**Cab Transaction Using Facial Recognition and Matching Engine**

B.E. Phase I project report submitted in partial fulfilment of the requirements of the degree of

**Bachelor of Engineering**

by

**Kshitij Shukla (EU2152053)**

**Rohan Chavan (EU1152082)**

**Saniket Patil (EU2152014)**

Under the guidance of

**Mr. Vivian Lobo**

(Assistant Professor)

****

**Department of Computer Engineering**

**St. John College of Engineering and Management**

**University of Mumbai**

**2019-2020**

CERTIFICATE

This is to certify that the project entitled **“Cab Transaction Using Facial Recognition and Matching Engine”** is a Project Phase I report of

**Kshitij Shukla (EU2152053)**

**Rohan Chavan (EU1152082)**

**Saniket Patil (EU2152014)**

Submitted to University of Mumbai in partial fulfilment of the requirement for the award of the degree of **“Bachelor of Engineering”** in **“Computer Engineering”.**

Mr. Vivian Lobo

Project Guide

Dr. Rahul Khokale Dr. G. V. Mulgund

Head of Department Principal

Project Report Approval for B. E.

This project synopsis entitled **Cab Transaction Using Facial Recognition and Matching Engine** by Kshitij Shukla, Rohan Chavan, Saniket Patil is approved for the degree of **Bachelor of Engineering** in **Computer Engineering** from **University of Mumbai**.

Examiners

**1.--------------------------------**

**2.--------------------------------**

Date:

Place:

**Abstract**

Currently when booking a Cab, at the end of the ride you make the transactions with either cash or Card/UPI/E-Wallet. Sometimes these methods are not hassle-free as they cause inconvenience to the customer. We propose a new System for transactions in Cabs, where face is your Transaction method. The system in the Cab will calculate your fare based on the distance and then it will authenticate your face and transact via the connected central database. Face Recognition begins with extracting the coordinates of features such as width of mouth; width of eyes, pupil, and compare the result with the measurements stored in the database and return the closest record (facial metrics). Main purposes of this research is to research different types of face recognition algorithms like Eigen face and Fisherface. Open CV provides these recognition algorithms. We do this by comparing the Receiver Operating Characteristic Curve to implement it in our Transaction using Facial Recognition. We have noted that EigenFace delivers better results than the Fisherface algorithm, Eigen face delivers between 70 to 80 % accuracy between faces. If the User’s input image matches with the trained dataset image then the User Profile and Transaction details will be loaded, and the subsequent trip details will be stored in the User Profile database. The database is connected to FRaME web server. The system has 95% accuracy with the dataset of 20 person images.

**Chapter 1**

**Introduction**

With the popularity in India of mobile payment platforms such as Paytm and PhonePe, QR codes can be found almost anytime, anywhere in Indian daily life. From luxury shopping centers to street vendors, consumers can make payments easily by scanning a QR code with their smartphones. The awkwardness of forgetting your wallets at home no longer exists. As long as you have a mobile payment set up on your phone, you can virtually always go cashless in India.

But, things are changing as we speak. QR codes are just a step in the evolution of mobile payment technology and they may soon be a thing of the past. In fact, soon people in India may be able to forget about QR codes, and pay with virtually nothing but... themselves. This new payment method we are talking about is facial recognition, which we are planning to implement in Cabs.

**How does facial recognition work?**

Using a series of algorithms, facial recognition technology works by scanning your face using a digital camera, analysing it based on a variety of physical traits. Using this analysis, the system can create a face print - a unique code of individual face, which is stored and accessed through an identity database.

**1.1 Motivation & Problem Statement**

The number of online banking users has increased in India and indeed the world; this has led to many experts in mobile banking software and mobile phone technology to research new and convenient methods for customers to perform banking transactions remotely via their mobile phones. Mobile banking is also known as mobile phone bank. It is referred to as the using mobile phone for banking related business. But the problem is that it is not convenient for users to enter long high security passwords every time they want to make a transaction or remember their UPI VPA(Virtual Private Address), or even carry credit cards or debit cards everywhere. That’s highly inconvenient to the users. So, we are proposing a system where you don’t have to carry cards or remember your VPAs.

