Acknoledgement

I would like to express my special thanks of gratitude to my teacher (Rujuta Mam)

as who gave me the golden opportunity

to do this wonderful project on the topic (Visual Cryptography for Biometric Privacy),

which also helped me in doing a lot of Research and i came to know about

so many new things I am really thankful to them.

Secondly i would also like to thank my parents and friends who helped me a lot in

finalizing this project within the limited time frame.

INDEX

ABSTRACT

Project Title - VISUAL CRYPTOGRAPHY FOR BIOMETRIC PRIVACY

Project Description - Bio-Metrics is the science of establishing the identity of an individual based on physical or behavioural traits such as face, fingerprints, iris, gait, and voice. A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., face image), extracting a feature set from the data (e.g., Eigen-coefficients), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The use of cryptography method we can easily encrypt and decrypt data. The template of a person in the database is generated during enrolment and is often stored along with the original raw data.

Modules - The system comprises of 2-major modules with their sub-modules.

1) Admin -

a) View/Edit/Delete - Can View/Update/Delete the added details from database.

b) View/Update - Can view all details of biometric and maintain accordingly.

2) Users –

a) Registration - User can register his detail.

b) Login - User login his account.

c) Home Page - User can visit their homepage.

d) Change Password - User can change their current password with new one.

Software Requirement –

- Windows 7 or higher
- Fire Base
- Android Studio or MIT App Inventor

Hardware Component –

- Processor – i3
- Hard Disk – 5GB
- Memory – 4GB
- Internet Connection

Chapter 1 - Introduction

1.1 Background -

Several years ago the manual method is used for maintain attendance like registers. The manual method founds lot of difficulties when generating the big number employees or students attendance, this makes the entire process time-consuming. There are many errors with the existing manual remarks in registers like absent & present. The manual method suffers from lot of set-backs such as time for record many registers and so on, making the process less time taken and minimum errors. All this leads to lot of errors like wrong place week off or present on week off, etc. it will directly effect in salary of employees. Due to usage of registers many student or employees miss use in the lecture or duty. Many times physically not present but presentty mark in registers.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system. Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994.

One such techniques is cryptography, which would help in protecting the information through encrypted text and these texts can be decrypted only by the specified person. The use of cryptography has begun much earlier than to be estimated certainly before four hundred decades in the form of hieroglyph by Egyptians to transfer the secret message to the kings. In today‟s world, we use cryptography for the secure transmission of data through internet channel but the disadvantage of using cryptography is that on both the end (sender and receiver) there should be a technical person which has paved way for visual cryptography, Where there is no need of the technical person in the receiver side because the decryption can be done with the help of the human visual system or by performing OR or XOR operations.

The convenient use of visual cryptography has laid the foundation for using this technique in various fields. The main plan of action for visual cryptography is that a single secret image would be split into two shares and are sent, on the receiver side these shares are collected, printed in transparency and overlapped one above the other to reveal the secret information Visual cryptography aided in moving information safe. Therefore, many fields have implemented this technique for image security, authentication, protecting biometric privacy, password protection, banking customer identification, key management, and son on. The traditional passwords do not exist any longer in the technical era, everyone has moved to biometrics to secure their information. There are various traits that are unique for every individual like iris, fingerprint, hand vein, palm print, ear, voice, signature, finger geometry, retina, DNA and grip recognition. The usage of biometric traits began in the 1800s where Alehouse Bertillon developed a method for identifying criminals using body measurements. In today’s world, over 7.5 million people are using biometrics to secure their computers, mobile phones, employee identification in companies, banking. In the sequence of securing these traits, various techniques have been formulated one of the effective techniques is visual cryptography. In this paper, we have done an extensive review of the various schemes available in visual cryptography for securing biometric privacy, scheme for authentication, for image security, and schemes that have used general access structure along with visual cryptography.

1.2 Objectives -

- The main objective of Visual Cryptography for Biometric Privacy project is that easily encrypt OR decrypt data in one system to another system.
- To increase the deficiency.
- Easy detection and correction of errors.

- To reduce the attendance pressure of employee or student.
- To make computation less manual.
- Provides view, update & delete biometric data administrator.
- It manages the information of various departments students or employees.
- It increase the efficiency of maintaining student or employee in & out details.
- To improve edit, add and update operations.

1.3 Purpose –

The purpose describes that the capabilities that will be provided by the Visual Cryptography for Biometric Privacy. It also states the various constraints by which the system will be follow. The intended audience of the system are developer, tester and the end user of application.

The development of this system contains following activities –

- The system provide secure registration and profile management of the user or admin.
- Administrator would authorized to handle details students and employees also add the new biometric details in system.
- College student & Organization employees can see the details according to fill in the system.
- Decrease the load of corrections involved in manual system like registers, etc.

1.4 Scope -

- It may help collecting perfect management in detail. In very short time the collection will be exact, simple and sensible. We have tried to computerize various process of Visual Cryptography for Biometric Privacy.
- It satisfies the user requirements.
- Be easy to understand by user and operate.
- Have a good user interface.
- User must have a valid User Id and password to login to the system.
- If a wrong password is given three times in succession, that account will be locked and the user will not be able to use it.
- When an invalid password is entered a warning is given to the user that account will be locked.
- Administrator can take a backup of the database for every moment that is happening, periodically.
- All users are authenticate to avail the service.

1.5 Applicability -

- There will be two interfaces which will include Admin and User.
- The whole project will be handled by one and only the administrator.
- Handling of the project includes maintaining the Students details, Employees details and administrator can do change in table data.

1.6 Achievements -

- The Visual Cryptography for Biometric Privacy is design in such way that consume the time also accuracy will taken form data.
- It is automated system of the early manual system. By this computerization method Visual Cryptography for Biometric Privacy is getting much faster than manual method.
- Students can easily handle website from anywhere.
- There two main reasons to develop this system.
- One is to reduce consume the time of students or employees means there is no need of the organization or college to maintain register entries and another is to reduce the use of papers. Lots of trees are used for making the papers.
- When result needed for any purpose we can simply download it. With the implementation of computerized system, the task of keeping records in an organized manner will be solved.
- We learned how to write a project SRS.
- We learn how to work with the Android Studio to develop an android application.
- We learn how to schedule a task so the productivity will be more.
- We gain lot of information about the software and technology available in this field.
- This web-application is user-friendly so this will cover a large amount of departments.
- Lesser the data redundancy and data in-consistency.
- Dynamic structure.
- Incorporate a huge amount of a data.
- It’s more reliable and improve productivity.
- The proposed system requires very less paper work. Because all the data is directly get stored on the cloud storage.

Chapter 2: Survey of Technology

There are many languages to be known by programmer. All of those languages use one which can be trendy and generally used. Every language has their exclusive characteristics, communities, help and ecosystems which have an effect on the decision-making system. The Android Operating System is the largest installed base among various mobile platforms across the globe. Hundreds of millions of mobile devices are powered by Android in more than 190 countries of the world. The company named open handset Alliance developed Android for the first time that is based on the modified version of the Linux kernel and other open-source software. Google sponsored the project at initial stages and in the year 2005, it acquired the whole company. In September 2008, the first Android-powered device launched in the market. Android dominates the mobile OS industry because of the long list of features it provides. It's user-friendly, has huge community support, provides a greater extent of customization, and a large number of companies build Android-compatible smartphones. As a result, the market observes a sharp increase in the demand for developing Android mobile applications, and with that companies need smart developers with the right skill set. At first, the purpose of Android was thought of as a mobile operating system. However, with the advancement of code libraries and its popularity among developers of the divergent domain, Android becomes an absolute set of software for all devices like tablets, wearables, set-top boxes, smart TVs, notebooks, etc.

The Tools and languages Used for Additional Course Management System:

2.1 Android -

Android is a mobile/desktop operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets. Android is developed by a consortium of developers known as the Open Handset Alliance and commercially sponsored by Google. It is free and open-source software; its source code is known as Android Open Source Project (AOSP), which is primarily licensed under the Apache License. However most Android devices ship with additional proprietary software pre-installed, most notably Google Mobile Services (GMS) which includes core apps such as Google Chrome, the digital distribution platform Google Play and associated Google Play Services development platform. Software packages on Android, which use the APK format, are generally distributed through proprietary application stores like Google Play Store, Samsung Galaxy Store.

