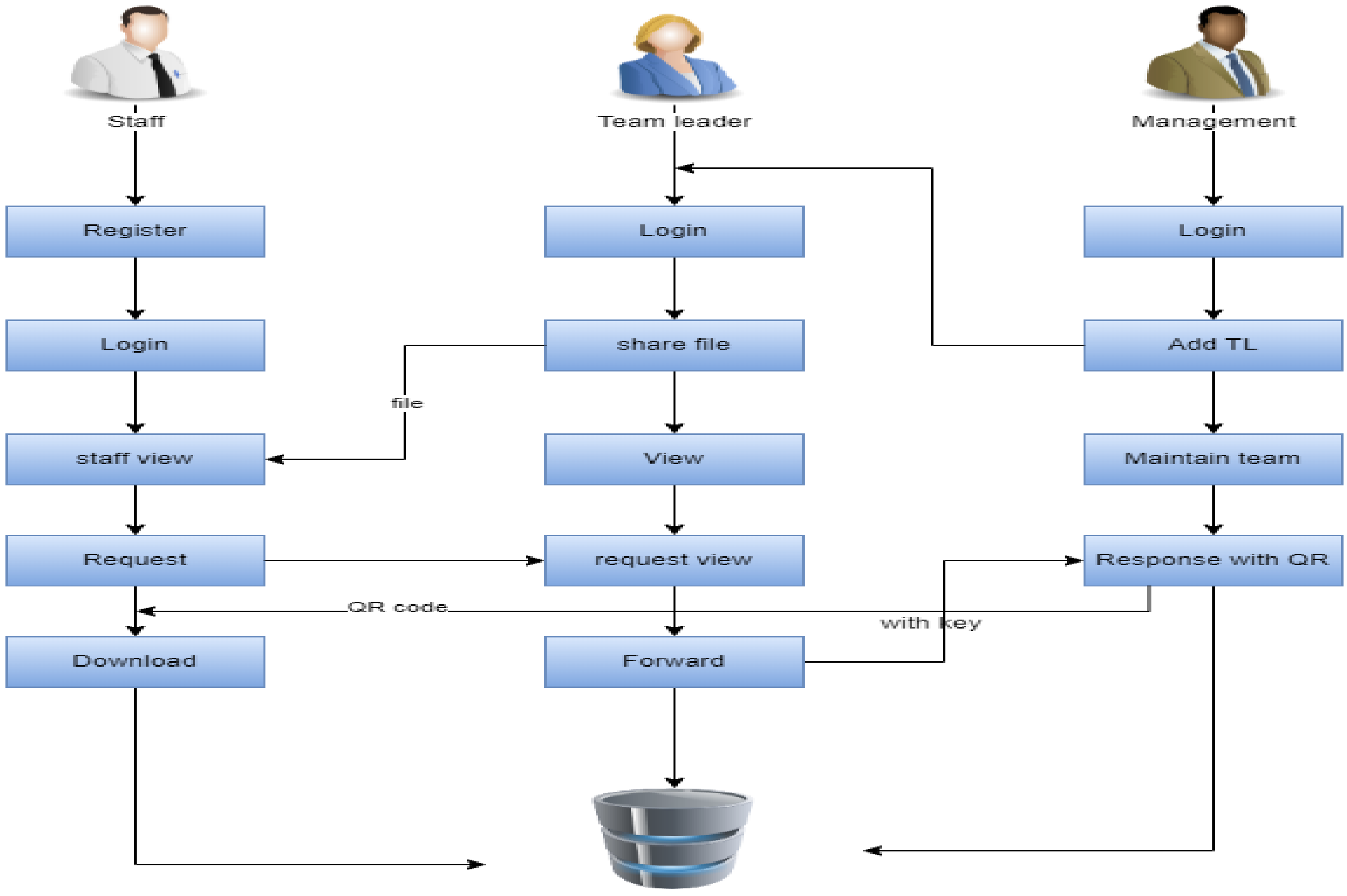


Fig 5.1 System Architecture diagram of Encryption-Decryption process

Explanation:

The frameworks planner lays out the essential construction of the framework, we propose a Hash code Solomon calculation and we can place a little piece of information in nearby machine and haze server to safeguard the security. Besides, in light of computational insight, this calculation can process the appropriation extent put away in cloud, haze, and nearby machine, individually. Through the hypothetical wellbeing examination and trial assessment, the practicality of our plan has been approved, which is actually a strong enhancement to existing distributed storage plot.

5.1 MODULE DESIGN SPECIFICATION:

SI.No	Module Name
1	Staff
2	Team leader
3	File encryption
4	Management
5	Hashing and QR generation
6	Permission grant and approval

5.1.1 STAFF

STAFF REGISTER:

The register module gives a reasonable structure to entering information on those staff such that: facilitates information passage and precision by matching the staff section to the information source (normally paper documents made at point of care), attaches effectively back to individual staff records to interface registers to staff information, and gathers information components to empower better management of gift programs.

STAFF LOGIN:

In this module in our venture, here represents a unit of work performed inside a data set administration framework (or comparative framework) against a data set, and treated in a reasonable and dependable way autonomous of different exchanges. An exchange for the most part addresses any adjustment of information base client will move the sum to supplier.

STAFF FILE VIEW:

In this module the staff will likewise see the group chief added record. What's more, examination the subtleties will be answerable for your document put away in data set.

STAFF FILE REQUEST:

In this module it is utilized to serve to the staff to Request for download document with the land longitude and the client will refresh the report alongside their perspective and the will be put away the data set.

STAFF FILE DOWNLOAD:

In this module the staff download the document after administration acknowledge the solicitation. It will be put away on neighborhood capacity.

5.1.2 TEAM LEADER

TEAM LEADER LOGIN:

In this module in our undertaking, here represents a unit of work performed inside an information base administration framework (or comparable framework) against a data set, and treated in a lucid and dependable way autonomous of different exchanges. An exchange by and large addresses any adjustment of data set client will move the sum to supplier.

TEAM LEADER FILE UPLOAD:

The group chief can then choose a document from their PC and tap the Upload button to present the record to the server. The Java record transfer Servlet will then, at that point, catch that document and persevere. It will be put away in information base.

TEAM LEADER FILE VIEW:

This module to assist us the staff with adding the record to the staffs. The information straightforwardly put away in data set. Then staff will see the transferred document.

5.1.3 FILE ENCRYPTION

The record to be gotten to by the staff is scrambled utilizing AES calculation. The document access authorization is mentioned by the staff part. The fractional decoding of the record happens just when the group chief gives the entrance key.

5.1.4 MANAGEMENT MODULE

MANAGEMENT LOGIN:

In this module in our undertaking, here represents a unit of work performed inside a database administration framework (or comparable framework) against a database, and treated in an intelligent and solid way autonomous of different exchanges. An exchange by and large addresses any adjustment of information base client will move the sum to supplier.

MANAGEMENT TEAM LEADER REGISTRATION:

The register module gives a reasonable structure to entering information in those group chief such that: facilitates information passage and exactness by matching the group chief section to the information source (generally paper documents made at point of care), attaches effectively back to individual group pioneer records to interface registers to group pioneer information, and gathers information components to empower better oversight of group programs.

5.1.5 HASHING AND QR GENERATION:

Hashing is intended to take care of the issue of expecting to find or store a thing in an assortment productively. Note: SHA calculation is utilized here to create hash code while a solicitation is given to track down a specific record from an information base. Since the consent demand contrasts starting with one staff then onto the next , different hash codes are produced making the entrance award incorporated QR code age happens when the client needs the endorsement for access of a document by the executives. QR code age is finished utilizing Jquery.

5.1.6 PERMISSION GRANT AND APPROVAL:

MANAGEMENT GENERATE KEY:

In this module the administration produce key for the staff demand. Since the key for the security reason. After get the key from the board the staff will download the document with key.

MANAGEMENT RESPONSE:

In this module the bank will reaction the information document completely examined information in classification wise view Bank will be answerable for your record put away in data set.