**1.3 Objectives**

* To design a system where we can login your profile using just your face.
* To design a system for cabs where you do not have to pay via card or cash.
* A System where once your load your profile you can initiate a transaction without any card. All we have to do is enter High security password as a second layer of security.
* To make this system robust enough to be used in future in other applications.

**Chapter 2**

**Review of Literature**

Literature Review acts as the basis of research and study of the various concepts required for a particular domain. It describes the theories and other methodologies that can be adopted in order to implement modules of the proposed system. This chapter includes literature survey of technical papers along with the advantages and disadvantage of each system.

**2.1 Face Recognition Techniques for Differentiate Similar Faces and Twin Faces**

In computer technology image based on identical twin, face recognition technology is challenging task. Traditional facial recognition system exhibit poor performance in differentiating identical twins and similar person under practical conditions. The following methods for differentiate identical twins.

Traditionally lot of manual experiments were performed to identify twins and also to recognize their features with difference, and many more systems were existed to show differences in twins by using finger prints, voice and iris as part of pattern recognition. In existing methods, many techniques are used for twin’s identification like finger print, voice and iris recognition.

The process of finger print identification is used to identify unique person in industry or organizations.

The method propose a scan image taken from the person and compare with database for identification. The iris recognition also similar method to finger prints identification.

**FACIAL RECOGNITION TECHNOLOGY:**

Facial Recognition technology s biometric identification by scanning a human face and matching with stored database images. Face recognition system can be used for identification and verification of a person.

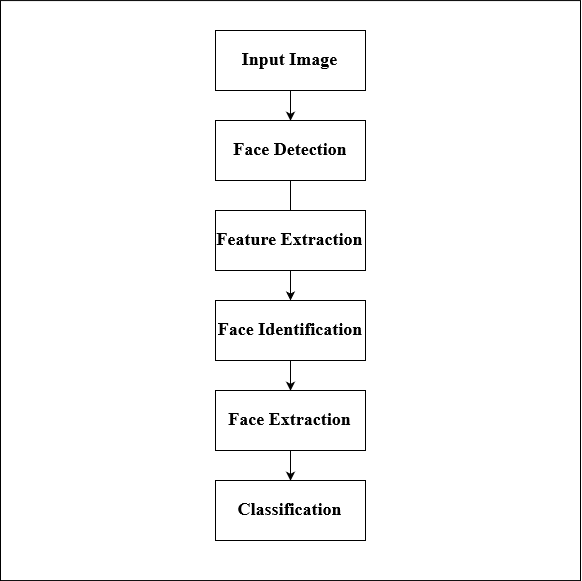


Figure 2.1: System Architecture for Face Recognition Technology

**2.2 Secure Authentication for Mobile Banking Using Facial Recognition**

In the past decades, banking was done inside the banking hall which was tasking to both the customers and the bankers. The long queues, paper-based data and even the time taken to perform even the smallest transaction can be an uphill task.

This has now been a thing of the past since the advent of the internet and mobile phones. The number of online banking users has increased in Nigeria and indeed the world; this has led to many experts in mobile banking software and mobile phone technology to research new and convenient methods for customers to perform banking transactions remotely via their mobile phones.

Mobile banking is also known as mobile phone bank. It is referred to as the using mobile phone for banking related business. Security has become a primary concern in order to provide protected mobile transaction between the clients and the bank servers. Secure authentication of client information depends on some fundamental security approaches which will not jeopardize the client sensitive information. This has led to different researches ranging from single-factor authentication, two-way authentication, and multifactor authentication. Bearing in mind the cost of providing these services to clients, most banks are weary of balancing profit making and security. In Nigeria today, most mobile banking applications use the single-factor authentication which consist of the username and password.

Secure mobile banking will build confidence in customers knowing that their information is secure and they can carry out secure transactions without fear of man-in-the-middle attacks. Though the issue of theft strongly depends on how a client protects his/her mobile phone device from third parties.

**Problem Identification of the Current System**

* 2-Way Authentication consists of Username and password only.
* Poor level of security.
* It is easy for hackers to breach into the account.
* It is possible for hackers to clone the SIM card.
* When SIM card is cloned, the bank server will assume the hacker as the authentic user.
* In case of theft, mobile phone can be hacked into, whilst the bank server would allow access into the account assuming the hacker to be the authentic user.