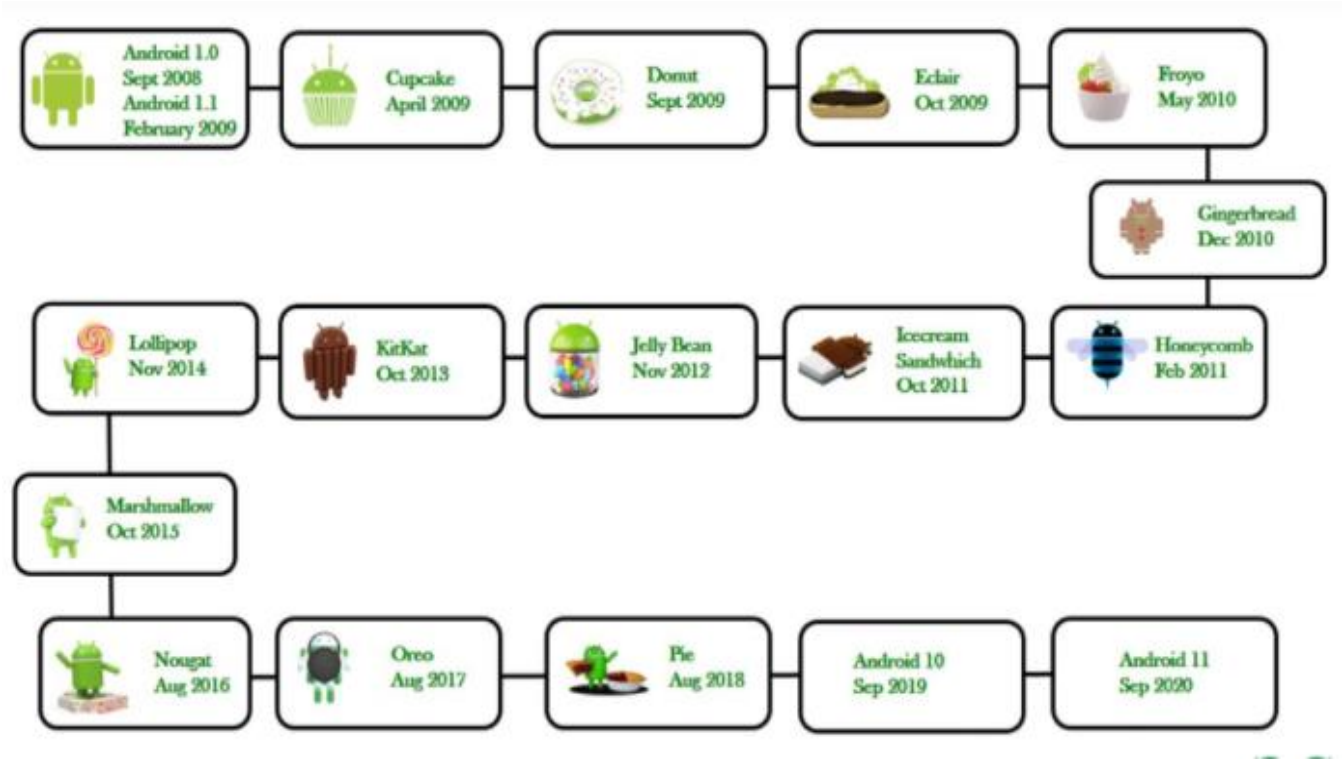
2.2 Features of Android -

Android is a powerful open-source operating system that open-source provides immense features and some of these are listed below.

- Android Open Source Project so we can customize the OS based on our requirements.
- Android supports different types of connectivity for GSM, CDMA, Wi-Fi, Bluetooth, etc. for telephonic conversation or data transfer.
- Using wifi technology we can pair with other devices while playing games or using other applications.
- It contains multiple APIs to support location-tracking services such as GPS.
- We can manage all data storage related activities by using the file manager.
- It contains a wide range of media supports like AVI, MKV, FLV, MPEG4, etc. to play or record a variety of audio/video.
- It also supports different image formats like JPEG, PNG, GIF, BMP, MP3, etc.
- It supports multimedia hardware control to perform playback or recording using a camera and microphone.
- Android has an integrated open-source WebKit layout based web browser to support User Interface like HTML5, CSS3.
- Android supports multi-tasking means we can run multiple applications at a time and can switch in between them.
- It provides support for virtual reality or 2D/3D Graphics

2.3 **Android Versions -**

Google launched the first version of the Android platform on Nov 5, 2007. Since then, Google released a lot of android versions such as Apple Pie, Banana Bread, Cupcake, Donut, Éclair, Froyo, Gingerbread, Jellybeans, Kitkat, Lollipop, marshmallow, Nougat, Oreo, etc. with extra functionalities and new features.



2.4 Android Studio -

Android Studio is the official integrated development environment (IDE) for android application development. It is based on the IntelliJ IDEA a java integrated development environment for software & incorporates its code editing and developer tools. To support application development within the android operating system, Android Studio uses a Gradle-based build system, emulator, code templates & github integration. Every project in Android Studio has one & more modalities with source code and resource files. These modalities include Android app modules, Library modules and Google app engine modules.

Android Studio uses an instant push feature to push code and resource changes to a running application. A code editor assists the developer with writing code and offering code completion, refraction and analysis. Application built an Android Studio are then compiled into the APK format for submission to the Google Play Store. Android Studio is available for Mac, Windows and Linux desktop platforms. It replaced Eclipse Android Development Tools (ADT) as the primary IDE for android application development.

2.5 Firebase –

Firebase is a Backend-as-a-Service (Baas). It provides developers with a variety of tools and services to help them develop quality apps, grow their user base, and earn profit. It is built an Google Infrastructure. Firebase is categorized as a NoSQL database program, which stores data in JSON like documents. It is set of key value pairs defined by a schema. A group of documents makes up a collection.

Key Features –

1) Authentication – It supports authentication using passwords, phone numbers, Google, Facebook, Twitter and more. The Firebase Authentication (SDK) can be used to manually integrate one or more sign-in methods into an app.

2) Real-time Database – Data is synced across all clients in real-time and remains available even when an app goes offline.

3) Hosting – Firebase hosting provides fast hosting for a web app, content is cached into content delivery networks worldwide.

4) Test lab – The application is tested on virtual an physical devices located in Google's data centre.

5) Notification – Notifications can be sent with firebase with no additional coding.

Chapter 3: Requirement and Analysis

3.1 Problem Definition -

The previously few decade ago in schools and organization all check-in and check-out will maintain in registers. Registers should maintain in wrong manner like wrong entries should be enter by employees or school. This methods will required lot of manpower and lot of registers. We are not secure data properly.

3.2 Existing System –

The Recent System or the website of that organization or school is Dynamic. That website should not have feature for encrypt and decrypt data. So, for the user or organization it was just informative application. It was like Dummy application.

Following are some problem in existing systems –

Security - Security of data is very critical issue which has to consider in the current record system.

Time Consideration - While maintaining records manually is time consuming. We have to wait for time to enter in register.

Need for System – We have to easily encrypt and decrypt data easily manner. It will help to secure system. We are made system like application.

3.3 Proposed System –

So I decided to make dynamic application it will help to easily maintain data and also encrypt and decrypt data. It is dynamic application it will easily store and maintain data.

Advantages –

• Speed and accuracy there are no redundancy of data.

• It will be easily handling.

• The proposed method maintenance of schedule erroneous and it is very easy to operate.

• Reduce the time spend on the paper work.

3.4 Requirement Analysis –

3.4.1 Functional Requirements -

Login by admin -

- Manage the entire departments details.
- Manage attendance details.
- Login of the user/admin.
- Change password
- Change Personal Details.

3.4.2 Non-Functional Requirement –

1) On actual moment whenever we start project this time detailed analysis of issues such as availability, security, usability and maintainability.

2) However, this document is only an outline specification.

3) It does not contain actual problem error of project making.