MODULE DIAGRAM:

STAFF REGISTER:

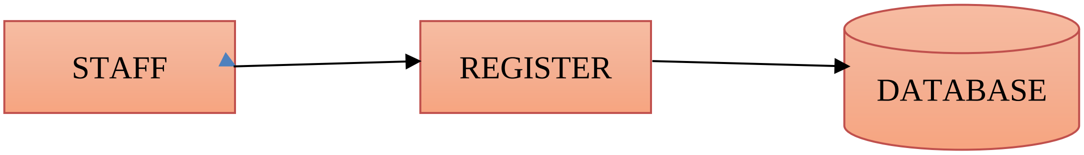


Fig 5.2 Staff Register process

STAFF LOGIN:

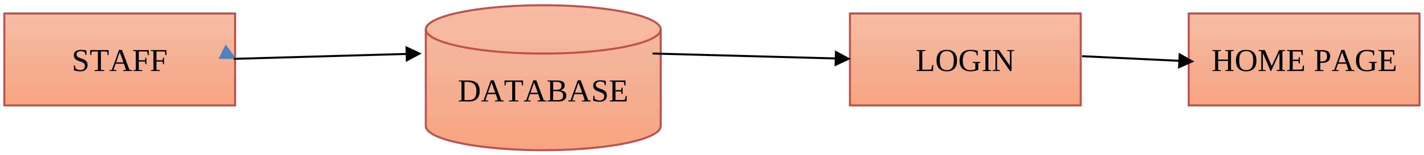


Fig 5.3 Staff Login Process

STAFF FILE VIEW:

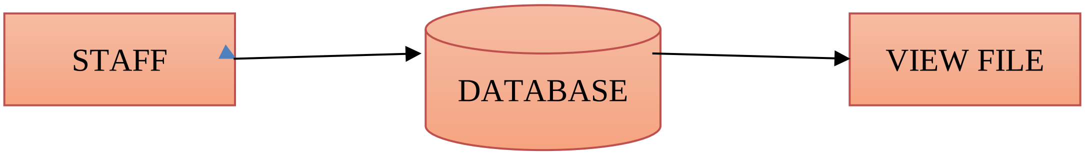


Fig 5.4 Staff File view process

STAFF FILE REQUEST:

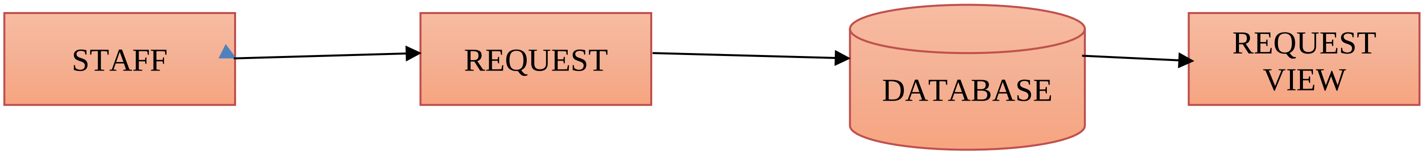


Fig 5.5 Staff file request process

STAFF FILE DOWNLOAD:

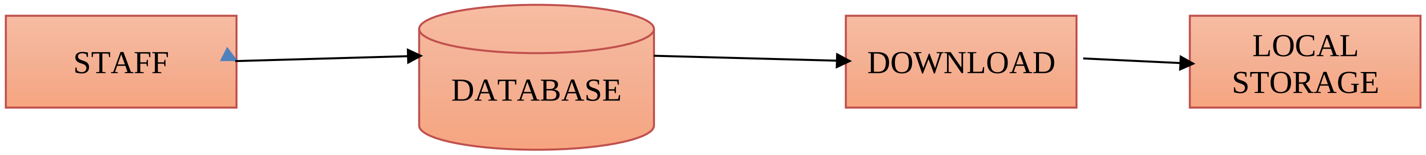


Fig 5.6 Staff file download

TEAM LEADER LOGIN:

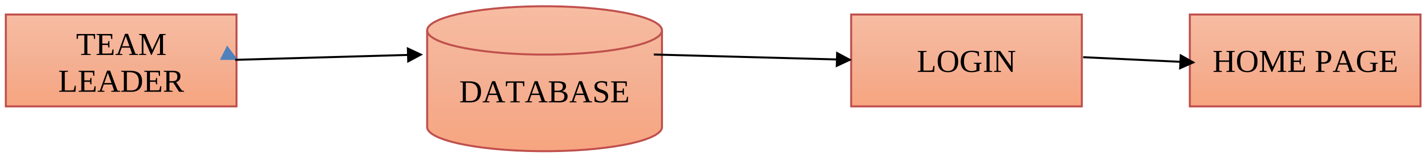


Fig 5.7 Team leader login

TEAM LEADER FILE UPLOAD:

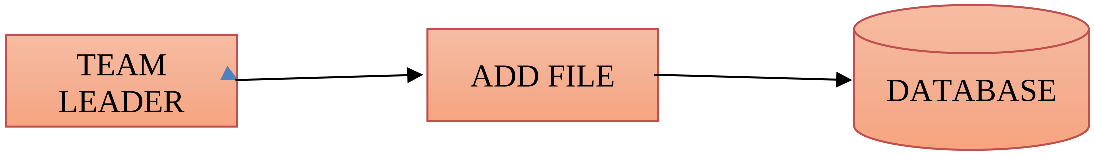


Fig 5.8 Team leader file upload process

TEAM LEADER FILE VIEW:

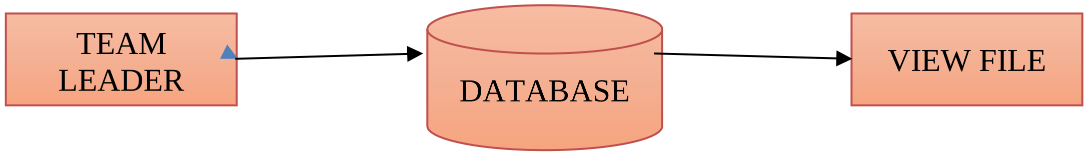


Fig 5.9 Team leader file view

MANAGEMENT LOGIN:

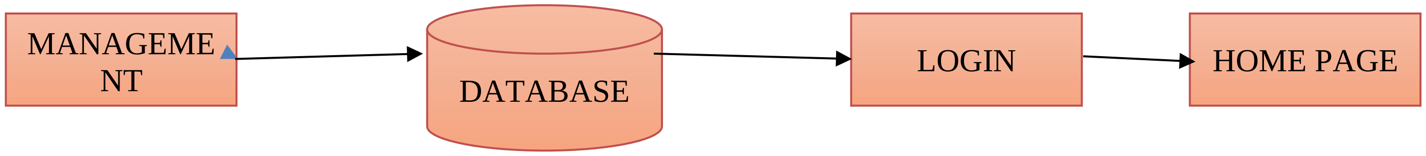


Fig 5.10 Management Login

MANAGEMENT TEAM LEADER REGISTRATION:

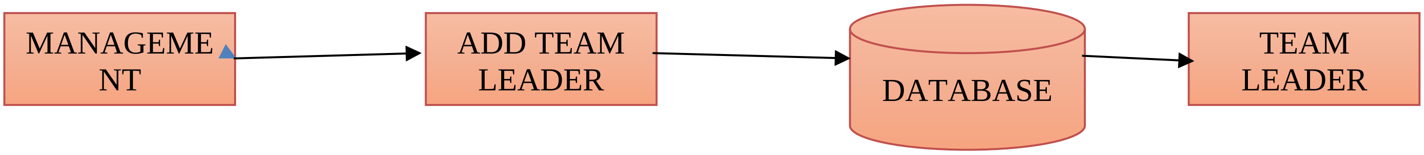


Fig 5.11 Management – Team leader registration

MANAGEMENT GENERATE KEY:

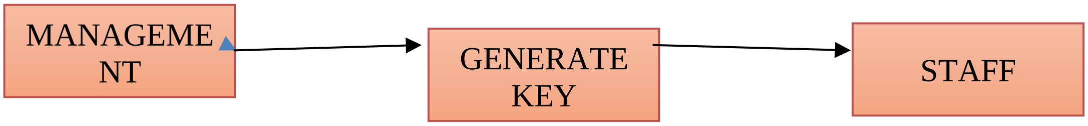


Fig 5.12 Management key generation

MANAGEMENT RESPONSE:

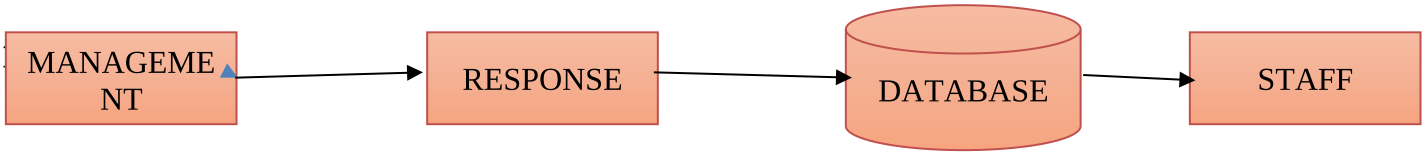


Fig 5.13 Management approval

5.2 ALGORITHMS:

SHA ALGORITHM:

In the area of cryptography and sepulcher examination, the SHA-1 calculation is a tomb designed hash work that is utilized to take a more modest info and produces a string that is 160 pieces, otherwise called 20-byte hash esteem long. The hash esteem in this way created, is known as a message digest which is commonly delivered and created as a hexadecimal number which is explicitly 40 digits in length.

Characteristics:

- The cryptographic hash capacities are used and used to keep and store the got type of information by giving three various types of qualities, for example, pre-picture opposition, which is otherwise called the principal level of picture obstruction, the second degree of pre-picture opposition and impact obstruction.

- The foundation lies in the way that the pre-picture tomb opposition procedure makes it hard and additional tedious for the programmer or the aggressor to track down the first expected message by giving the particular hash esteem.

- The security, in this way, is given by the idea of a one way that has a capacity that is generally the vital part of the SHA calculation. The pre-picture obstruction is critical to tidy up beast force assaults from a bunch of colossal and strong machines.

- Also, the second opposition strategy is applied where the assailant struggles with disentangling the following mistake message in any event, when the primary level of the message has been unscrambled. The last and generally challenging to break is the crash opposition, making it incredibly difficult for the aggressor to find two totally various messages which hash to a similar hash esteem.