**OVERVIEW OF THE PROPOSED SYSTEM**

The proposed system is expected to provide higher level of authentication (multifactor authentication) which will bring unauthorized access to the barest minimum. Before access will be granted, the user will have to take a facial photograph to have access to his/her account, the geometry of the face, distance of the eyes and the nose is compared. This photograph will be compared with the photograph in the bank server and the NCC server for verification, if it passes the verification, access will be granted, otherwise it will denied. In the event of unauthorized access, a security alert message will be sent to the bank.

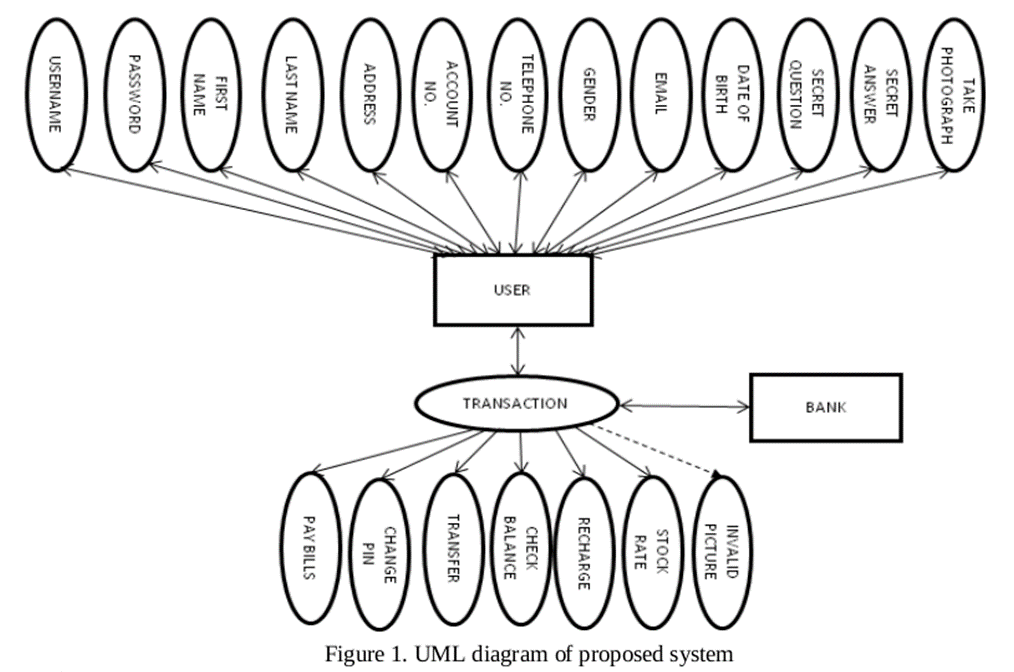
**Result And Discussion**

On the program end, the security is multi-factored. A username and password level, a facial recognition level and a secret question and answer level. Users are limited to five trials after which access is denied. Two dependable databases are also used to authenticate genuine users; these databases are the NCC database and the issuing bank database. In an advent of facial defection, users are advised to see their bank information technology operators. The response time for a complete transaction is seven minutes maximum putting other limiting factors into consideration; the false acceptance rate is 3%.the implication of false acceptance rate is given by elements on image background and facial defects. The advantages of this system include;

i.Secure and transaction

ii.Cost effective

iii.Transaction can be done anywhere remotely (with availability of mobile network)



**Chapter 3**

**Requirement Analysis**

**3.1 Performance Requirements**

**Response Time**

It is basically the time taken to do something after it has been given enough input. Whatever is been given as an output must be measurable in the real system. Care must be taken to ensure that the performance measurement is unambiguous, concise and completely defined.

**Scalability**

In one respect scalability is simply specified as the increase in the system’s workload that the system should be able to process. The scalability required is often driven by the lifespan and the maturity of the system.

**3.2 Software Requirement**

* Operating System: Windows 7 and Above / Any Linux
* XAMPP / LAMP stack: Webapp
* Python3: Face Recognition
* OpenCV: Image Processing

**3.3 System Hardware Requirement (Minimum)**

* Processor: Quad Core 32/64 bit
* RAM: 4 GB
* Hard Disk: 3 GB
* GPU: 1 GB

**3.4 Hardware Components Required**

* Web Camera.