4) Therefore, the sections below should be seen as indicative rather than providing specific requirements.

3.5 Requirement Specification –

3.5.1 Hardware Requirement –

Minimum RAM -> 2 GB

Minimum Hard disk -> 30 GB

Monitor Key-Board

Mouse

Processor: Intel i3

3.5.2 Software Requirement –

Front-end: Android Studio

Back-end: Firebase

Operating System: Microsoft Windows 10

The Functional/Purposeful Requirements of the System are as follows –

1) Login the System or else Sign up into the System.

2) Authenticate the user.

3) New details added.

4) Easily manage data.

1) Login the System or Sign up into the System -

The most important part in order to proceed further into the application is to Sign up or if you already have an account then you can choose to login and then proceed to the next part of the system.

2) Authenticate the user –
In practicality there could be multiple users situated at different places around the organization so where user can authorize the page at the same time with which device needs to be check before the access to the system.

Other Non-functional Requirement –

1) Availability -
An alternative database could be used as backup in case of failure or if the main server goes down could increase the availability of system.

2) Reliability –
System will work robustly without loss of any data even in the phase of numerous failures. The system should be able to give output even in low internet connection in the local areas.

3) Security -
The correct authenticated user should only be allowed to access and to use the system. And no other anonymous user should be granted the permission to use the application.

4) Safety –
The system should not fail and should not give the wrong information because if the information is not given properly there might be chance that the users might feel that the system is not meeting it is requirement and hence misguiding the users.

5) Maintainability -
The system should maintain the updates correctly and user data properly.

6) Usability -
The system should be easy to handle. The user of the system can easily use the application on his/her mobile phone to have the best result.

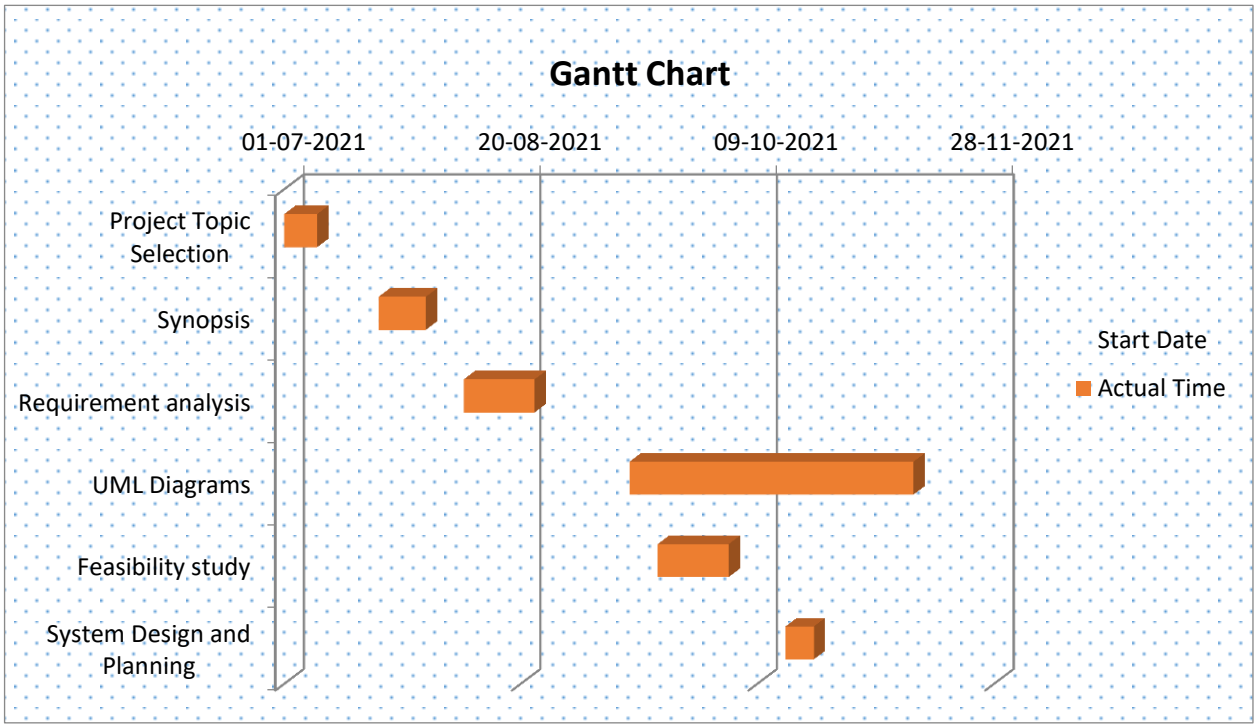
3.6 Planning &Scheduling –

Planning and Scheduling are two of the most important aspects of project planning. Proper planning can help your project to succeed. If the project is not schedule proper it may cost the organization. If the project is now scheduled properly the price of the project may improve.

3.6.1 Gantt chart -

Gantt chart is one of the most commonly used tools for analyzing and planning complex projects. Gantt charts help to prepare a proper path or schedule for each activity to be done in the creation of the project. It helps to know at the end of each activity whether they are running on time or not. One of its main objectives is to access about how much time will be needed to complete each activity as well as how much time the creation of the project is going to take. It also speaks about what all activities are needed to be performed. It helps the organization to know where they will need to allocate their resources. It gives a basis for scheduling each activity.

Task	Start Date	End Date	Estimate Times (Days)	Actual Time
Project Topic Selection	01-07-2021	20-07-2021	19	7
Synopsis	21-07-2021	07-08-2021	17	10
Requirement analysis	08-08-2021	08-09-2021	31	15
UML Diagrams	12-09-2021	15-11-2021	64	60
Feasibility study	18-09-2021	28-10-2021	40	15
System Design and Planning	15-10-2021	18-11-2021	34	6

