Major Project Report

“Multi-modal Biometric Verification Using Face, Finger and Voice”

This report is submitted for the evaluation of Major project of B. Tech Degree to

Department of Computer Science and Engineering

at

NATIONAL INSTITUTE OF TECHNOLOGY SIKKIM

Submitted By:

Shashi Saurabh Sinha

Roll No: B180043CS

B. Tech, 4th year, 8th Semester

Concerned Faculty and Supervisor

Dr. Pankaj Kumar Keserwani

Assistant Professor

Department of Computer Science & Engineering

National Institute of Technology Sikkim

National Institute of Technology Sikkim
Ravangla, South Sikkim – 737139, Sikkim, India

CERTIFICATE

This is to certify that the project entitled **"Multimodal Biometric Verification using face, finger and Voice"** being submitted **Shashi Saurabh Sinha (B180043CS)** is a bonafide record of work carried out by him under my supervision and guidance, and hence approved for submission to the **Department of Computer Science & Engineering, National Institute of Technology Sikkim** in partial fulfilment of the requirements for the award of the degree in **Bachelor of Technology (B. Tech) In Computer Science & Engineering**. The content embodied in this project has not been submitted anywhere else in full or in parts to obtain any degree or diploma.

Dr. Pankaj Kumar Keserwani
Project Supervisor

Dr. Pratyay Kuila
Head of the Department

Date: 2nd July 2022

Contents

List of Figures

Acknowledgement

I am tremendously indebted to my supervisor **Dr. Pankaj Kumar Keserwani**, Assistant Professor, Department of Computer Science and Engineering, National Institute of Technology Sikkim for his invariable guidance and assistance throughout the project. His advice and suggestions have been prized in the development and progress of the content. Furthermore, the skills and knowledge which I have gained throughout this project I perceive as very valuable and significant for my future.

I take this opportunity to acknowledge all professors and research scholars who have provided their valuable experience throughout this entire curriculum and led to my piece-meal growth as a student. Finally, I express my deepest gratitude to my family & friends for their untiring encouragement and unconditional support.

Shashi Saurabh Sinha

Roll No: B180043CS

Computer Science & Engineering

National Institute of Technology Sikkim

Ravangla, South Sikkim-737139

Abstract

For many years, people have seen one other in various ways. When we meet people, we see them through their looks and hear them through their voices. In computer systems, verification (authentication) is usually dependent on an individual's ownership (key, magnet, or chip card) or personal information (PIN, password). Keys and cards, on the other hand, are often stolen or lost, while passwords are frequently forgotten or exposed. The advantages of biometric authorization are that it requires the user to be there and avoids the inconveniences of passwords and PINs.

The goal of our project is to create a multi-model biometric verification system that could successfully validate a person's identification by matching the scanned fingerprint, matching face and matching voice at same time. The project's purpose is to build and improve the security of system by using the fingerprint scanner and face verification and voice verification processes on Android for ultimate deployment in a real-time system. In this paper discusses how we developed this system and then analyses the outcomes.
Keywords: Face detection, Biometric, Fingerprint, Voice, Multi-Model Biometric, Android

CHAPTER-1

INTRODUCTION

1.1 Introduction: -

Biometric verification has often been recognized as the most trust proof, or at the very least the most difficult to fake or spoof. Diagnostic and verification systems have been physically based aspects in the IT industry since the early 1980s. These biometric methods were sluggish, intrusive, and repetitively costly, but they seem to function in certain high-security circumstances since they were frequently employed to monitor access to vast frames or visual constraints logging in to a few people again and over again. Computers are now lot quicker and less expensive than they were twenty years ago. This, along with new, low-cost gear, has rekindled interest in biometrics.

Identify theft and management or disclosure of data and intellectual property connected to increasing concerns in this computer-driven world. We all have several accounts and use a large number of passwords on an increasing number of machines and websites. It is getting more challenging to maintain and manage access while securing both user identification and computer data and systems. The principle of authentication, which guarantees the user is who they say they are, is fundamental to all security.

To get more trustworthy verification or identification, we must employ something that accurately portrays the individual. Biometrics offers automated techniques of authenticating identity or identify based on quantifiable or behavioral attributes such as fingerprints, voice, or facial recognition. Features are quantifiable and distinct. These characteristics should not be duplicated, but it is frequently easy to generate a clone that the biometric system accepts as the original sample. This is a frequent circumstance in which the degree of protection given is determined by the amount of money required by the fraudster to get unauthorized access.

Biometric data is individual private information that is uniquely and permanently connected with a person and, unlike credentials or keys, could be changed. Once an opponent breaches a user's biometric data, the data is gone permanently, perhaps resulting in a large financial loss. As a result, one key problem is how to preserve a person's biometric data after it has been gathered.

1.2 History and development of Biometric: -

Frank Burch, an optometrist, advocated the use of patterns for identity information in 1936. By the 1980s, the concept had featured in James Bond films, but it remained science fiction and speculation. This notion was patented in 1987 by two additional ophthalmologists, Aram Safir and Leonard Flom, and in 1987 they invited John Daugman to attempt to construct practical algorithms for this iris identification. Daugman's patented methods from 1994 serve as the foundation for all modern iris recognition systems and products.

The Daugman algorithms are owned by Iridian Technologies, and the method is licenced to numerous other organizations who act as system integrators and creators of specialized platforms that use iris recognition. Several devices have been created in recent years to acquire its photos across a range of distances and in a number of applications. In 1996, Sensor, a licensee, developed an active imaging system that employed specialized cameras in bank ATMs to capture IRIS pictures from up to one meter away. From 1997 to 1999, NCR Corps and Diebold Corp successfully tested this active imaging technology in cash machines in a number of countries. A new and smaller picture device is the low-cost "Panasonic Authentic" camera for portable, laptop, e-commerce, and other information security applications. Based on iris recognition kiosks at airports, Eye ticket has developed ticket-less air travel, verification, and security processes. Daughman's methods are now employed in a range of products by firms all around the world.

1.3 A biometric system's basic structure is as follows:

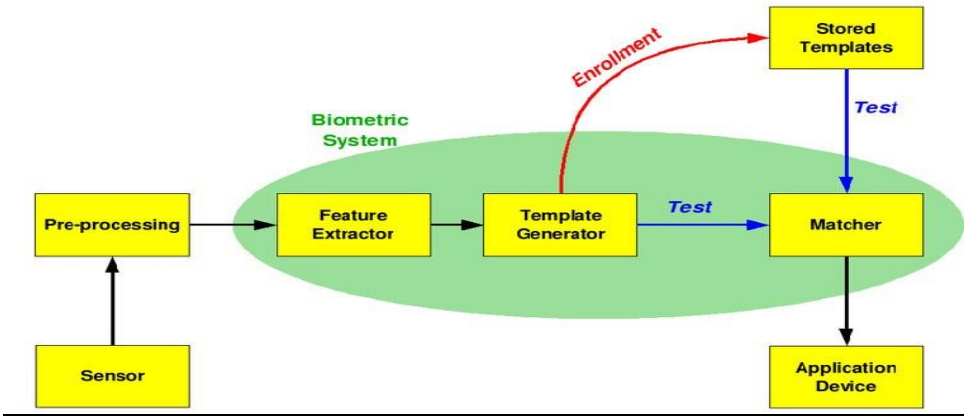

Figure 1 Structure of a Biometric System

For biometric authentication, a recorded or enrolled biometric sample (biometrics pattern or identifier) is compared to a freshly obtained biometric trait (for example, a fingerprint captured during a login).