- Hence, the proportion to the quantity of sources of info and the results ought to be comparative in design to consent to the categorize guideline. The impact opposition suggests that finding two distinct arrangements of information sources that hash to a similar hash is incredibly troublesome and along these lines denotes its security.

Uses of SHA Algorithm:

These SHA calculations are broadly utilized in security conventions and applications, including the ones like TLS, PGP, SSL, IPsec, and S/MiME. These likewise find their place in all most of cryptanalytic strategies and coding norms which is principally planned to see the working and working of significantly all administrative as well as confidential associations and establishments. Significant monsters today like Google, Microsoft, or Mozilla have begun to suggest the utilization of SHA-3 and stop the use of the SHA-1 calculation.

AES ALGORITHM:

The AES calculation (otherwise called the Rijndael calculation) is a balanced square code calculation that takes plain text in squares of 128 pieces and converts them to encode text utilizing keys of 128, 192, and 256 pieces. Since the AES calculation is thought of as secure, it is in the overall norm.

How does AES work?

The AES calculation utilizes a replacement change, or SP organization, with different rounds to deliver figure text. The quantity of rounds relies upon the key size being utilized. A 128-digit key size directs ten adjusts, a 192-piece key size directs 12 rounds, and a 256-bit key size has 14 rounds. Every one of these rounds requires a round key, however since only one key is inputted into the calculation, this vital should be extended to get keys for each round, including cycle 0.

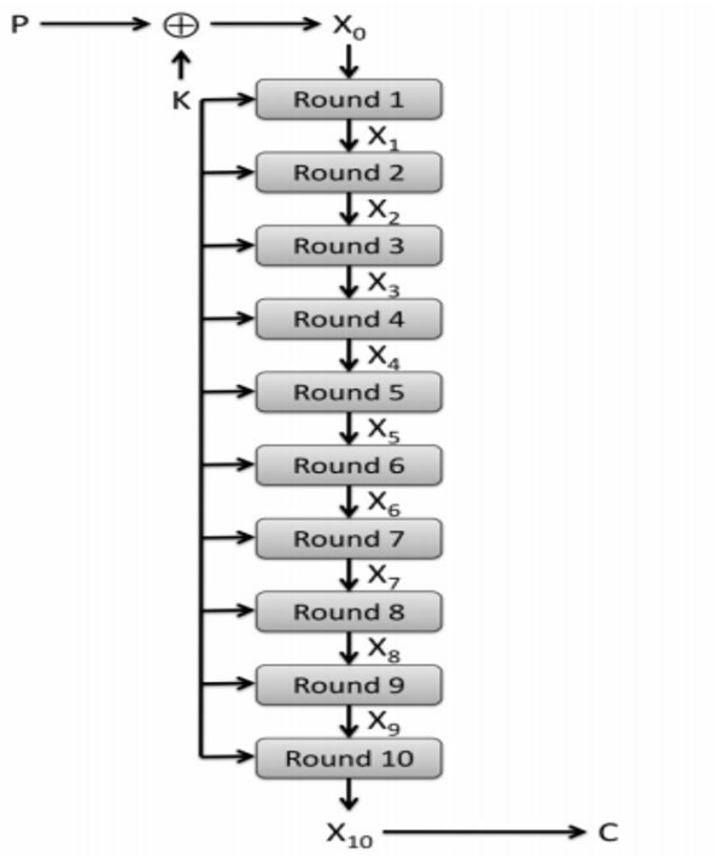
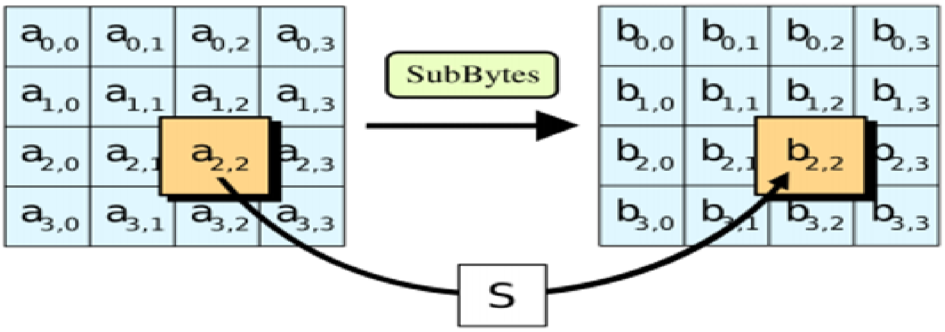


Fig 5.14 Round key generation

1. Substitution of the bytes

In the initial step, the bytes of the square text are subbed in view of rules directed by predefined S-boxes (short for replacement boxes).


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

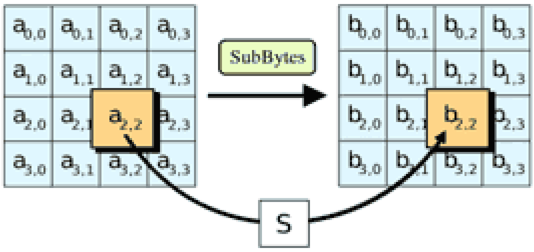

SubBytes
S
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig 5.15 Substitution of bytes

2. Shifting the rows

Next comes the stage step. In this progression, all lines aside from the first are moved by one, as displayed beneath.

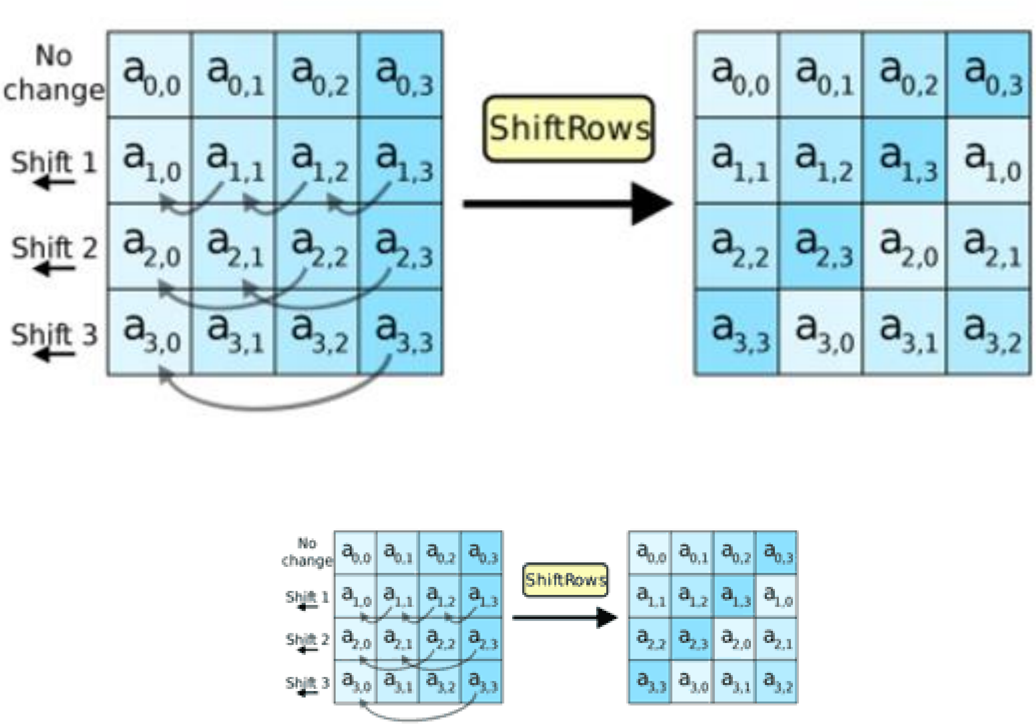

No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig 5.16 Shifting the rows

3. Mixing the columns

In the third step, the Hill cipher is utilized to muddle up the message more by blending the square's segments.

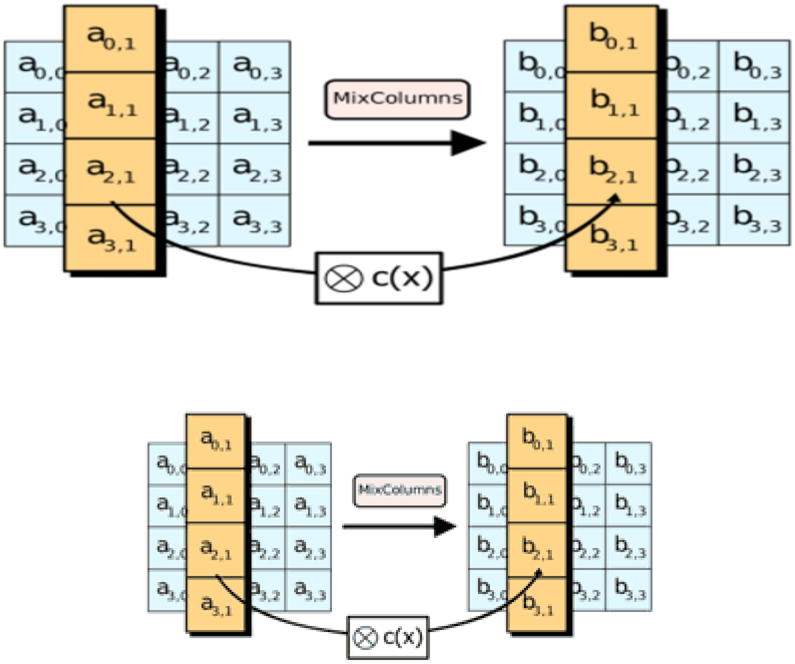

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig 5.17 Mixing the columns

4. Adding the round key

In the last advance, the message is XORed with the separate round key.