**Chapter 4**

**Design**

Designing basically refers to developing the various designs and diagrams that are required to implement a project. This chapter focuses on the various diagrams that are developed as a part of the proposed system and gives their short description. UML diagrams used are Sequence diagram, Activity diagram and Deployment diagram.

**4.1 Sequence Diagram**

A sequence diagram simply depicts interaction between objects in a sequential order i.e. the order in which these interactions take place. We can also use the terms event diagram**s** or event scenarios to refer to a sequence diagram. Sequence diagrams describe how and in what order the objects in a system function.

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

Figure 4.1 shows the sequence diagram for Cab Transaction using Facial Recognition and Matching Engine.

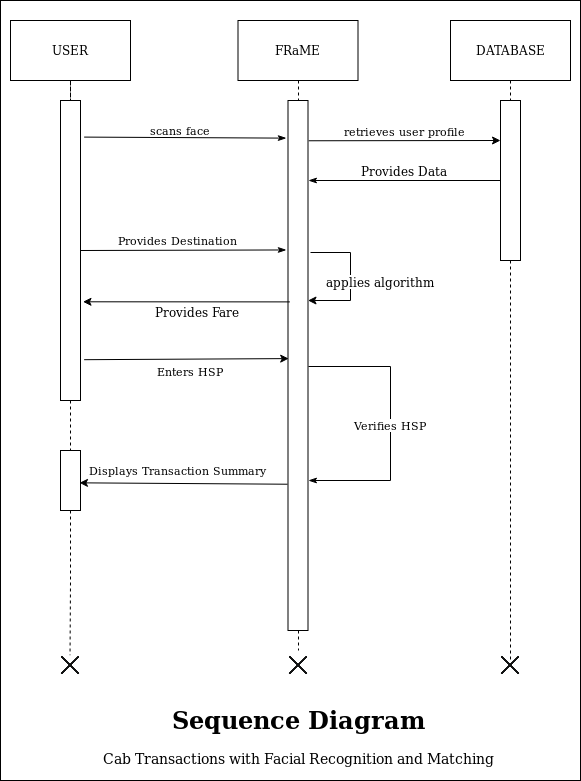


Figure 4.1

**4.2 Activity Diagram**

Activity diagram is a flow chart to represent the flow form one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc.

Figure 4.2 shows the Activity diagram of the system.