A sample of the biometric property is acquired at enrolment, analyzed by a computer, and preserved for future comparison.

In Verification mode, the biometric system identifies a person from the whole increase the participation by searching a database for a physical match. A whole dataset, for example, may be searched to guarantee that no one has claimed for payments under two distinct identities. This is referred to as "one-to-many" matching.

A system may also be used in Verification mode, which involves the biometric system validating a person's declared identity using a previously registered pattern. This is also known as "one-to-one" matching. For most computer access or network access circumstances, verification mode would be used. Instead of a login, a user can enter an identity, user name, or puts a token including a card slot, but a mere touch of a finger or a peek at a camera is enough to validate the user.

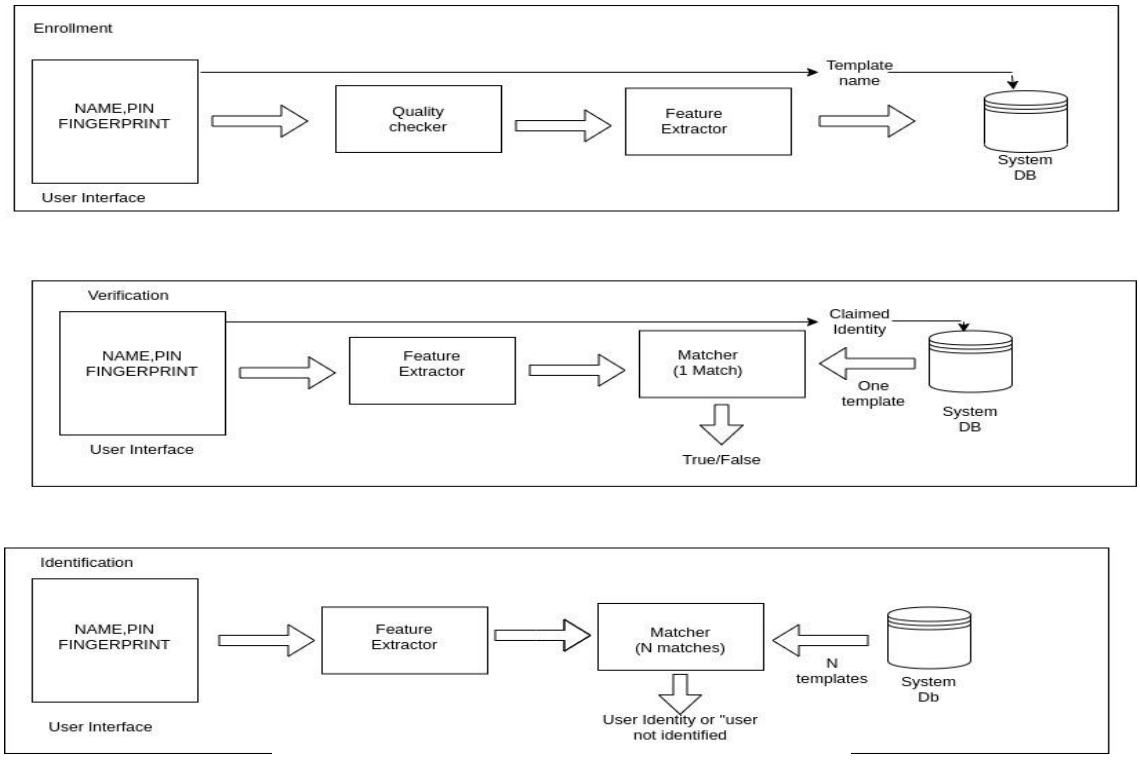

Figure 2 Enrollment, Verification, Identification

1.4 Authentication:

In many respects, the question "How do I know who you are?" is critical. Unless it is adequately replied, the identity is incomplete, and no authorization is available or required. But how does the system know the user is who he or she says he or she is? Simply inputting your password does not establish your identity. Someone else might be using your password. A thorough verification method is the solution. In general, the three factors listed below may be used to verify a person.

1. The user is aware of something. This is a reused username, a password, a unique ID number, or a user-only information, including a mother's forename.
2. Something that the user has. A key, a magnetized card, an id cards, or a special identification gadget (called a tokens) that creates an OTP or a particular answer to a server-issued challenge might be used.
3. The user is missing something. This is determined by a certain physical trait or features. Examples of biometric verification include fingerprinting, retinal (eye) patterns, gesture recognition, voice control, face recognition, typing pattern recognition, and signing strength.

These authentic elements are given below in order of strength, since they affect how tough it is to walk or lie. Each of these options offers some level of protection on its own. However, each has its own set of issues or flaws.

Finally, if the route is in danger, a person cannot be given a new identity. You may alter your passwords or security token, but not your biometrics or eye patterns.

1.5 Two-Factor Authentication: -

Experts recommend combining two of the three techniques for maximum security, a practice known as two-factor authentication. To utilize a prevent cyber that creates a one-time login, for example, you may need to input the Identification number with in token itself. A card key may also be used in combination with a biometric system. This is what occurs when you enter an airport ticket desk. You provide your identification ticket. Then display the picture ID of a certain kind. It’s something you carry with your, and the biometric (something you are) except

that the clerk must determine if the photo on the card resembles you. Two-factor authentication adds another layer of safety to the verification process by making it more difficult for attackers to obtain access to a person's devices or login details because, even if the victim's password is obtained, a password alone would not suffice to pass the authentication check.