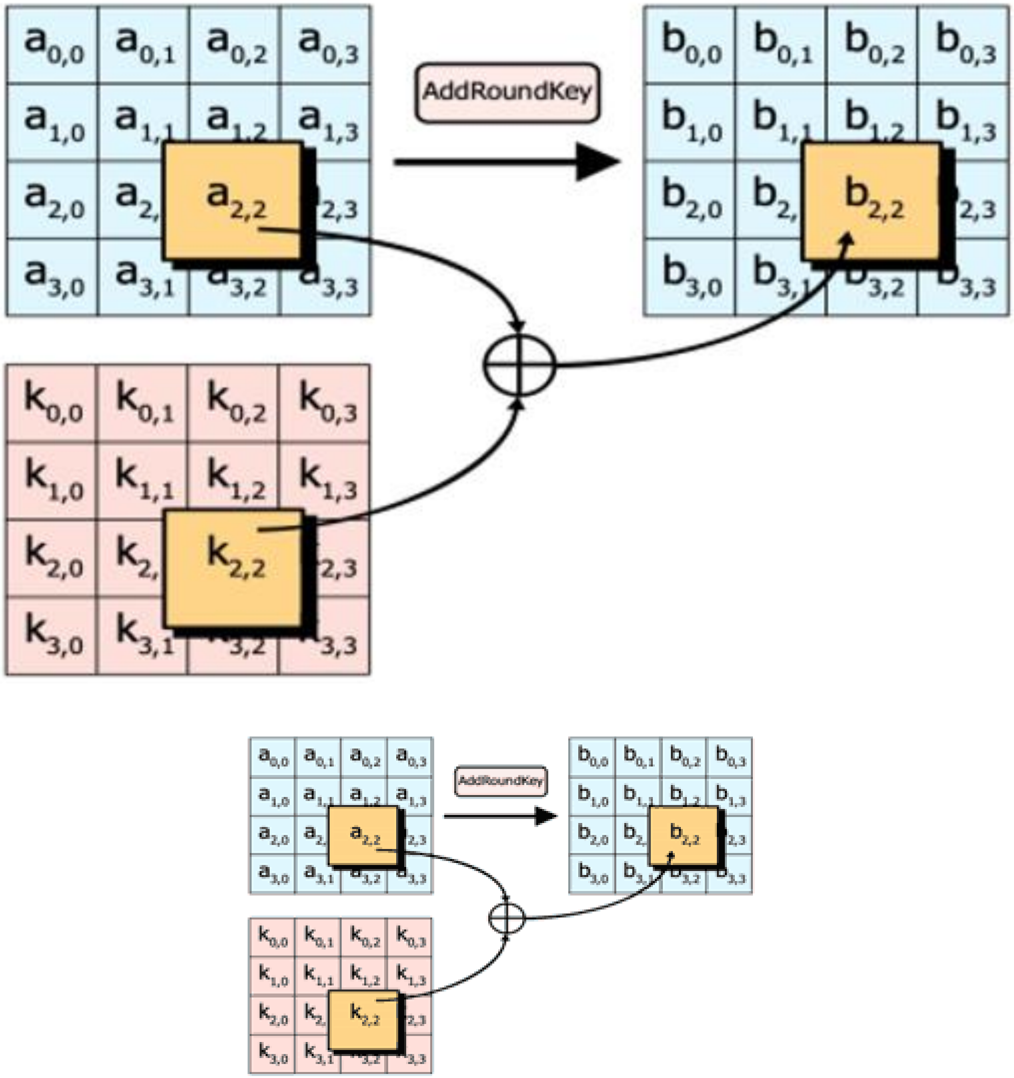

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Fig 5.18 Round key addition

When done over and again, these means guarantee that the last ciphertext is secure.

SYSTEM IMPLEMENTATION

6.1 CLIENT-SIDE CODING

Index.jsp:

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"

    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
      <link rel="stylesheet" href="css/bootstrap.min.css">

        <script type="text/javascript" src="js/jquery.min.js"></script>
        <script type="text/javascript" src="js/bootstrap.min.js"></script>
</head>

<style>
html, body, #main {
  font-size: 16px;
  width: 100%;
  height: 100%;
  background-image:url("image/bu.jpg");
  background-size:cover;
}
#main{

  overflow: auto;
  box-sizing: border-box;
  padding-top:2rem;
}

.navbar{
  background-color:#222;
  border:1px solid grey;
  z-index: 1;
 position:absolute;
```

```
  top:50%;
  left:50%;
  transform:translate(-50%,-50%);
  box-shadow: 1px 1px 5px rgba(0,0,0,.5);
}

.navbar-default .navbar-nav > li > a{
  color:#fff;
  padding:15px 15px;
  outline:none;
}

.navbar-nav>li>.dropdown-menu {
  border-radius:6px;
}

.navbar-default .navbar-nav > li > a:hover{
  color:#121212;
  background-color:#fff;
}

.navbar-default .navbar-nav>.open>a, .navbar-default .navbar-nav>.open>a:focus,
.navbar-default .navbar-nav>.open>a:hover {
    color: #fff;
    background-color: #000;

}

.dropdown-menu>li>a:hover {
    color: #c9c3c3;
    text-decoration: none;
    background-color: #121212;
}

.navbar-default .navbar-nav>.active>a, .navbar-default .navbar-nav>.active>a:focus,
.navbar-default .navbar-nav>.active>a:hover {
    color: #fff;
    background-color: #d71919;
}
```

```
.dropdown-menu>li>a {
    color: #000;
}

@media screen and (max-width:768px) and (min-width:100px) {

  .main{
    width:25%;
  }
 .navbar-default .navbar-nav > li > a {
    color: #fff;
    outline: none;
   overflow:hidden;
}
  .navbar {
  overflow:hidden;
    width:25%;
}
  .navbar ul li{
    position:relative;
  }
    .navbar ul li a{
      margin-left: 15px;

    }
    .navbar ul li:active {
   color:green;
    }


  .navbar-nav .open .dropdown-menu {
    position: static;
    float: none;
    width: auto;
    margin-top: 0;
    background-color: transparent;
    border: 0;
    -webkit-box-shadow: none;
    box-shadow: none;
}

.navbar-nav .open .dropdown-menu>li:hover a{

    background-color: transparent;
  margin-left:18px;
  color:#fff !important;

}
  .navbar-nav .open .dropdown-menu>li:hover:before{
    font:normal normal normal 14px/1 FontAwesome;
    content:'\f054';
     width:10px;
    height:10px;
    position:absolute;
    left:18%;
    top:46%;
    transform:translate(-50%,-50%);
    color:#e14444;


  }


  .navbar-default .navbar-nav .open .dropdown-menu>li>a {
    color: #e14444;
}
}

</style>
<body>
<div id="main">
<nav class="navbar navbar-default">
  <ul class="nav navbar-nav">
    <li><a href="#0">HOME</a></li>
    <li><a href="stafflogin.jsp">STAFFS</a></li>
    <li class="dropdown">
```

```
      <a href="#0" class="dropdown-toggle" data-toggle="dropdown" data-target="dropdown" role="button" aria-haspopup="true" aria-expanded="false">TEAM <span class="caret"></span></a>
      <ul class="dropdown-menu" id="dropdon-menu">
        <li><a href="teamleaderlogin.jsp">LOGIN</a></li>

      </ul>
    </li>
    <li class="dropdown">
      <a href="#0" class="dropdown-toggle" data-toggle="dropdown" data-target="dropdown" role="button" aria-haspopup="true" aria-expanded="false">MANAGEMENT<span class="caret"></span></a>
      <ul class="dropdown-menu" id="dropdon-menu">
        <li><a href="managementlogin.jsp">MANAGEMENT LOGIN</a></li>
        <!-- <li><a href="#0">Web Design</a></li>
        <li><a href="#0">Mobile App Development</a></li> -->
      </ul>
    </li>