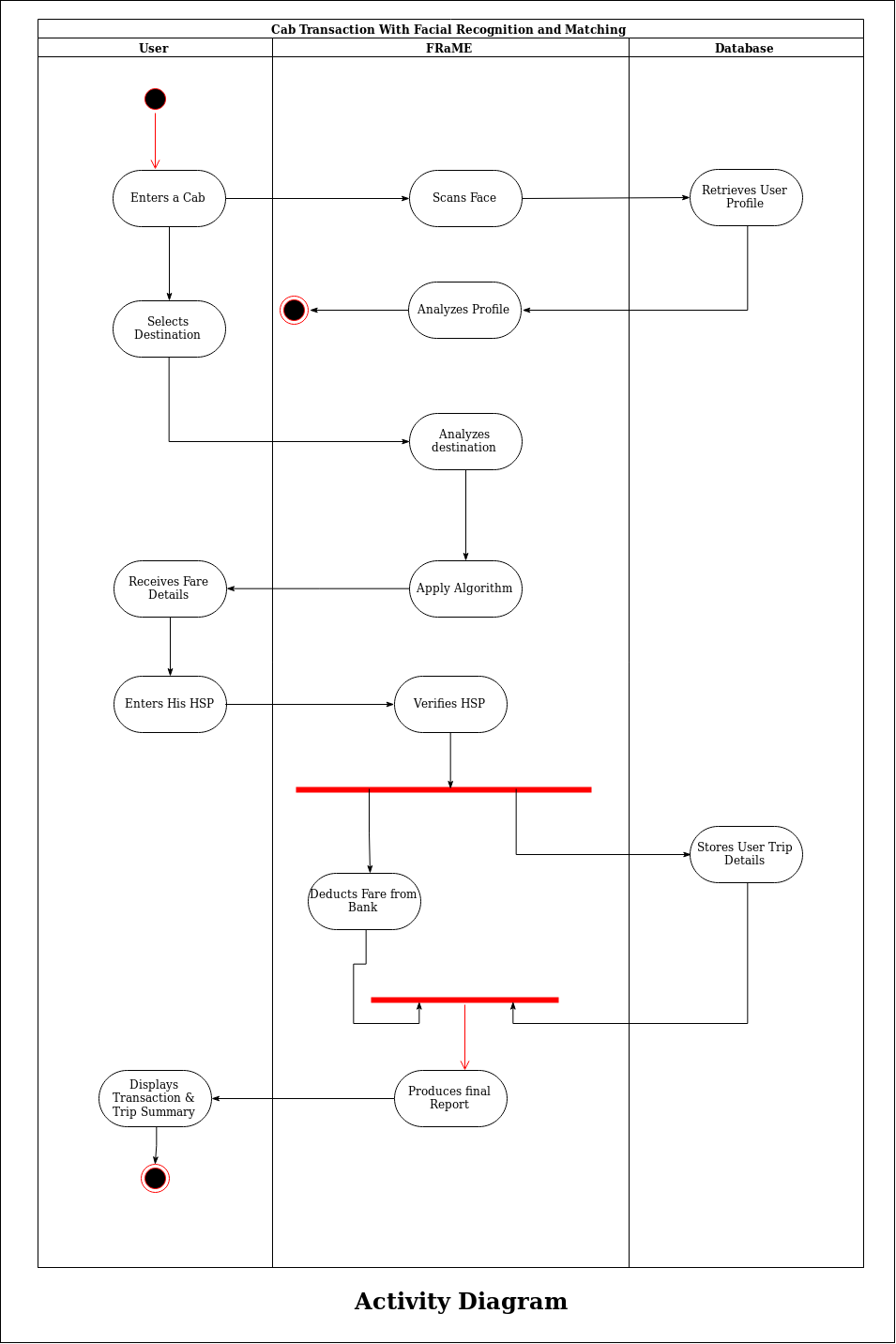


Figure 4.2

The basic purpose of activity diagram is similar to other four diagrams. It captures the dynamic behaviour of the system. Other four diagrams are used to show the message flow from one object to another but activity diagram is used to show message flow from one activity to another.

**4.3 Data Flow Diagram (DFD)**

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated.

Figure 4.3 shows the DFD diagram of the system.

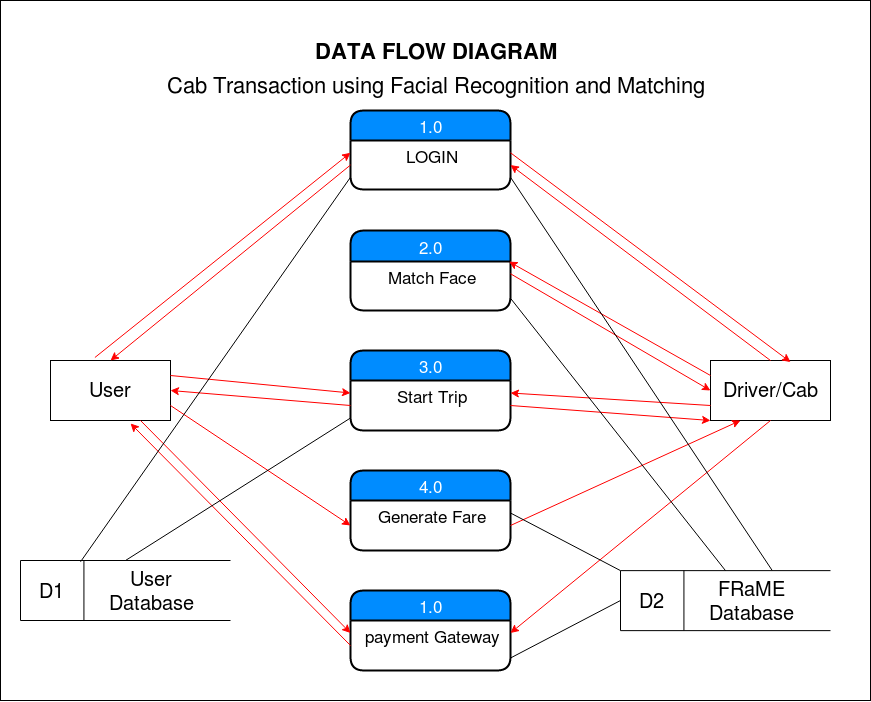


Figure 4.3