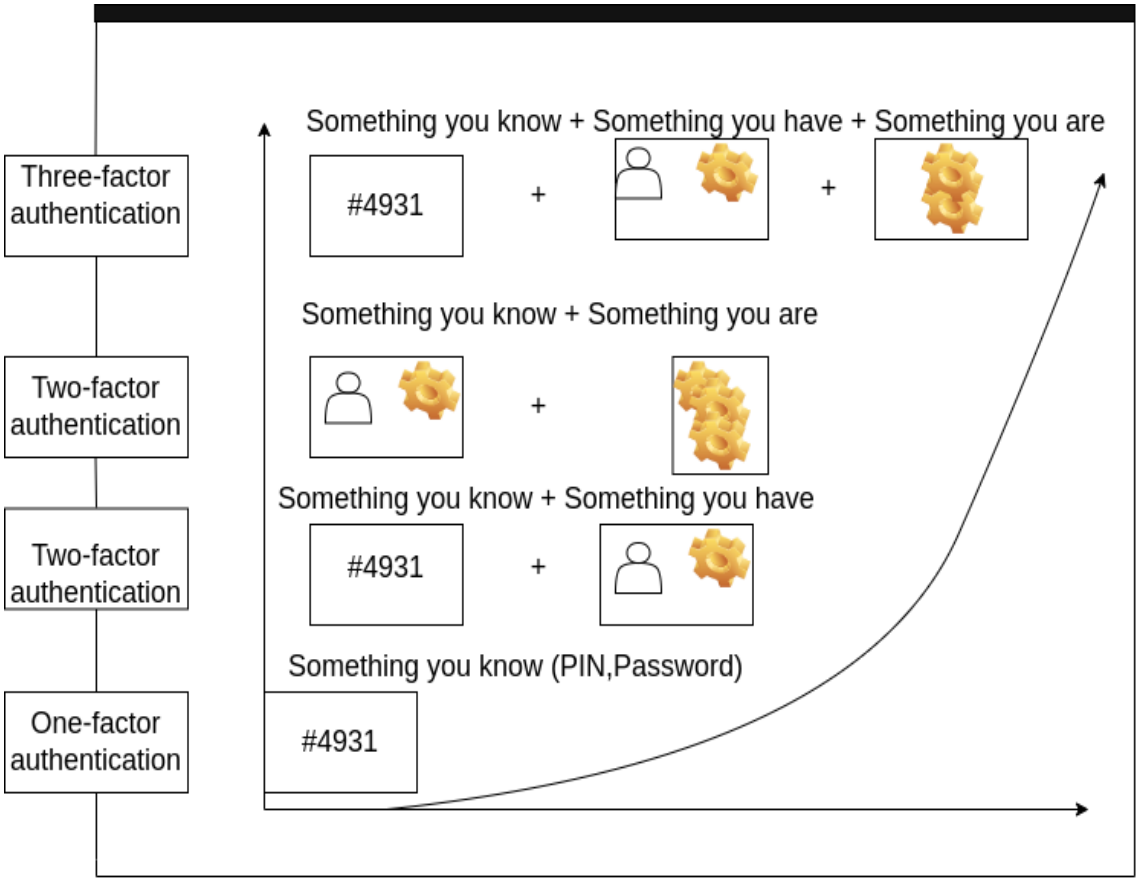

Figure 3 Types of Authentication

1.6 What is Biometric: -

The term biometrics comes from the Greek word's bio and metric. The phrase Biometrics refers to biometric identification metrics. Biometrics makes use of a number of physical or behavioral characteristics. Fingerprints, hand geometry, retina, Iris, facial expressions, and other biometric measures are common. Signatures, voice recordings, key beat rhythm, and other typical biometric information are included. With the growing significance of security, it is critical to guarantee that only authorized users have access to the network. Biometrics validation has experienced substantial increases in consistency and validity in recent years,

with certain features giving great performance. Even the greatest biometric features available today, however, have a number of issues, some of which are connected to the technology itself. Because of non-standard biometric characteristics, biometric authentication systems often have registration issues. poor precision due by noisy data gathering in specific locations Because of environmental noise, signal distortion, changes in biometric traits, and variability, biometric readings fluctuate naturally. Diagnose based on a single biometric component may be insufficient and has limited capacity to detect fraud.

1.7 Type of Biometric Verification: -

- Fingerprint identification.
- Face recognition.
- Iris recognition.
- Hand geometry.
- Signature recognition.
- Retinal scanning
- Voice verification

1.8 Biometric System Components and Process: -

A biometric system typically has four major components.

1. Well how scan and capture a digital edition of a live unique biometric element.
2. Raw data processing software is converted into a format (referred to as a template) that may be used either storage and matching.
3. Being software that compares a pre-stored biometric data to a live example template.
4. A visual interface for communicating the match impact with the app. The biometric system has two distinct categories: identification and verification

- **Enrollment: -** During the registration procedure, a unique biometric sample is collected The components retrieved from a biometric sample (E.g. - picture) are then combined to form a user biometric template. This base model is saved on a device ID card for haters to use during the matching process.
- **Matching: -** It accepts data and displays the biometric numerical simulations. A biometric sample was also collected. To construct a "live" biometric template for the user, unique characteristics are derived from a biometric sample. This fresh design is

then compared to a previously created template, and the same amount of points (points) are created based on the two templates' common denominator. The system's designers set the limit of this school to assure depending on the system's safety and comfort criteria.

Biometrics can be used in biometric enabled security systems for two primary purposes: -

- **Identification** (1: N comparison /one-to-many or): - It determines whether a person exist among the number of people registered by comparing a live sample template to all the templates stored in the system. Identification can confirm that a person is not registered with any other identity or is not on a pre-determined list of unauthorized persons. The biometric of the person under consideration for registration should be compared with all the biometric records. For some authentication applications, the biometric identification process is used at the time of registration to ensure that the person is not already registered.