  </ul>
</nav>
</div>
</body>

</html>
```

Teamleaderlogin.jsp:

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
</head>
<style>
body{
background-image:url("image/b4.jpg");
background-repeat:no-repeat;
background-size: 1370px  640px;

}
.myDiv {

  background-color: #fff5e600;
  border-radius: 1px;
  width:400px;
  height:280px;
  margin: auto;
  padding-top:30px;
  /* box-shadow: 25px 20px 20px #888888; */

}
.myDiv2 {
  font-size:25px;
  font-style: italic;
font-weight: bold;
color:red;
}
span{
color:black;
}
a{
text-decoration:none;
font-weight: bold;
color:black;
 font-size:25px;}
lable{
color:white;
font-size:25px;
}
</style>
<body>


<center>
<div class="myDiv2">
Team Leader Login
```

```
</div>
</center>
<br><br><br><br><br>
 <form action="teamlog" method="post">
<div class="myDiv">
<center>

   <lable> Team Name:</lable><br><br>
   <select name="teams" id="cars" style="width:280px;height:40px;border-radius: 
1px;text-align:center;"><br><br>>
_<option value="Team A">Team A</option>
  <option value="Team B">Team B</option>
  <option value="Team C">Team C</option>
  <option value="Team D">Team D</option>

</select><br><br>
<lable> Password     :</lable><br><br>
  <input type="password" name="pass" placeholder="Password" 
style="width:280px;height:40px;border-radius: 1px;text-align:center;"><br><br>
  <input type="submit" value="Submit" style="width:100px;height:40px;border-
radius: 1px;"><br><br>

 <a href="teamleaderreg.jsp">REGISTER HERE!!!</a>
  </center>
</div>

 </form>
</body>

</html>
```

Upload.jsp:

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" 
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
```

```
</head>
<style>
body{
background-image:url("image/b4.jpg");
background-repeat:no-repeat;
background-size: 1370px  640px;

}
.myDiv {

  background-color: #fff5e600;
  border-radius: 1px;
  width:400px;
  height:280px;
  margin: auto;
  padding-top:30px;
  /* box-shadow: 25px 20px 20px #888888; */

}
.myDiv2 {
  font-size:25px;
  font-style: italic;
font-weight: bold;
color:red;
}
span{
color:black;
}
a{
text-decoration:none;
font-weight: bold;
color:black;
 font-size:25px;}
lable{
color:white;
font-size:25px;
}
</style>
<body>
```

```
<center>
<div class="myDiv2">
```

6.2 SERVER-SIDE CODING:

```
Block.java;
package servlet;

import java.util.Date;

import servlet.StringUtil;

public class Block {

	public String hash;
	public String previousHash;
	private String data; //our data will be a simple message.
	private long timeStamp; //as number of milliseconds since 1/1/1970.

	public Block(String data,String previousHash ) {
		this.data = data;
		this.previousHash = previousHash;
		this.timeStamp = new Date().getTime();
		this.hash = calculateHash(); //Making sure we do this after we set
the other values.
	}
```

```
    public String calculateHash() {
        String calculatedhash = StringUtil.applySha256(
                previousHash +
                Long.toString(timeStamp) +
                data
                );
        return calculatedhash;
    }
}
```

AES.java;

```
  package servlet;
import java.security.Key;

import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

import sun.misc.*;

public class AES
{
private static String algorithm = "AES";
private static byte[] keyValue=new byte[]
{ 'A', 'S', 'e', 'c', 'u', 'r', 'e', 'S', 'e', 'c', 'r', 'e', 't', 'K', 'e', 'y' };

   // Performs Encryption
   public static String encrypt99(String plainText) throws Exception
   {
        Key key = generateKey();
        Cipher chiper = Cipher.getInstance(algorithm);
        chiper.init(Cipher.ENCRYPT_MODE, key);
        byte[] encVal = chiper.doFinal(plainText.getBytes());
        String encryptedValue = new BASE64Encoder().encode(encVal);
        return encryptedValue;
    }

    // Performs decryption
    public static String decrypt(String encryptedText) throws Exception
    {
        // generate key
        Key key = generateKey();
        Cipher chiper = Cipher.getInstance(algorithm);
        chiper.init(Cipher.DECRYPT_MODE, key);
        byte[] decordedValue = new
BASE64Decoder().decodeBuffer(encryptedText);
        byte[] decValue = chiper.doFinal(decordedValue);
        String decryptedValue = new String(decValue);
        return decryptedValue;
    }

//generateKey() is used to generate a secret key for AES algorithm
    private static Key generateKey() throws Exception
    {
        Key key = new SecretKeySpec(keyValue, algorithm);
        return key;
    }
```

```
}
```

Staffreg.java;

```
package servlet;

import imple.imple;
import inter.inter;

import java.io.IOException;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import bean.stafregbean;

/**
 * Servlet implementation class staffreg
 */
@WebServlet("/staffreg")
public class staffreg extends HttpServlet {
	private static final long serialVersionUID = 1L;

    /**
     * @see HttpServlet#HttpServlet()
     */
    public staffreg() {
        super();
        // TODO Auto-generated constructor stub
    }
          /**
           * @see HttpServlet#doGet(HttpServletRequest request,
HttpServletResponse response)
           */
          protected void doGet(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
                    // TODO Auto-generated method stub
          }

          /**
           * @see HttpServlet#doPost(HttpServletRequest request,
HttpServletResponse response)
           */
          protected void doPost(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
                    // TODO Auto-generated method stub

                    String name=request.getParameter("name");
                    System.out.println("name"+name);

                    String team=request.getParameter("teams");
                    System.out.println("team"+team);

                    String email=request.getParameter("email");
                    System.out.println("email"+email);
                    String number=request.getParameter("number");
                    System.out.println("number"+number);

                    String pass=request.getParameter("pass");
                    System.out.println("pass"+pass);

                    String cpass=request.getParameter("cpass");
                    System.out.println("cpass"+cpass);

                    stafregbean s=new stafregbean();
                    s.setName(name);
                    s.setTeam(team);
                    s.setEmail(email);
                    s.setNumber(number);
                    s.setPass(pass);
                    s.setCpass(cpass);

                    inter n=new imple();
                    int b=n.reg(s);
                    if(b==1){
                        response.sendRedirect("stafflogin.jsp");
                    }
                    else{
                        response.sendRedirect("error.jsp");
                    }
          }
}
```

Dbcon.java;

```
package dbcon;

import java.sql.Connection;
import java.sql.DriverManager;



public class dbcon {
	static Connection con;

	public static Connection create()
	{
	try
	{
		Class.forName("com.mysql.jdbc.Driver");

	con=DriverManager.getConnection("jdbc:mysql://localhost:3306/team","root","root");