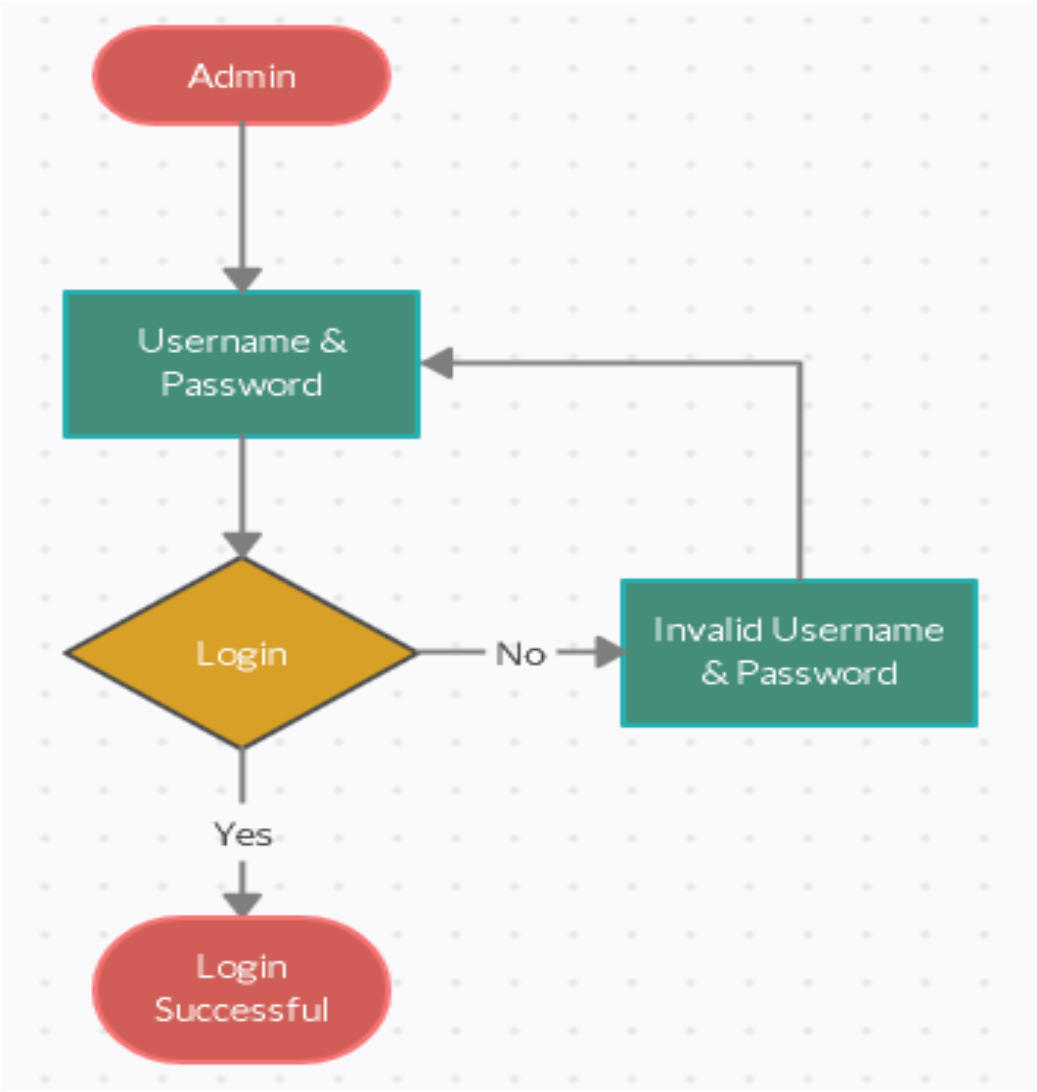


Chapter 4: System Design

4.1 Module Design –

This project has the following modules, to manage all the requirements of the college or organization –

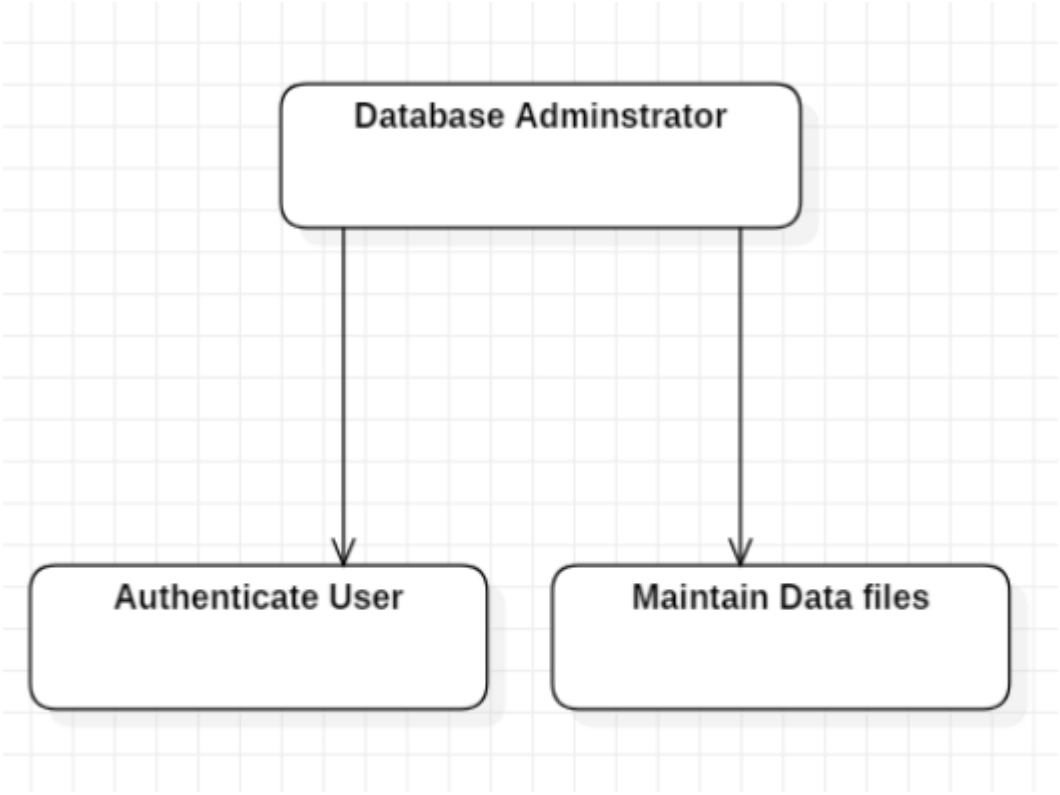
1) Admin Login
2) User Login
3) Authentication
4) User Details



4.2 Database Administrator –

The database administrator is the person who is responsible for authenticating the user as well as Storage and maintaining the detail of the user.

The user will be authenticated based upon his/her username and password and then only he/she will be given the access to the system through which he/she can punch the data.

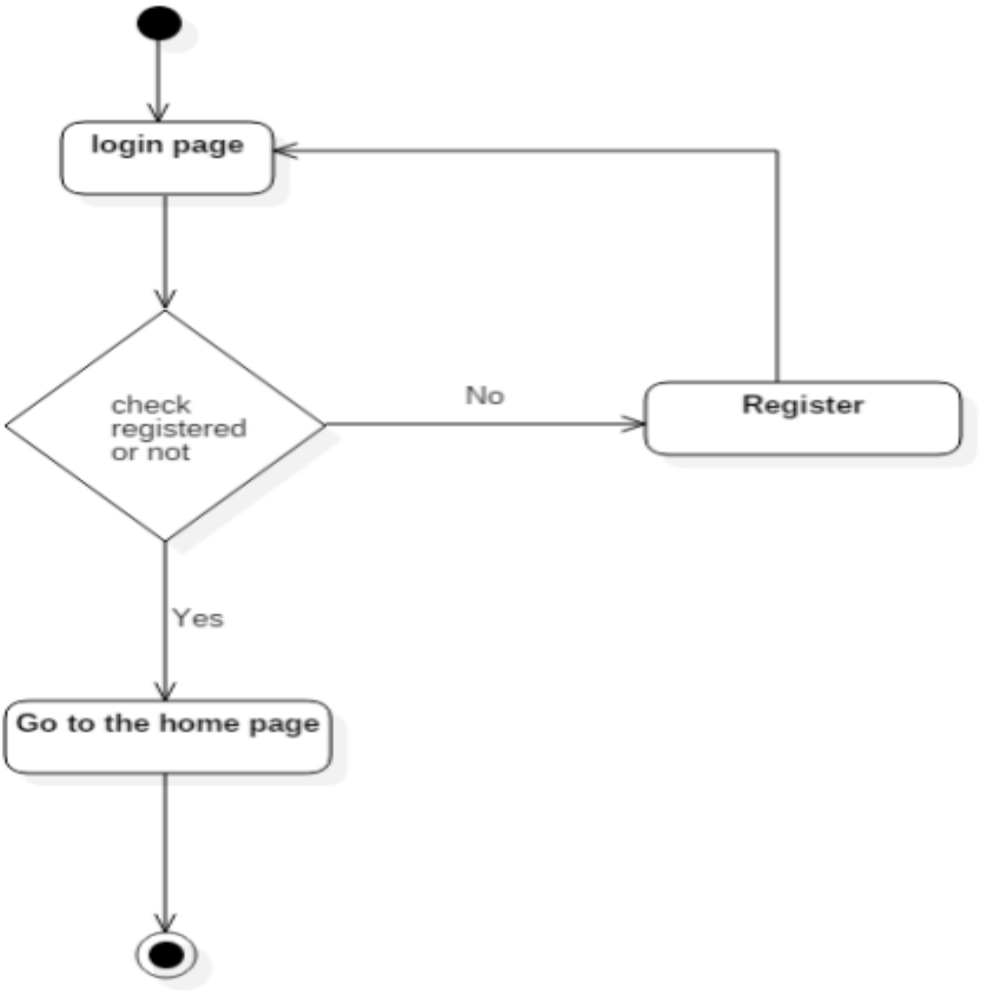


4.3 Data Dictionary -

Admin Login –

Field	Description	Type	Constraint
Username	Name	Varchar(25)	Null
Password	Password	Varchar(25)	Null

Flow of Login Activity:



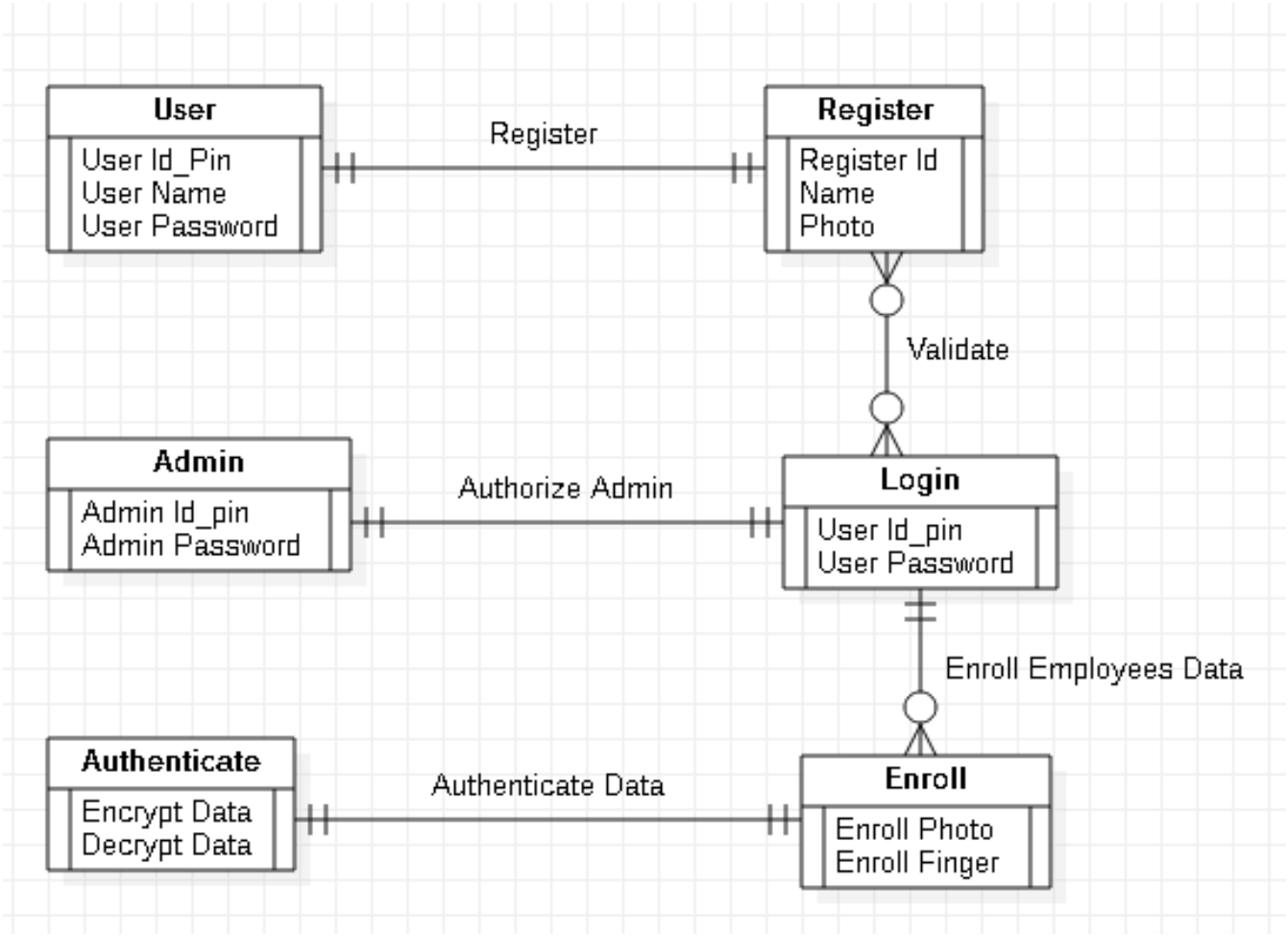
1) In the login activity 1st there's a start node once the user first login into the system.

2) The system can check whether or not the user is registered or not if the user is registered it'll transfer it to the subsequent page or we will say the activity.

3) If the user isn't registered with the system, then the another page can open wherever he need to register his details.

4) At the moment he can get transfer back to the login page where he need to re-login within the system and also the system can once more check whether or not the user is registered or not then he can get transfer to the new page or next page that’s our main activity page were all the most options of the website get visible to the user.

ER Diagram –



Data models are tools used in analysis to describe the data requirement and assumptions in the system from a top-down perspective. They also set the stage for design of databases later on in the SDLC.

There are three basic elements in ER model –

Entities are the "things" about which we seek information.

Attributes are the data we collect about the entities.

Relationships provide the structure needed to draw information from multiple entities.

Entity - It represents a collection of objects o things in the real world whose individual members or instances have the following characteristics: Each can be identified uniquely in some fashion.

Attributes - They express the properties of entities. Attributes having unique values are called candidate keys (Primary key).

Relationships - They describe the association between entities.

They are characterized by cardinality as follows:

1) One-to-One relationship means an instance of the first entity is associated with only one instance of second entity.

2) One-to-Many relationship means that one instance of the first entity is related to many instances of second entity, while an instance of second entity is associated with only instance of the first entity.

3) Many-to-Many means that an instance of the first entity is related to many instances of the second entity and the same is true in the reverse direction also.