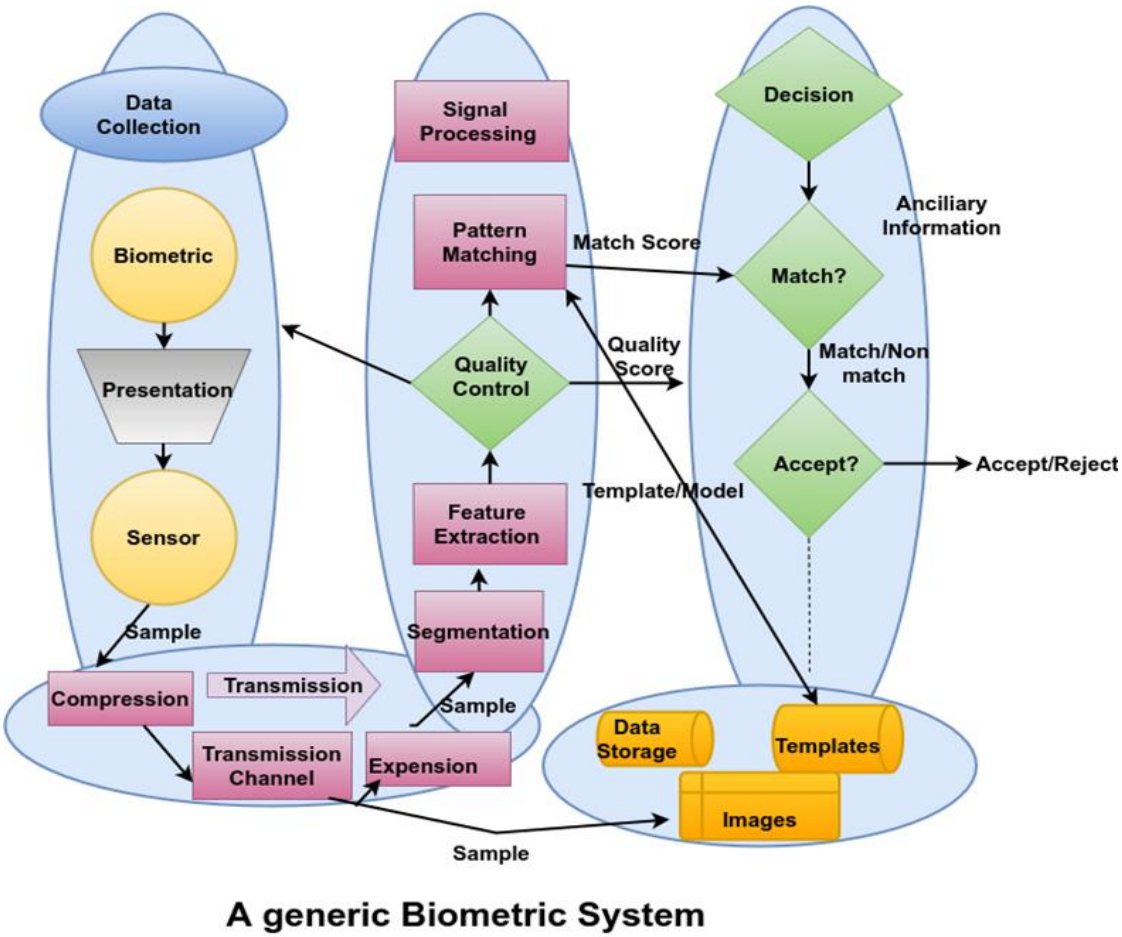

Figure 4 Generic Biometric System

- **Verification** (1:1comparison or one-to-one) estimate the live biometric template is the same as the registered template record. This requires a "claim" for the identity of the person you want to verify in order for the record template to be accessible. An example would be a smart card proof presentation and a live sample biometric template with a registered template stored in a smart card memory. Another example would be the insertion of a username or ID number that could point to a registered template record on a website.

1.9 Different types of Algorithm in Biometric Verification: -

The ability of four machine learning algorithms to combine several biometric modalities to create a multimodal biometric security system. Among the methodologies examined are Gaussian Mixture Models (GMMs), Artificial Neural Networks (ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs). Biometric fusion results in security systems with greater recognition rates and reduced false alarms as compared to unimodal biometric security systems. A variety of patterns from a well-known benchmark biometrics database were used for supervised learning, while patterns from the same database that were not included in training dataset were used for validation/testing. According to the algorithm comparison, the biometrics fusion system beats both the basic unimodal systems and other fusion procedures presented in the literature.

1. **Supervised Fusion Algorithm: -**In multimodal biometric systems, fusion at the matching score level is the most common method. This is due mostly to the ease of access and availability of matching scores in different biometric modules. The (dis-)similarity score produced by a biometric module is the input to a fusion algorithm at the matching score level. There are many methods for integrating scores at the matching score level. In this method, the output scores of separate matching algorithms form the components of a multidimensional vector; for example, a 3D vector is formed if scores from a face, gait, and voice matching module are available. The resulting multi-dimensional vector is then categorized using a classification method such as Support Vector Machines (SVM), Fuzzy Expert Systems (FES), neural networks, and so on, to fix the 2-class classification problem of classifying the output sequence into either "impostor" (unauthorized users) or "genuine" (approved users) (authorized users, or clients). The strategy has the benefit of allowing for inhomogeneous scores, such as a mix of similarities and distances arranged in discrete intervals. As a consequence, classification fusion requires no pre-processing. In supervised learning, a training set of patterns (or inputs) with related labels is

provided to the learning algorithm (or outputs). Patterns are often represented as attribute vectors, and once these vectors are accessible, machine-learning methodologies ranging from basic Boolean operators to Bayesian classification and more complex algorithms may be used. A fusion algorithm's performance is determined by system configuration. This tuning often consists of a set of hyper-parameters that may be changed manually (for example, the type of kernel in SVMs, the number of chromosomes in Genetic Algorithms (GA), and so on) and a set that is changed during the training process. Training is critical to the effectiveness of the fusion system because it enables the algorithm to estimate (learn) the clients and impostor spaces.

This research included four cutting-edge fusion techniques: Support Vector Machines, Fuzzy Expert Systems, Gaussian Mixture Models, and Artificial Neural Networks. Each of these systems uses a different approach to integrating unimodal biometric information to determine if the person is a client or an imposter.

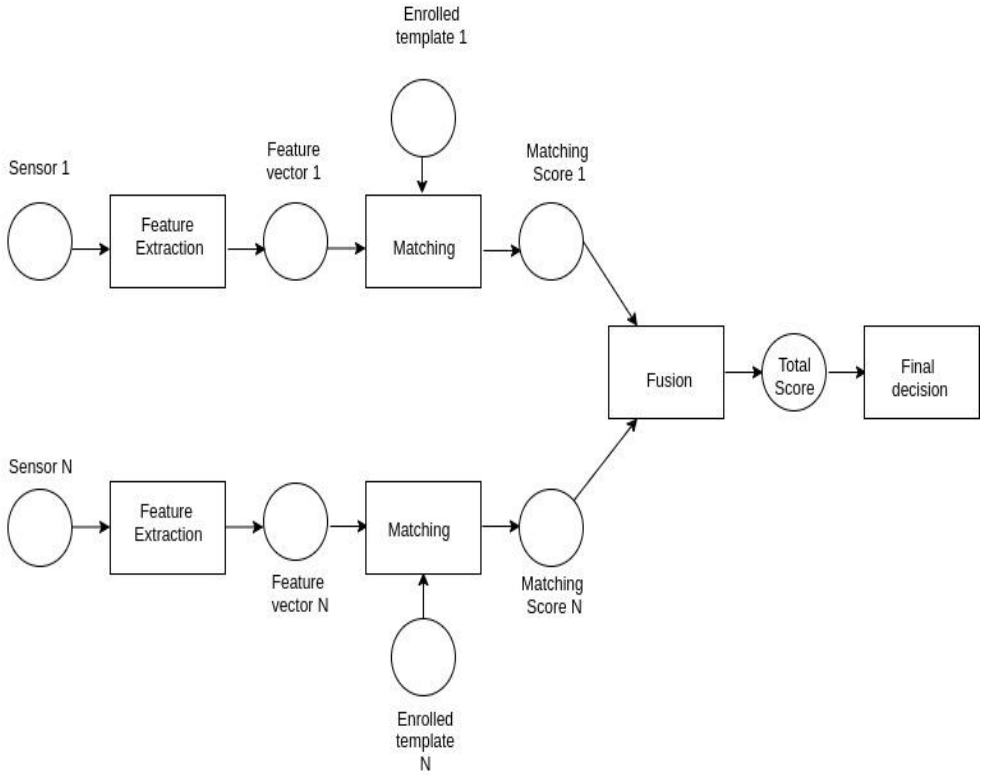

Figure 5 Supervised Fusion Algorithm

2. **Support Vector Machine: -**A common SVM implementation has been created. The input data was transferred to a higher fourth dimension where it was linearly separable using a radial basis kernel function. To handle any nonlinearities between

the input vectors and their associated class, the radial basis kernel (RBF) was applied. It also has fewer hyperparameters than the polynomial kernel, which simplifies training.