	}catch(Exception e)
	{
		e.printStackTrace();
	}

	return con;
	}}
```

PERFORMANCE ANALYSIS

7.1 RESULTS AND DISCUSSIONS

This paper proposes a strategy for secure information exchange among associations and its representatives. In this framework, information is moved among prevalent and delegates utilizing a solid convention. The exchange of documents and information is confirmed. Encryption calculations have expanded the effectiveness of safety and genuineness. Blockchain system forced the usefulness of the hash capacity to additional increment secure information exchange. In this way, the target of the proposed framework is carried out.

7.2 TESTCASES AND REPORTS

TESTCASE OBJECTIVES:

- Team Leader new registration.
- New document upload.
- File decryption.

TESTCASE	TESTCASE NAME	EXPECTED OUTPUT	ACTUAL OUTPUT	RESULT (Pass/ Fail)
TC01	Team Leader new registration	Team Leader added to database	New member added to database	Pass (Fig.A5)
TC02	New document upload	Document added to database (encrypted)	Employee can view document added to database	Pass (Fig.A8)

TC03	File decryption	Access Keys generation	File decrypted and downloaded	Pass (Fig.A9)

REPORTS:

All the testcases (TC01, TC02, TC03) have passed and the proof of the actual output is added below in the appendices column (Fig.A5, Fig.A8, Fig.A9).

.

CONCLUSION

8.1 CONCLUSION:

Information awareness concerns data that ought to be safeguarded from unapproved access or divulgence because of its delicate nature. For some's purposes, that may be Team pioneer, Staff subtleties records. Delicate information is private data that should be remained careful and far away from all untouchables except if they have consent to get to it. Admittance to delicate information ought to be restricted through adequate information security and data security rehearses intended to forestall.

8.2 FUTURE ENHANCEMENTS:

1. Implementing a certifiable unknown information base framework.
2. Improving the proficiency of conventions, as far as number of messages traded and concerning their sizes, too.
3. Implement utilizing two are more calculations.

APPENDICES

A1 SAMPLE SCREENS

Home page:

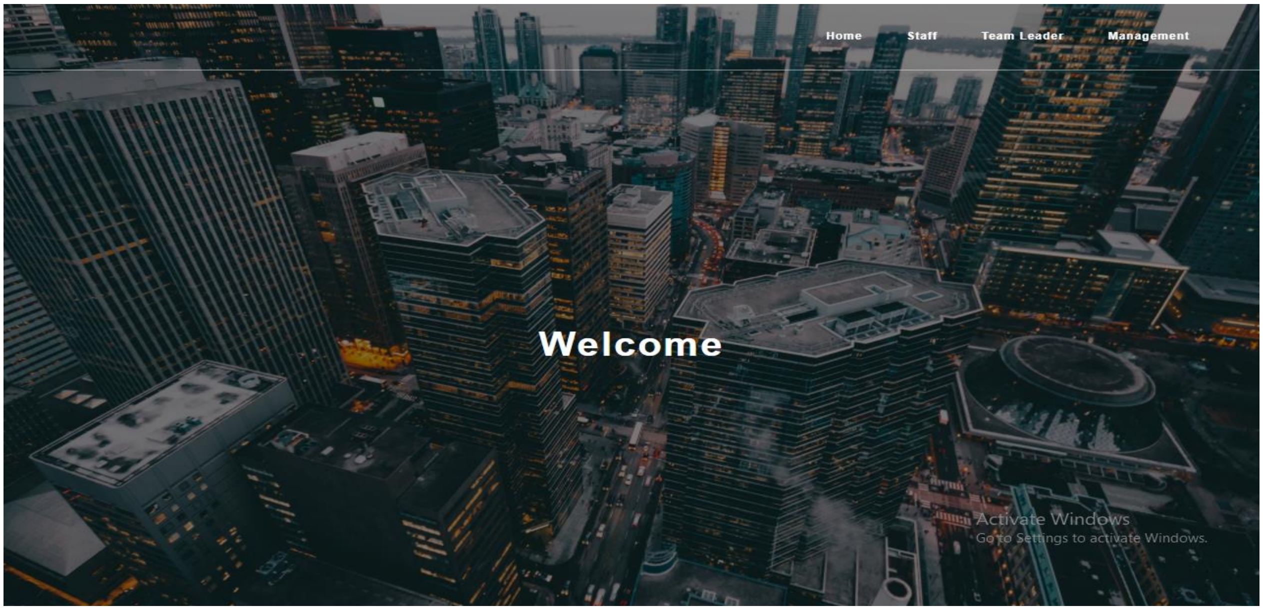


Fig A1 Home page