Working of ER diagram –

1. User is register his account on college or organization Application.

2. User is login his /her account after registration.

3. If user is not having account and it will login then application doesn't allow them.

4. For security application doesn't allow unauthorized user.

5. Admin will handle application database easily.

6. Admin will have authority to handle the application.

7. Admin is update / delete details.

8. User is en-roll data.

9. User authenticate data.

DFD Diagram -

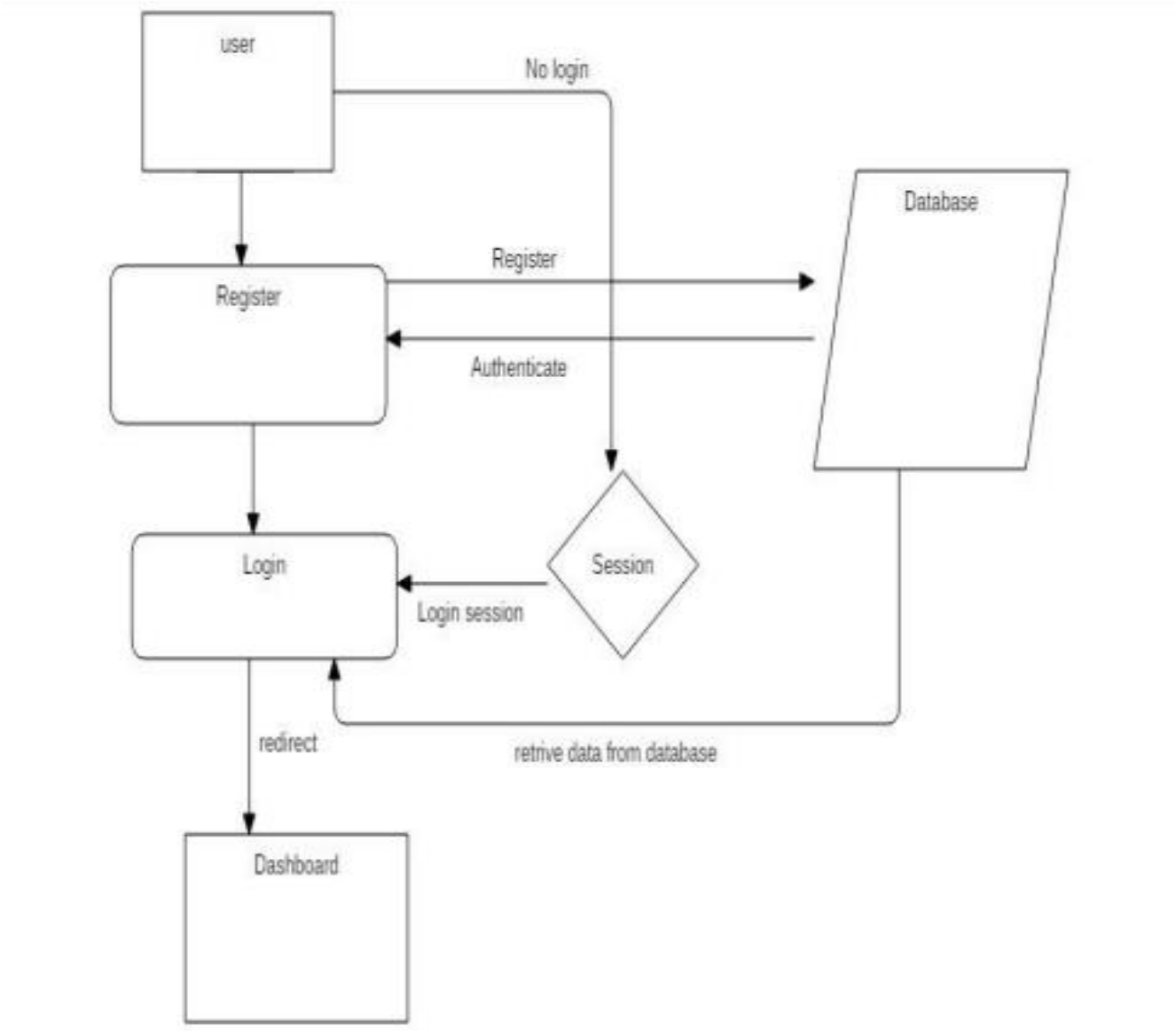
Working of Data flow diagram –

1) Admin is update / delete details.

2) Authorize user will be handle database.

3) User will login with Username & Password.

4) User choose data as user can store in system.



1) A data flow diagram (DFD) maps out the flow of information for any process or system.

2) It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination.

3) Data flowcharts can range from simple, even hand-drawn process overviews, to in-depth, multi-level DFDs that dig progressively deeper into how the data is handled.

4) They can be used to analyze an existing system or model a new one.

5) Like all the best diagrams and charts, a DFD can often visually "say" things that would be hard to explain in words, and they work for both technical and nontechnical audiences, from developer to CEO.

6) That's why DFDs remain so popular after all these years.

7) While they work well for data flow software and systems, they are less applicable nowadays to visualizing interactive, real-time or database-oriented software or systems.

Use Case Diagram:

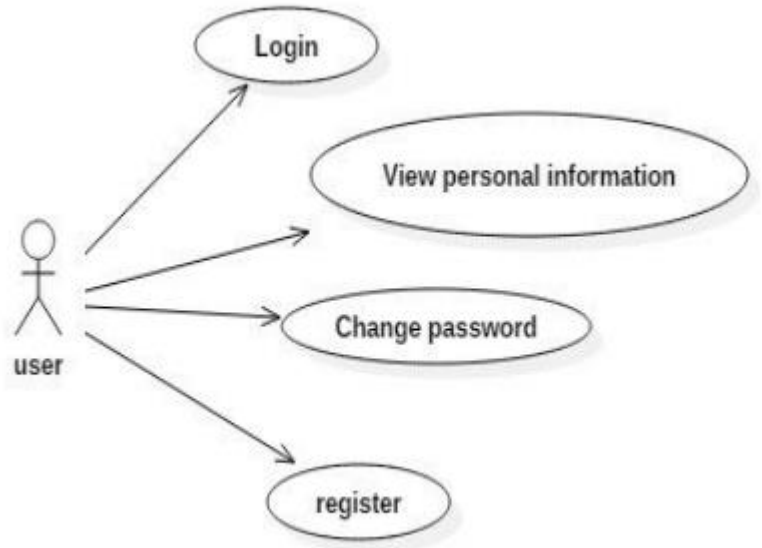
A Use Case Diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved.

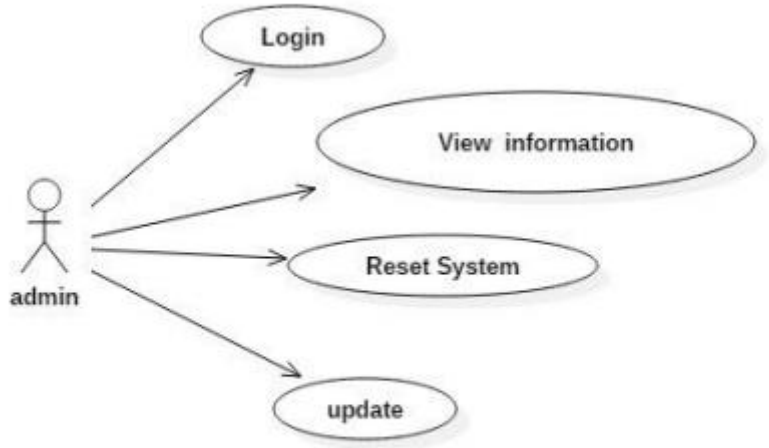
A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well.

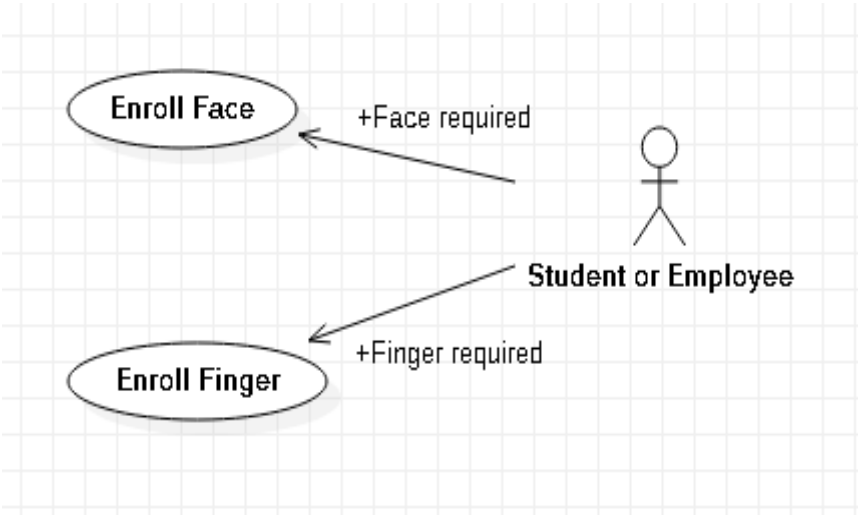
The purpose of the use case is to define the piece of coherent behavior without reviling the internal structure of the system.

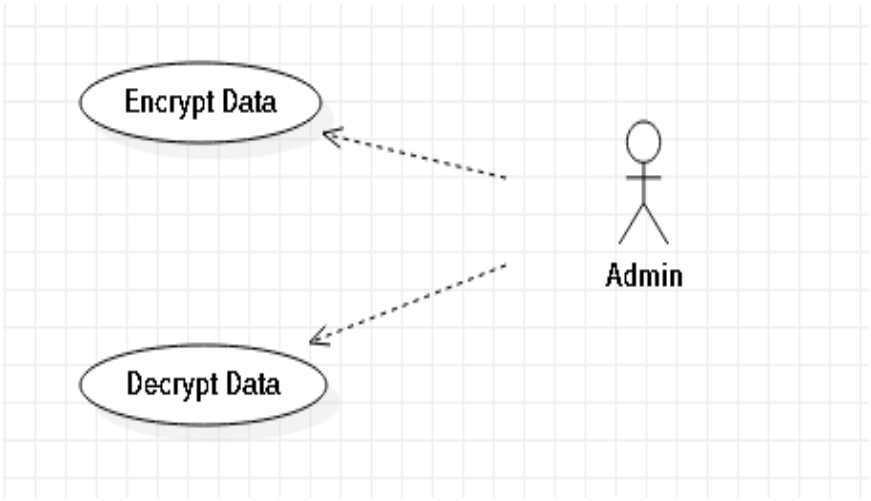
A use case typically represents a sequence of interaction between the user and the system. These interactions consist of one main line sequence is represent a normal interaction between the user and the system.