Following the kernel selection, the technique selects the optimal pair of and, that is, the pair with the highest cross-validation accuracy. Following the addition of the criteria, the training set was divided into equal-sized subsets, with one subset serving as the validation dataset and the remaining subsets being used to train the classifier. The procedure was repeated until all of the subsets were used as validation datasets. Grid search was used to choose and, which required analysing exponentially growing sequences of and. Complete enumeration trials were used to compute the penalty levels for each of the two groups ("Genuine" and "Impostor").

The final trained SVM model was then utilised with the best pair to evaluate classifier performance on the test dataset, which contained "unknown" characteristics that had not been used for SVM training.

3. **Gaussian Mixture Model: -**Bayesian categorization and decision making are based on probability theory and the idea of selecting the “with the highest probability or lowest risk (anticipated cost). In an appropriately chosen feature space, the Gaussian distribution is often a suitable approximation for a class model shape. The assumption in a Gaussian distribution is that the class model is a model of one basic class. If the underlying distribution is multimodal, however, this model will be unable to describe it coherently. Because the Gaussian Mixture Model (GMM) blends several Gaussian distributions, it may represent distinct subclasses within a class. A weighted sum of Gaussian distributions is used to define the probability density function.

   A Gaussian mixed probability density function, to be precise. Unsupervised learning is used to estimate the Gaussian mixture parameters for one class since the samples are produced by independent components of the mixture distribution and it is hard to tell which sample was generated by which component.

   A GMM with four mixture components was created. Extensive testing was used to estimate the component weights.

4. **Artificial Neural Network: -**Artificial neural networks (ANNs), also known as neuronal networks (NNs), are networks that are modelled after the biological neural networks seen in animal brains.

   An ANN is made up of a network of connected units or terminals called artificial neurons, which are modelled after neurons in the human brain. Like synapses in the

human brain, each link may send a signal to other neurons. An artificial neuron receives impulses, processes them, and may interact with other neurons to which it is connected. Each neuron's output is determined by some non-linear function of the sum of its inputs, and the "signal" at a connection is a real number. The connections are referred to as edges. As learning happens, the weight of neurons and edges often fluctuates. The weight changes the strength of the signal at a connection. In neurons, a threshold may exist that causes a signal to be delivered only if the aggregate signal crosses it. Neurons are often organised in layers. Various transformations may be done to inputs of various levels. Signals are routed numerous times from the first layer (the input layer) to the final layer (the output layer).

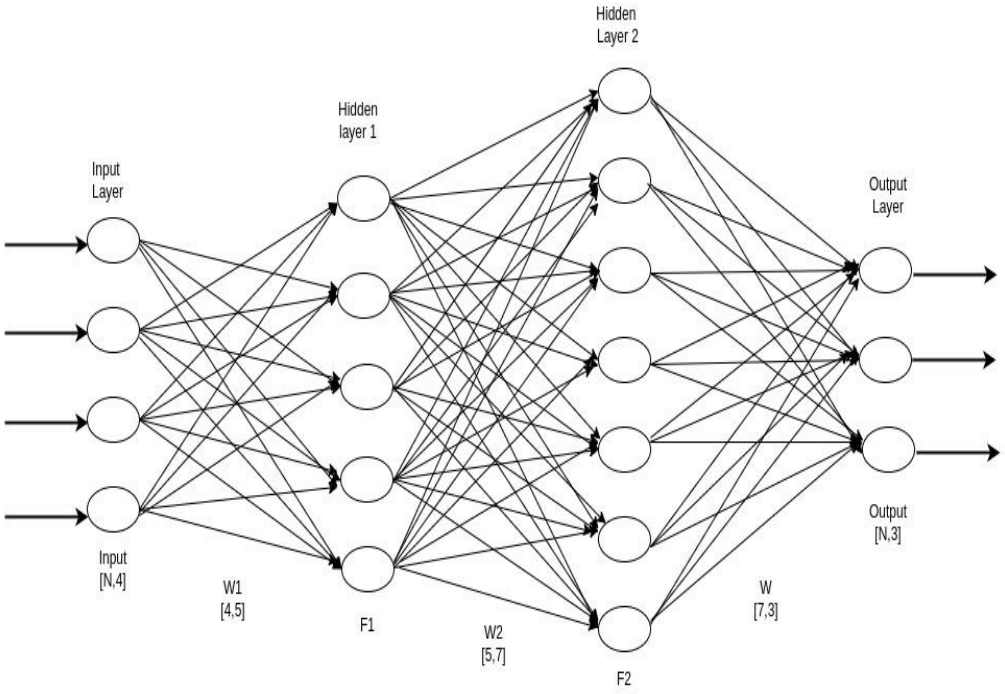

Figure 6 Artificial Neural Network

CHAPTER -2

LITERATURE SURVEY

Find Error in Biometrics and Make This Safe from Normal Attack. Prevent biometric systems from accessing unreasonable automatic detection and use multiple biometric modals Problems in uni-modal. This type of error is deliberately trying to avoid this.

In this study, we outline the many challenges that prohibit biometric systems from accurately recognizing each son. We also demonstrate how using different biometric approaches might mitigate some of the issues associated with uni-modal biometric systems. Finally, we address biometric system dangers and strategies for protecting biometric systems from typical threats.

Fingerprints, facial recognition, hand geometry and the iris recognition used can be concluded as simultaneous verification and verification is very promising on the iris, fingerprint and vanity plum policies.

As seen in the preceding section, biometric systems have a lot of constraints that restrict their usage in real-world systems. As a result, the assessment of biometric systems is given serious consideration in the literature. Such studies may be classified into three broad areas, as shown in the diagram:

1) quality of the data,

2) usability, and

3) security.

We give these assessment factors in this part, discussion.

Biometrics verification is a burgeoning and contentious topic, with privacy and copyright concerns expressed by civil liberties organizations. Biometric rules and regulations are still in effect today, and biometric industry standards are being evaluated. Facial recognition biometrics have not yet achieved the standard level of fingerprints, but with continuing technological demands and the danger of terror, scientists and biometric programmers will boost this security technique in the twenty-first century. Biometric traits may be split into two categories in the present day.