Team Leader Login Page:

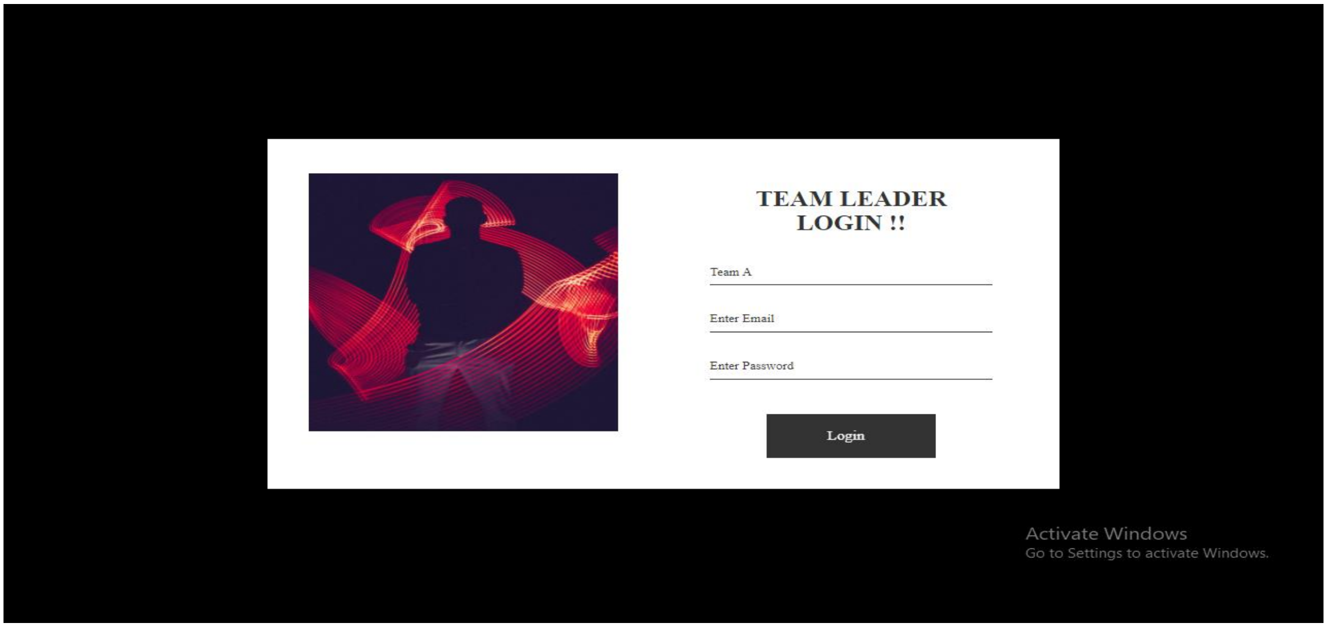


Fig A2 Team Leader Login page

Management Login Page:

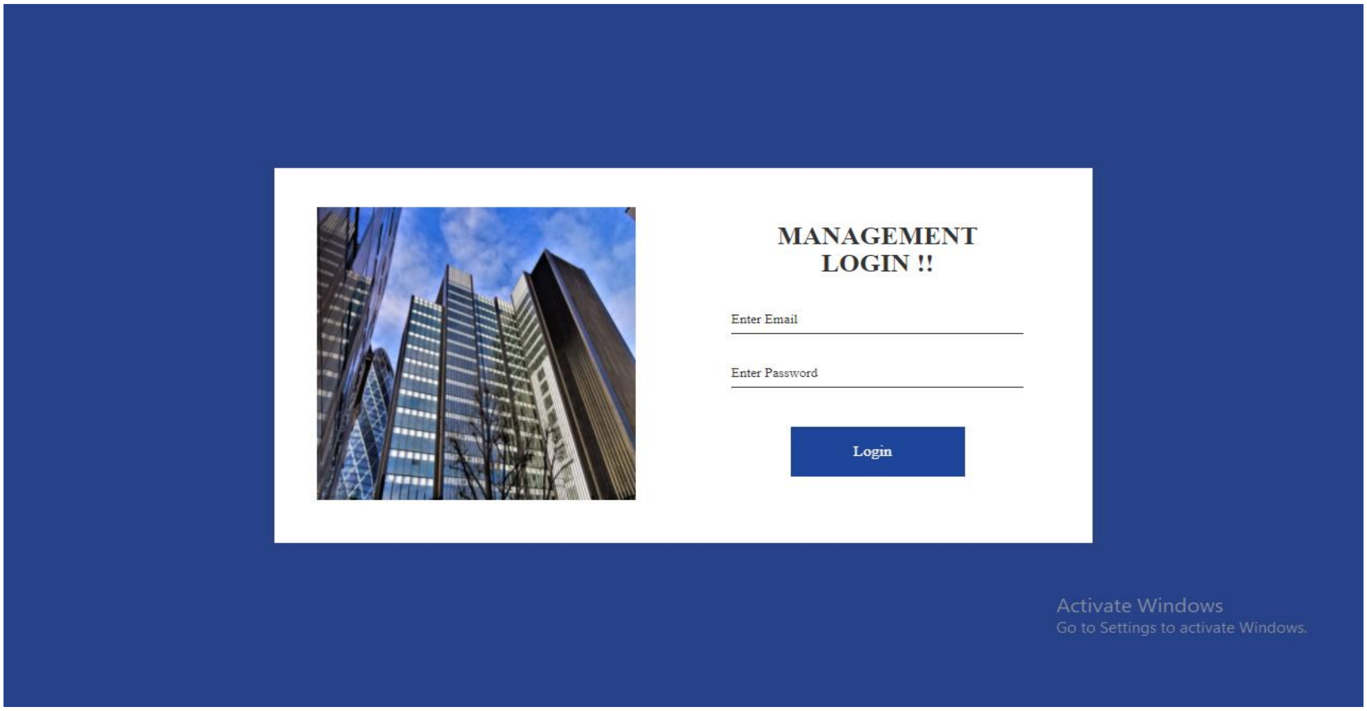
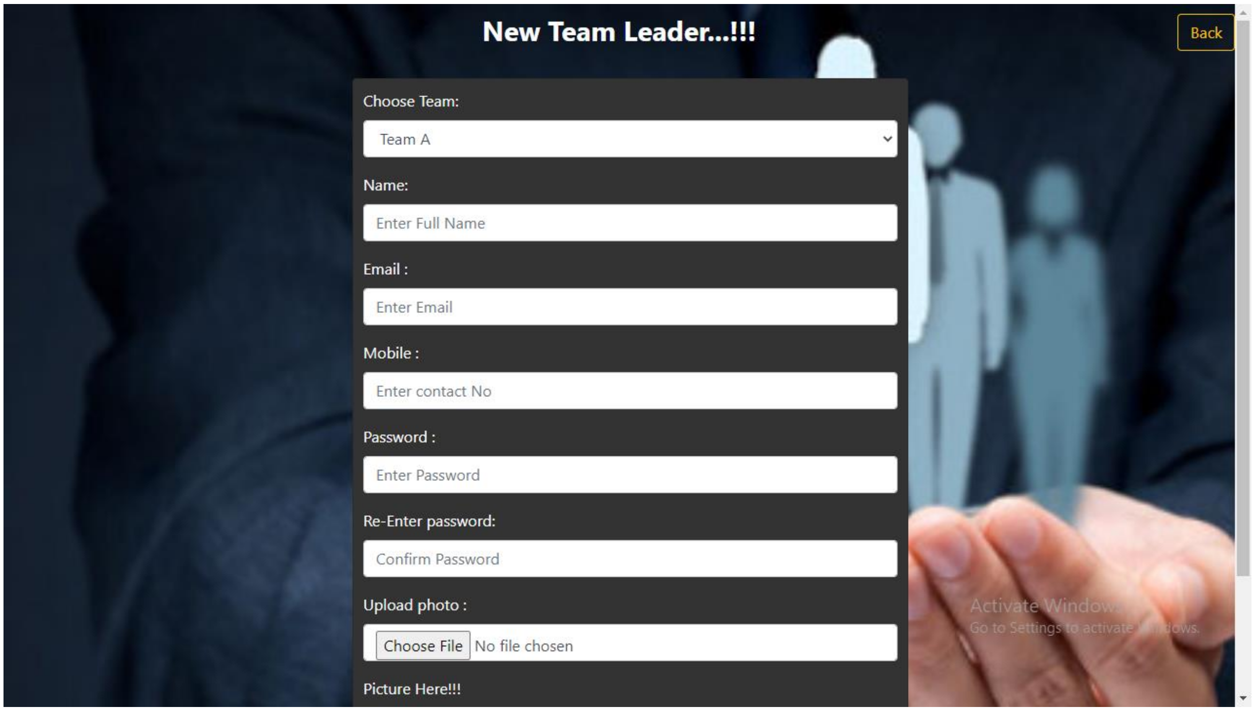


Fig A3 Management login page

Team Leader Add Page:



New Team Leader...!!!

Choose Team: Team A

Name: Enter Full Name

Email : Enter Email

Mobile : Enter contact No

Password : Enter Password

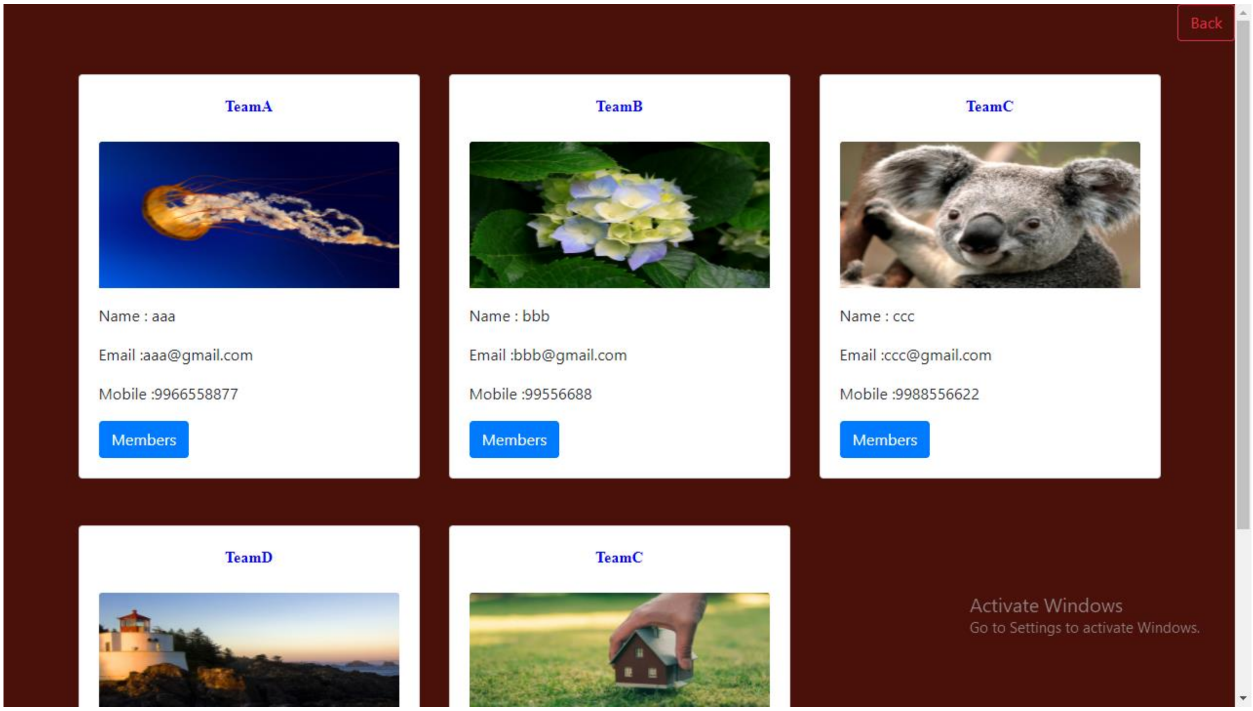
Re-Enter password: Confirm Password

Upload photo : No file chosen

Picture Here!!!

Fig A4 Team Leader Add Page

Team View Page:



TeamA

Name : aaa

Email :aaa@gmail.com

Mobile :9966558877

TeamB

Name : bbb

Email :bbb@gmail.com

Mobile :99556688

TeamC

Name : ccc

Email :ccc@gmail.com

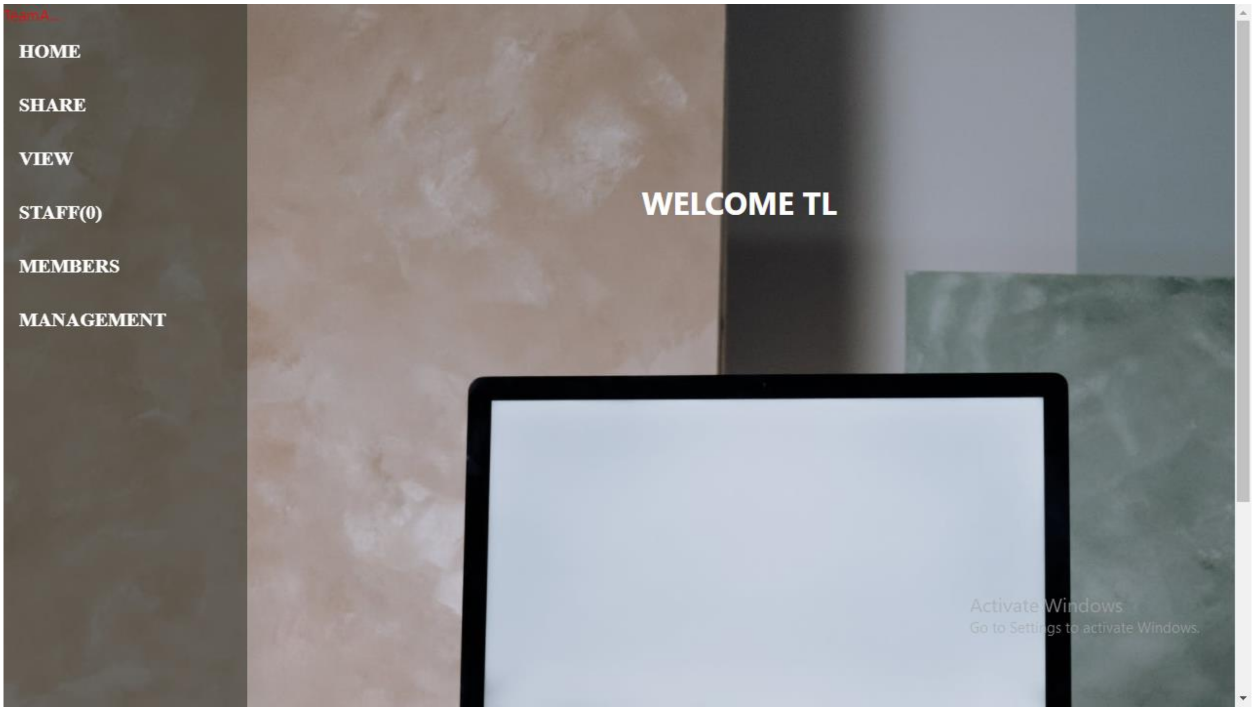
Mobile :9988556622

TeamD

TeamC

Fig A5 Team View Page

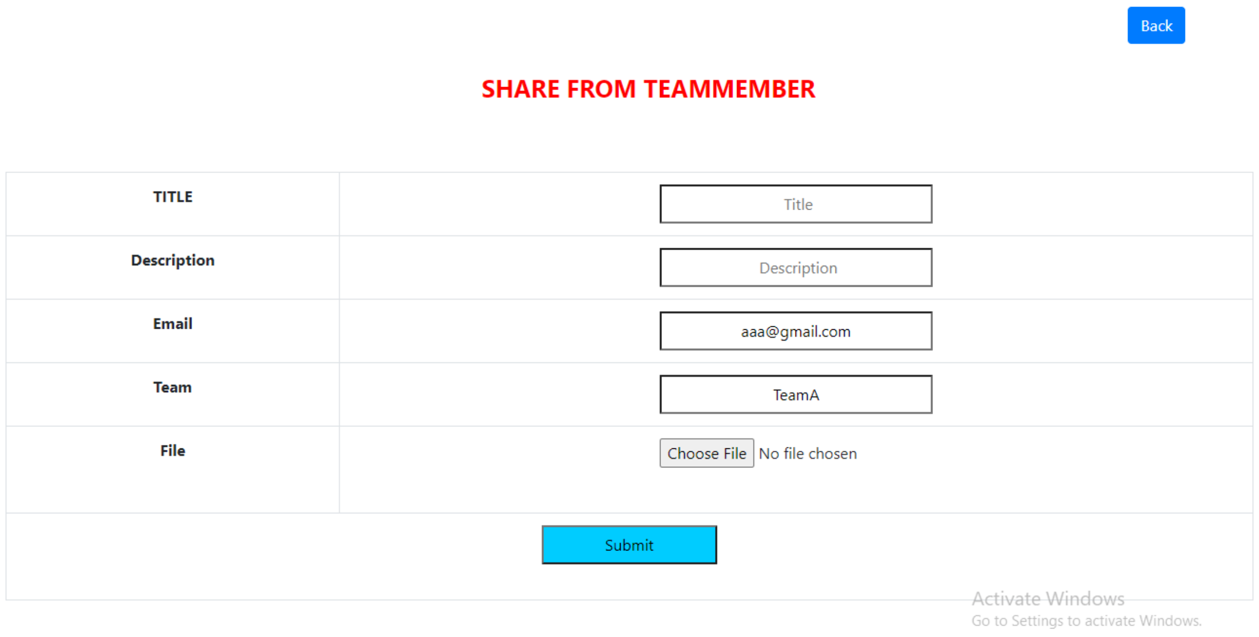
Team Leader Home Page:



WELCOME TL

Fig A6 Team Leader home page

Team leader file Share page:

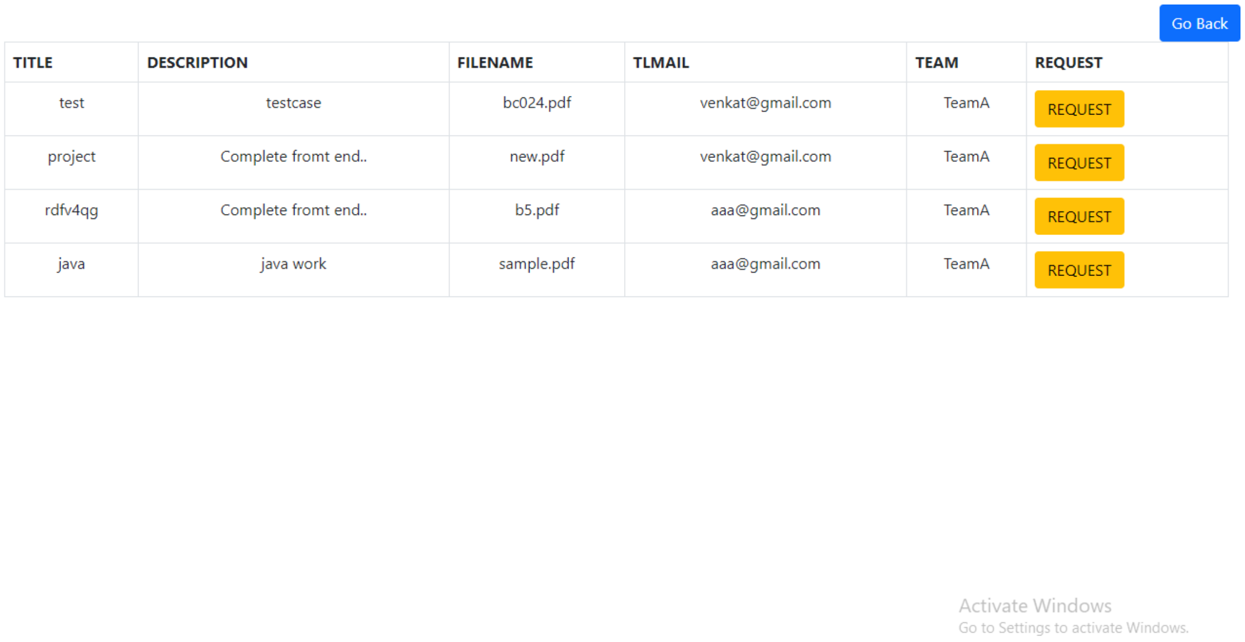


SHARE FROM TEAMMEMBER

TITLE	Title
Description	Description
Email	aaa@gmail.com
Team	TeamA
File	Choose File No file chosen

Fig A7 Team Leader file share page

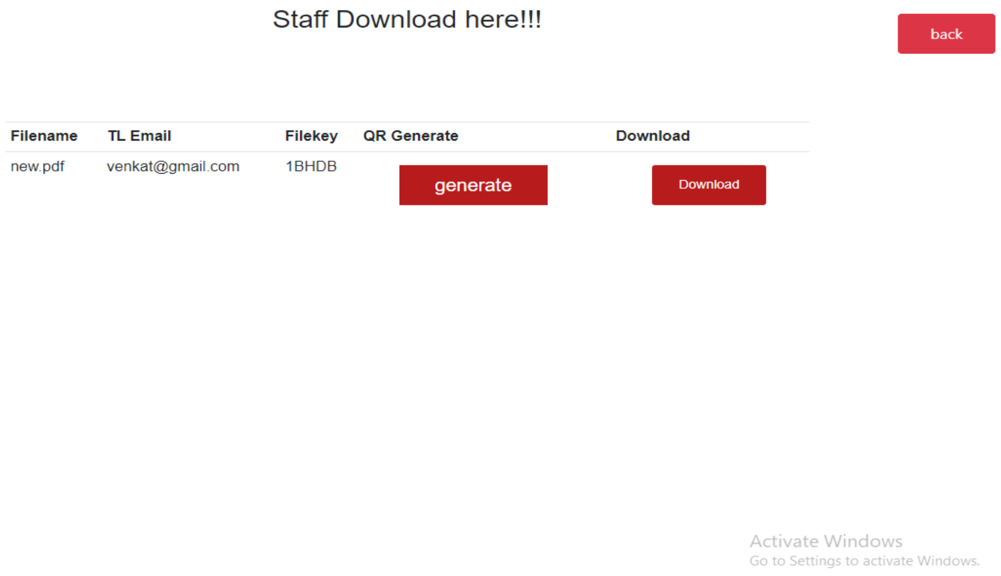
Employee File View Page:



TITLE	DESCRIPTION	FILENAME	TLMAIL	TEAM	REQUEST
test	testcase	bc024.pdf	venkat@gmail.com	TeamA	REQUEST
project	Complete fromt end..	new.pdf	venkat@gmail.com	TeamA	REQUEST
rdfv4qg	Complete fromt end..	b5.pdf	aaa@gmail.com	TeamA	REQUEST
java	java work	sample.pdf	aaa@gmail.com	TeamA	REQUEST

Fig A8 Employee File View page

Employee Download page:



Staff Download here!!!

Filename	TL Email	Filekey	QR Generate	Download
new.pdf	venkat@gmail.com	1BHDB	generate	Download

Fig A9 Employee download page

REFERENCES:

[1] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, vol. 6, no. 2, pp. 147-156, 2020.

[2] D. Liu and J. Lee, “CNN based Malicious Website Detection by Invalidating Multiple Web Spams,” *IEEE Access*, vol. 8, no. 1, pp. 97258-97266, 2020.

[3] W. Martin, V. Friedhelm, and K. Axel, “Tracing manufacturing processes using blockchain-based token compositions,” *Digital Communications and Networks*, vol. 6, no 2, pp. 167-176, 2019.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, “Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6-14, 2018.