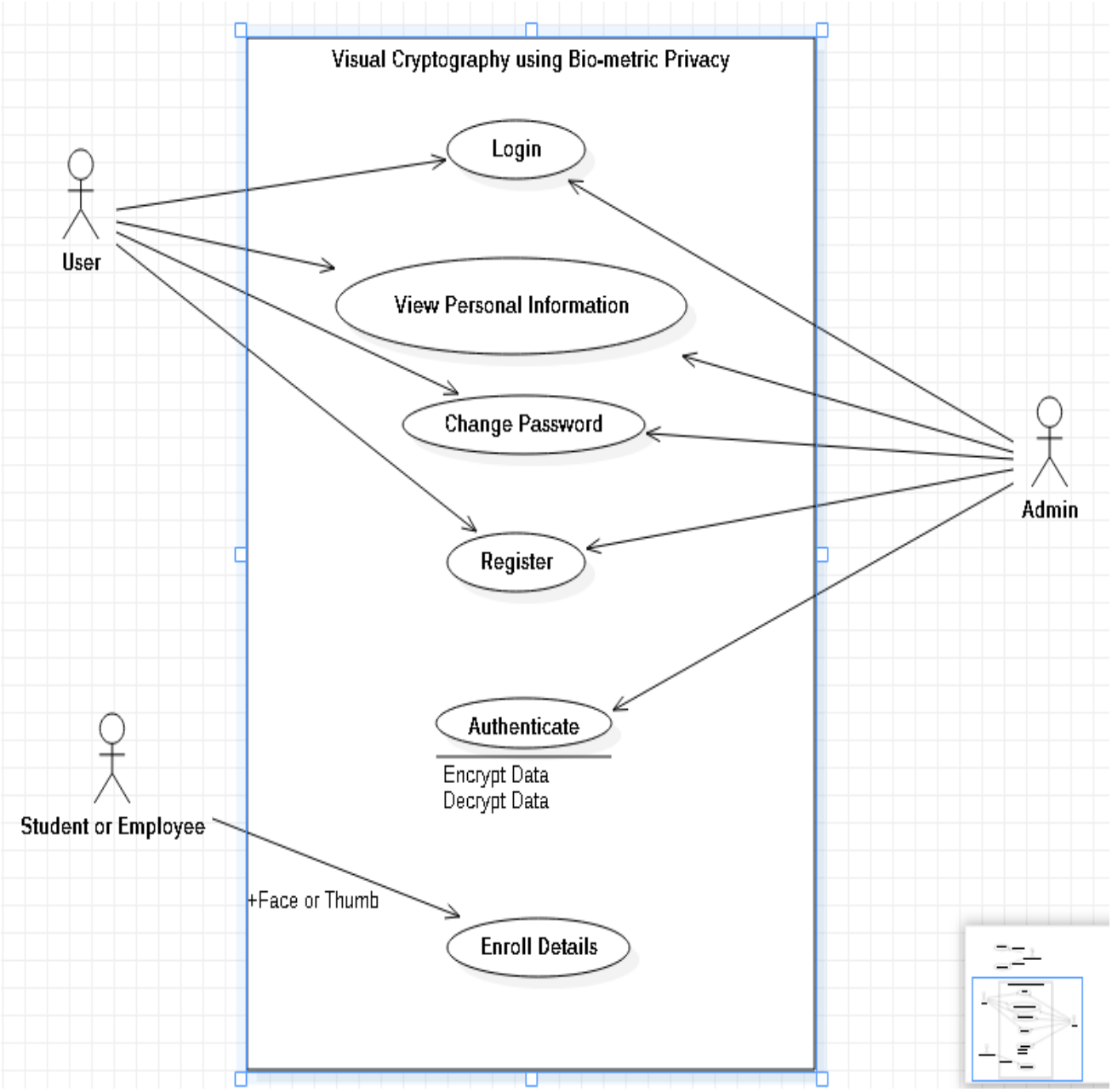
The use case model is an important analysis and design task. Use case can be represented by drawing a use case diagram and writing an accompany text elaborating the drawing


Login
View personal information
user
Change password
register


Login
View information
admin
Reset System
update


Enroll Face
+Face required
Student or Employee
+Finger required
Enroll Finger


Encrypt Data
Admin
Decrypt Data


Visual Cryptography using Bio-metric Privacy
Login
User
View Personal Information
Change Password
Admin
Register
Authenticate
Encrypt Data
Decrypt Data
Student or Employee
+Face or Thumb
Enroll Details

Sequence Diagram –

1) A sequence diagram shows object interactions arranged in time sequence.

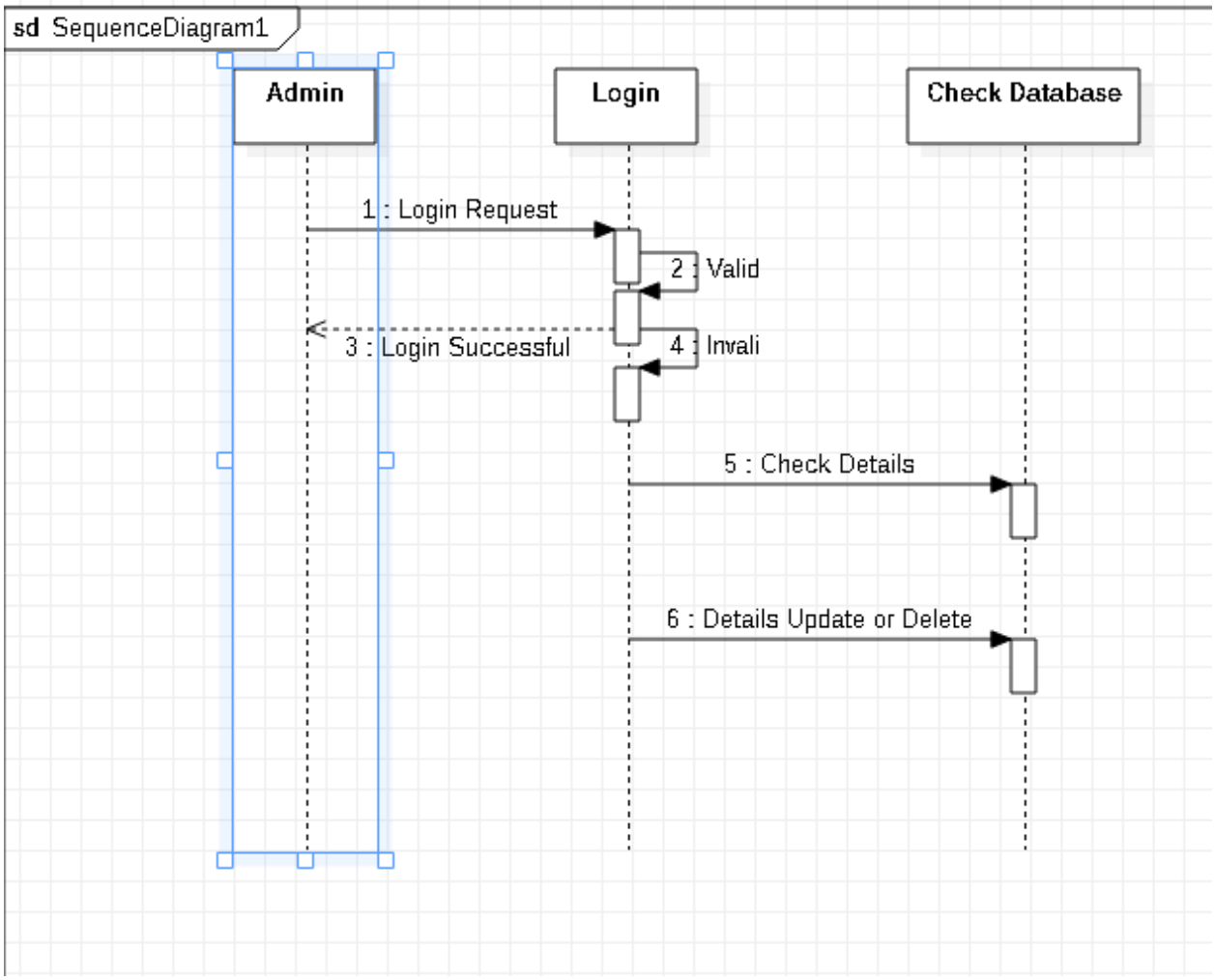
2) It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

3) Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development.

4) Sequence diagrams are sometimes called event diagrams or event scenarios.

5) A sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur.

6) This allows the specification of simple runtime scenarios in a graphical manner.