The primary goal of information security is to prevent unauthorized access to and correction of data. This may be accomplished by creating rules, processes, programs, and algorithms that promote confidentiality, integrity, and security (CIA). As the first line of defense in security systems, verified

authentication has become a highly required indication of data protection, particularly as the Internet of Things (IoT) comes to the surface.

Big Data refers to a massive, complicated, and ever-increasing number of multi-sources, diverse data sets. Big Data is presently quickly developing in all sectors of research and engineering, including environmental, biological, and biomedical sciences, due to the fast growth of networks, storage systems, and the power of data collecting. From a data mining standpoint, this study provides a HACE theory that emphasize characteristics of Big Data transformation and suggests a Big Data processing model.

It emphasizes the importance of a biometric system for pattern classification and its functions by collecting, extracting, and analyzing biometric data for each person. Multi-modal biometric systems have higher precision than uni-modal biometric systems, and technique analysis is substantially more difficult. In this work, the researcher discusses the many forms of multi-modal biometric systems, as well as the various techniques of integrating the judgments utilized and their capabilities across different metric biometric systems.

Presented a multi-modal biometric system for personal verification using voice and facial data There are two dividers that use the sum rule after the norm. Multi-modal biometric authentication provides more than simply authentication validation. Using Linear Prediction Cepstral Coefficients, the face system designed to employ 2D Linear Discriminate Analyses is compared to a speech pathologist as a feature key.

Face detection is a computer technique that uses an abstract (digital) picture to estimate the position and size of a person's face. In digital imaging, facial traits are detected but other things such as trees, buildings, and bodies are disregarded. It is a ‘specific condition' for the acquiring of an object category in which the function determines the position and size of all items in the picture that belong to a given category. Face detection is a 'normal' method for detecting local face emotions. The goal of local face recognition is to discover the size and location of a given face number (usually one). There are two methods for locating a portion of a face in a given picture: the element technique and the image base approach. The basic feature technique attempts to extract picture characteristics and is complemented by face feature information. While the image basis technique seeks the greatest possible similarity between learning and image testing.

S. No	Year	Methodology	Reference
1	2017	Find Error in biometric and make this safe from common attack. Prevent biometric systems from achieving foolproof automatic person recognition and use multiple biometric modal. Which is problem in uni modal	[3]
2	2019	Fingerprints, Face recognition, hand geometry and iris recognition used. it can be concluded that simultaneous authentication and verification is most promising for iris, finger print and palm vain policies.	[5]
3	2018	It works on Uniqueness, Permanency, Collectability and Acceptability. It provides a better security comparing to traditional solutions. These systems suffer from solve several limitations.	[9]
4	2019	A combination of biometric Fingerprint scanner, cryptography, OTP used for better security. Design and implement an application using biometry and cryptography	[1]
5	2020	This propounds a multimodal biometric user verification system by integrating. fingerprint; facial recognition and lip print images. In this it uses lip print verification which make it unique and more secure.	[7]
6	2021	Accurateness, serviceability and reducing cost have made the biometric technology a secure. In this paper it deals with almost all verification process and also compare its advantage and disadvantage and compare between all on feature.	[2]

CHAPTER-3

PROBLEM DEFINITION

3.1 Objective:

Biometric Most verification in today's world depends on fingerprint identification, face authentication, voice and video recognition, and behavioral settings. The attack ecology has grown to include techniques for bypassing the authentication mechanism using false video, audio, and even behavioral aspects. The attack vectors leverage deep learning skills to prepare and launch the assault in novel and automated ways. Because biometric authentication is so important in digitalization, such flaws might lead to identity theft, transaction integrity, and financial loss. They would also erode end-user trust and impair the attainment of digitalization goals. Criminals use artificial intelligence and machine learning, namely deep learning and generative adversarial networks, to exploit biometric authentication for a range of destructive and illegal purposes. Image/video/audio morphing or doctoring is used to produce phony videos for financial fraud. Biometric authentication opens up several digitization opportunities. Digitization requires a robust defense against such complex attacks.

3.2 Present System: -

3.2.1 Face Recognition: -Face recognition is by far the most natural biometric diagnostic tool. Everyone can learn to distinguish one person from another. Until recently, facial recognition was not considered a science. To picture the face, any camera (with suitable resolution) may be used. Any scanned picture may be reused. When we need precise findings, we frequently photograph the source (this camera or camera). Face detection algorithms often rely entirely on grayscale data. Colors (if present) are just used to help locate the picture inside the image. The lighting conditions required are dictated by the quality of the camera. In low-light conditions, isolated objects may be difficult to notice. Infrared cameras may also be used in conjunction with facial recognition systems. Most face recognition systems require the user to stand a certain distance away from camera and gaze at it directly.

A technology that has caught many people's curiosity, yet its capabilities are frequently misconstrued. Extensive claims for face recognition technology have been made on occasion, but have proved difficult, if not impossible, to back up in training. It's one thing to match two static photographs (which is all some systems do - not biometrics at all), but it's quite another to detect and verify the identity of a person inside a group surreptitiously (as some systems claim). It's simple to understand why face recognition is tempting from the user's standpoint, but be realistic about the humankind's capabilities. So far, facial recognition systems have had

minimal practical success. However, there has been improvement. Continued progress in this area is being made, and it will be fascinating to watch how future implementations fare. If technological barriers can be overcome, face recognition might become the dominant biometric approach.

- **Different Approaches of Face Recognition: -**
  - Geometry (element-based) and photometric face recognition algorithms are the two types (visual-based). As the researchers' interest in face recognition evolved, several new algorithms were created, three of which were extensively researched in facial recognition literature. There are two kinds of recognition algorithms
  - **Geometric:** It is based just on geometric connection or spatial arrangement of the earth's face characteristics. This implies that the key geometric characteristics of the face are recognized first, such as the eyes, nose, and mouth, and the face is split based on the geometric various distances between the pieces.
  - **Photometric stereo:** It is used to restore item composition in a sequence of images taken in different lighting conditions. A gradient map generated by a typical spatial network determines an object's form.
- **Popular recognition algorithms include: -**
  1. Eigenfaces for Principal Component Analysis
  2. Analysis of Linear Discrimination
  3. The Fisher face technique is used to match elastic bunch graphs.

Work on face detection may be broken into two parts. The first stage is a separation function, which takes an unexpected picture and inserts and subtracts a binary value of yes or no, indicating if a face is present in the image. The second phase is a face-to-face exercise in which you insert and replace any face or faces inside the picture as an interconnect box (x, y, width, height).