[5] L. Peng, W. Feng, and Z. Yan. (2020). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*. [Online]. Available: https://doi.org/10.1016/j.dcan.2020.05.008.

[6] N. Kakade and U. Patel, “Secure Secret Sharing Using Homomorphic Encryption,” in *Proc. 2020 11th International Conference on Computing, Communication and Networking Technologies*, 2020, pp. 1-7.

[7] S. Sundari and M. Ananthi, “Secure multi-party computation in differential private data with Data Integrity Protection,” in *Proc. 2015 International Conference on Computing and Communications Technologies*, 2015, pp. 180-184.

[8] S. Jiao, T. Lei, Y. Gao, Z. Xie and X. Yuan, “Known-Plaintext Attack and Ciphertext-Only Attack for Encrypted Single-Pixel Imaging,” *IEEE Access*, vol. 7, no.2, pp. 119557-119565, 2019.

[9] S. Kaushik, and S. Puri, “Online transaction processing using enhanced sensitive data transfer security model,” in *Proc. 2012 Students Conference on Engineering and Systems*, 2012, pp. 1-4.

[10] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, “NutBaaS: A Blockchain-as-a-Service Platform,” *IEEE Access*, vol. 7, pp. 134422-134433, 2019.

[11] F. Casino and C. Patsakis, “An Efficient Blockchain-Based Privacy-Preserving Collaborative Filtering Architecture,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1501-1513, Nov. 2020.

[12] D. Chkliaev, J. Hooman and P. van der Stok, “Mechanical verification of transaction processing systems,” in *Proc. ICFEM 2000. Third IEEE International Conference on Formal Engineering Methods*, 2000, pp. 89-97.

[13] S. Zhang, and J H. Lee. “Mitigations on Sybil-based Double-spend Attacks in Bitcoin,” *IEEE Consumer Electronics Magazine*, vol.7, no. 2, pp. 1-1, 2020.

[14] X. Wang, Q. Feng and J. Chai, “The Research of Consortium Block chain Dynamic Consensus Based on Data Transaction Evaluation,” in *Proc. 2018 11th International Symposium on Computational Intelligence and Design*, 2018, pp. 214-217.

[15] S. Zhang, and J. H. Lee, “A group signature and authentication scheme for blockchain-based mobile-edge computing,” *IEEE Internet of Things Journal*, vol. 7, no. 5, 4557-4565, 2019.