Working of sequence diagram –

1) User is register his account on application.

2) User is login his /her account after registration.

3) If user is not having account and it will login then application doesn't allow them.

4) For security application doesn't allow unauthorized user.

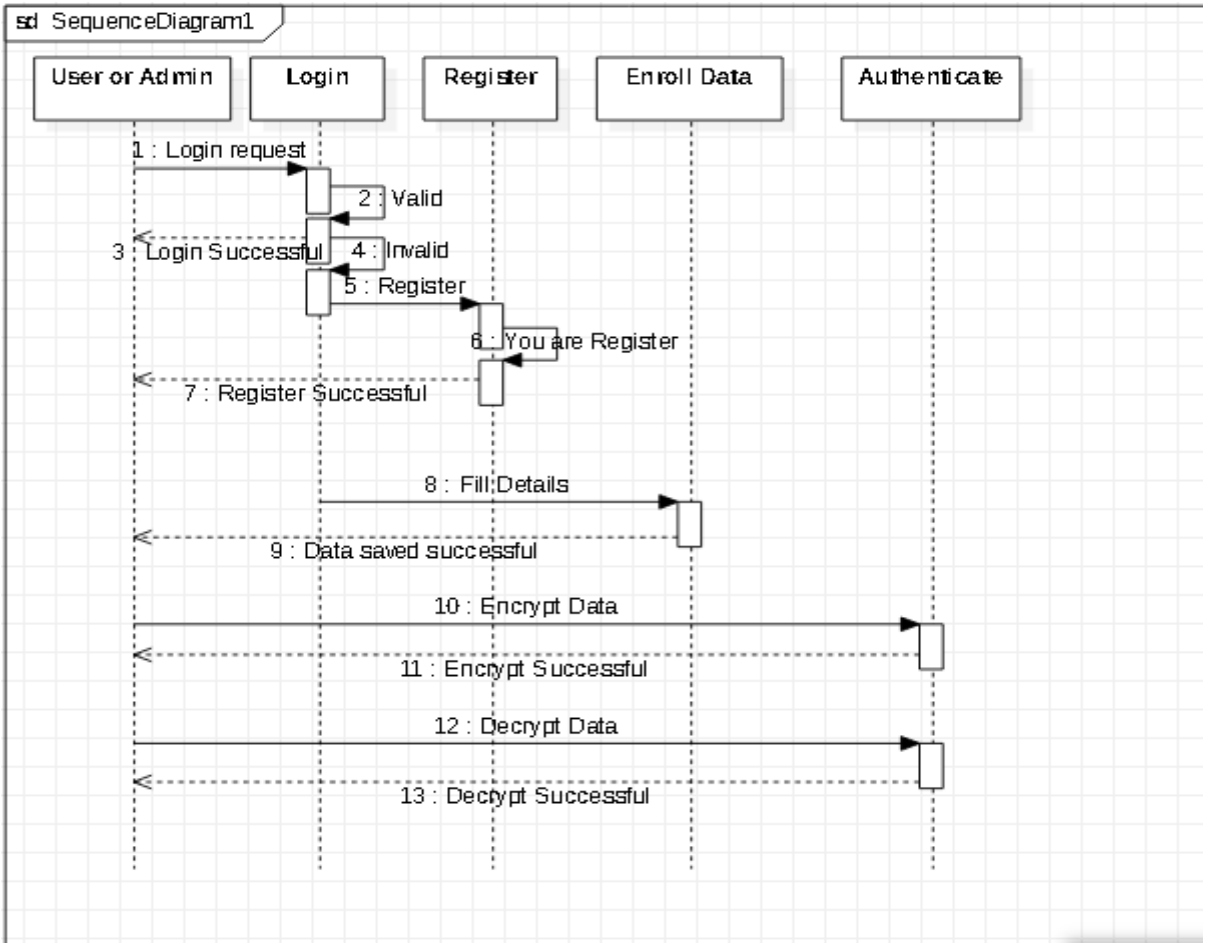
5) Admin will handle application database easily.

6) Admin will have authority to handle the application.

7) Admin is update / delete details.

8) User will enroll data in application.

9) Authentication allows data easily encrypt or decrypt when share to one-another.

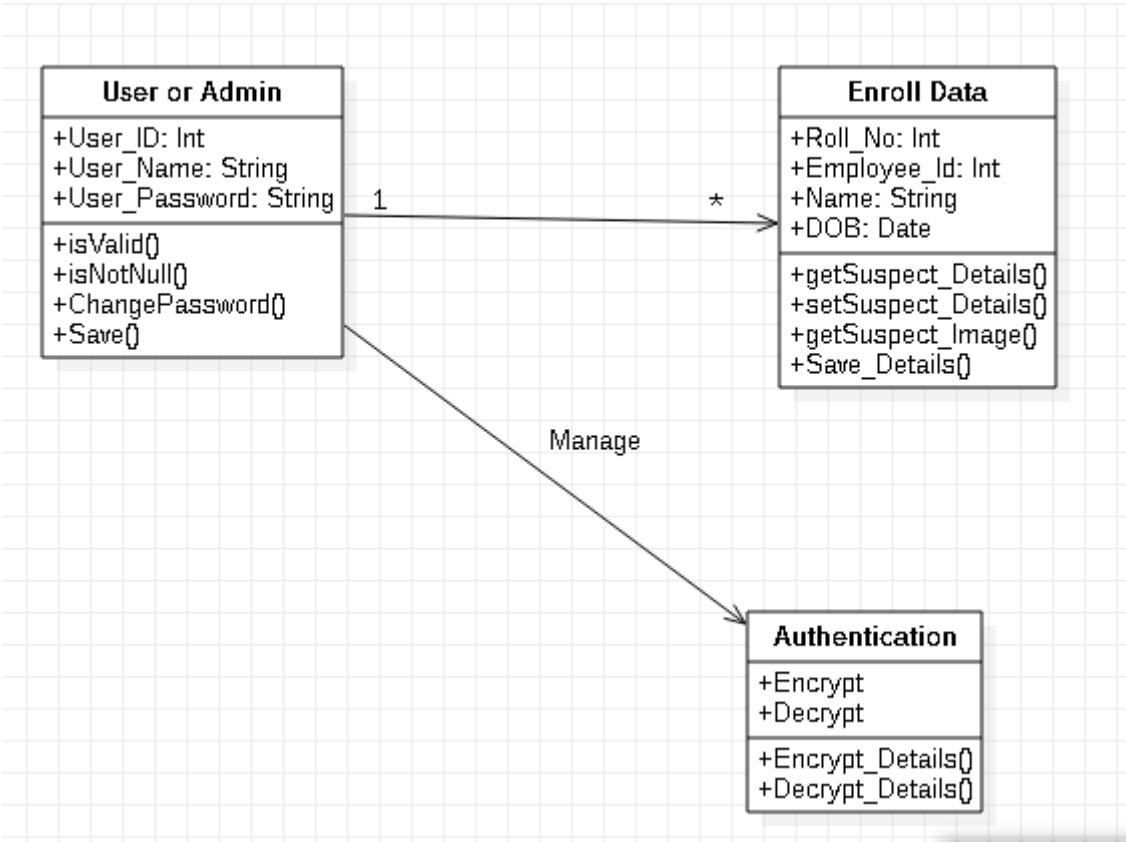


Class Diagram –

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

Explanation of the Class Diagram with respect to Visual Cryptography for Biometric Privacy:

The pivot classes which will be created are, the databases will also be managed for the same.



4.4 Security issues –

1) The database may get crashed at any certain time due to virus or operating system failure.

2) Therefore, it is required to take the database backup some of the factors that are identified to protect the software from accidental or malicious access, use, modification, destruction or disclosure are described below.

3) Keep specific log or history data sets.

4) Assign certain functions to different modules

5) Restrict communications between some areas of the program

6) Check data integrity for critical variables.

7) Later version of the software will incorporate encryption techniques in the user/license authentication process

Reference:

https://www.academia.edu

https://mafiadoc.com

https://www.sitepoint.com

https://www.geeksforgeeks.org

https://en.wikipedia.org

https://www.netl.doe.gov