- **The face detection system is comprised of the following steps: -**
  1. **Pre-Processing:** Images can be processed before being put on a network to eliminate face variability. Cropping photographs with the front faces to include just the front view yields all excellent instances of face painting. After that, all cropped photos are ready to be lit using conventional methods.
  2. **Classification:** In these instances, neural networks are trained to identify photos as facial or non-facial. For this challenge, we utilize both our neural network and the MATLAB neural network toolkit. To enhance outcomes, several network configurations are examined.

3. **Localization:** The trained neural network can then be used to search for faces in images and, if found, to locate them inside a bounding box. Various Face Features on which work has been done include: Position Scale Alignment Illumination.

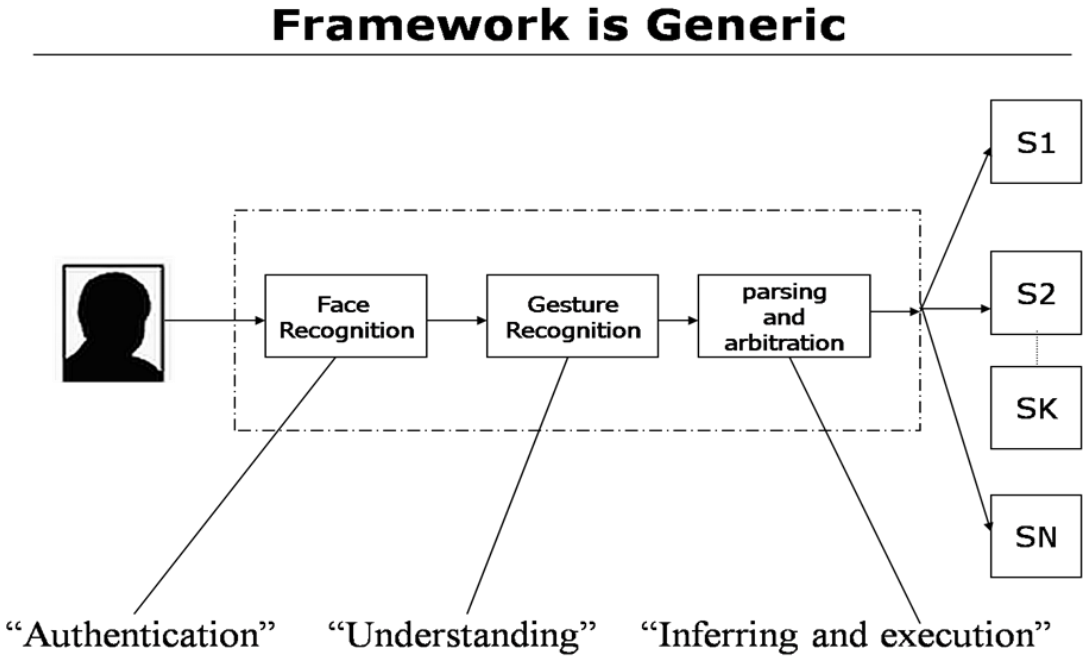

Figure 7 Framework is Generic

3.2.2 Fingerprint: - Fingerprint recognition is one of the earliest biometric methods. Fingerprints were previously employed in ancient China to identify the author of this literature. Their legal applicability from the previous century is widely established and enables for finger movement = crime. This has raised some questions about whether users would embrace fingerprint-based systems. As these initiatives proliferate and become more prevalent, the situation improves. Law enforcement organizations have been using systems that can automatically verify the intricacies of human fingerprints since the 1960s. Sandia Labs' research comparing different biometric technologies used for diagnosis in the early 1970s has been authorized by the US government. According to the findings of the research, fingerprint technology has the potential to deliver outstanding diagnosis accuracy. The study is no longer relevant, but it has shifted the emphasis of research and developments in fingerprint technology since its publication.

Fingerprint authentication may be a viable alternative for in-house systems when users can be adequately explained and trained and the system is used in a controlled environment. Because of their cheap cost, compact size (easily incorporated into keyboards), and simplicity of

integration, fingerprints seem to be used nearly entirely in the workstation entry application area.

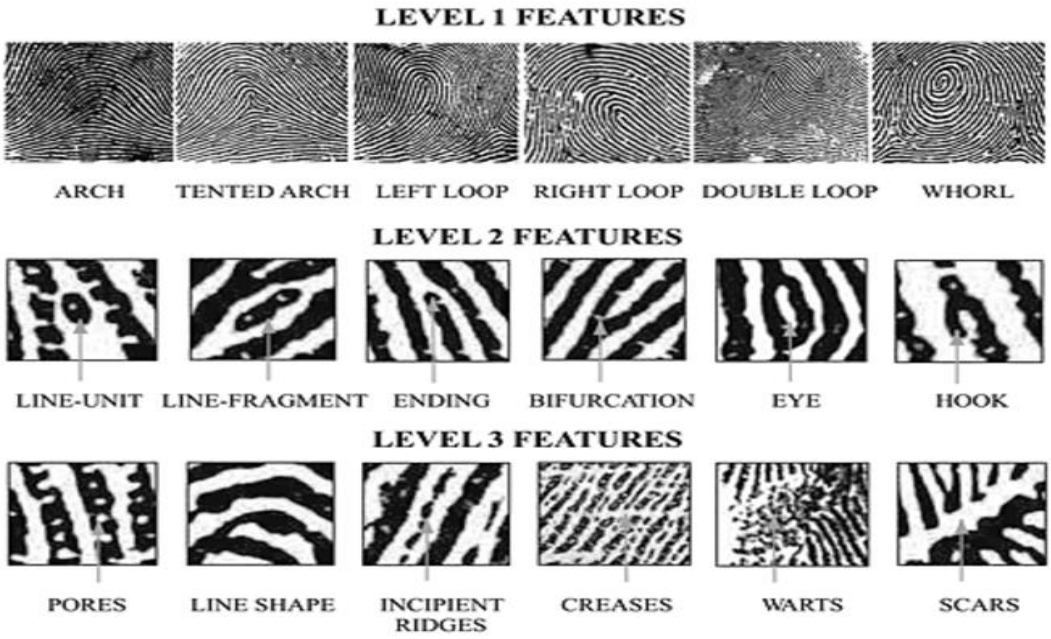

Figure 8 Level Features

- **Readers of fingerprints**-We must first get digital fingerprints before proceeding. Ink is used in the conventional way to print fingerprints on paper. This piece of paper is then scanned using a regular scanner. When an old paper-based website is digitized, a fingerprint recovered at a crime scene is evaluated, or in AFIS law enforcement systems, this approach is seldom employed nowadays. Alternatively, live modems operators are utilized. They no long need ink. These interactive textbooks are often based on optical, thermal, silicon, or ultrasonic principles. At the present, optical fingerprint scanners are the most frequent. It is based on the change in expression in locations where the popular lines of the finger come into contact with the student's area.
- **Processing of fingerprints**-Fingerprints are not similar and are seldom saved as bitmaps. There are two types of fingerprint matching strategies: minutiae-based and communication-based.

Minutiae-based strategies first locate minutiae points and then map out their associated location placement. Minutiae are distinguishing characteristics of a fingerprint pattern, such as hind ends, double splits, splits, dots, or islands (see photo on next page). In recent years, the comparison of automated fingerprints has often relied on minutiae. The minutiae issue is

that it is difficult to extract minutiae points properly when the fingerprints are low. The worldwide pattern of hills and canals is ignored by this strategy. The link-based technique overcomes some of the shortcomings of the minutiae-based approach. It does, however, have certain restrictions. Collaborative techniques need an exact registration point position and are impacted by picture translation and rotation.

Fingerprint readability is affected by a range of functions and environmental conditions. Age, gender, employment, and race are all factors. A young Asian girl miner is seen as a challenging topic. A shockingly big number of persons have missing fingers, with the front left finger accounting for 0.62 percent of the total. A typical fingerprint picture obtained by a live fingerprint reader has roughly 30 minutiae. The quantity and distribution of minutiae areas vary depending on fingerprint picture quality, finger pressure, humidity, and positioning. The biometric system tries to identify minor differences between the current distribution and the stored template throughout the decision-making process. A concurrent choice is made based on the probability and difficulty of the desired modifications. Resolution typically takes between 5 milliseconds and 2 seconds.

The speed of the decision is occasionally affected by the degree of security, and the negative answer frequently lasts longer than the pass (often even 10 times longer). According to our understanding, there is no direct relationship between the speed and accuracy of the same algorithm. We've seen quick and accurate matching algorithms becoming more sluggish.

3.2.3 Voice Recognition: -Speech recognition is a technique that allows a phone to capture human speech using a microphone. A speech impairment later detects these words, and the system finally releases recognizable terms. The voice recognition process consists of many processes, which will be explored in detail in the following paragraphs.

The voice recognition system has the advantage of seeing all of the words said by a person; nevertheless, the performance of a speech recognition engine is likely to be affected by the quantity of objects. The key criteria that are thought to be reliant on speech recognition engines include names, many users, and a loud environment.

Given the prevalence of voice communication in everyday business transactions, this may be an attractive method. Some designs concentrated on wall-mounted readers, while others sought to incorporate voice verification into ordinary telephone handsets. While several speech verification devices have been introduced to the market, many of them have failed in practice owing to transducer variability and local acoustics. Furthermore, the registration procedure for voice verification has typically been more onerous than for other biometrics, adding to a poor perception of the technology in certain quarters. However, considerable work has been and continues to be done in this environment, and it will be fascinating to see how things go.

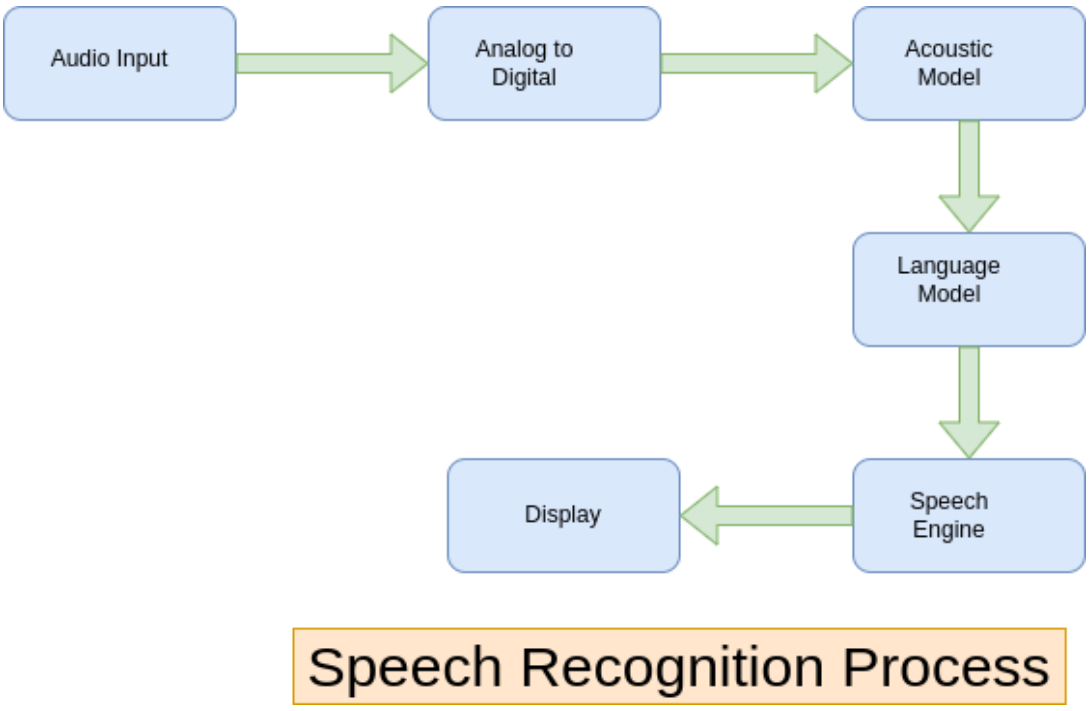

Figure 9 Speech Recognition Process

- **Type of Speech Recognition system: -**Speech recognition software is classified into many groups depending on its ability to identify words and word lists. The following are some voice recognition categories:
  - **One Speech**: -Individual words often entail standing between two words; this does not imply that it takes just one word, but rather that it demands only one utterance at a time.
  - **Connected Speech**: -Connected words or connected speech are similar to a single speech but allow for diverse expressions with a gap in between.

- **Continuous discourse**: -98.8% Continuous speech, often known as computer dictation, enables the user to talk naturally.
- **Automatic Speech**: -It may be viewed of as a natural and repeating statement at its most fundamental level. An ASR system with autonomous speaking capability should be able to handle many features of genuine speech, such as word combinations, "ums" and "ahs," as well as tiny languages.

➢ **Components of the Speech Recognition Program**

- **Voice input**: -The pc sound card generates an equivalent digital representation of the incoming sounds using the microphone audio input mechanism.
- **Digital making**: -Digitization is the process of turning an analogue signal into a digital form that includes both sampling and measuring. Sampling is the act of converting a continuous signal into a distinct signal, while quantization is the process of reaching a continuous range of values.
- **Acoustic model:** -Acoustic Simulation An acoustic model is created by recording voice as well as writing text and then utilizing software to construct sound statistics that compose each word. To detect speech, it employs a speech recognition engine. The software's acoustic model breaks down words on phones.
- **Language Model**: -Many natural language processing applications, such as voice recognition, employ language modelling to collect language characteristics and predict the next word in a speech sequence. The software language model compares phonemes and words from a dictionary.
- **Speech Engine**: -The voice recognition engine's role is to translate the input sound into text; to do so, it employs a variety of data, software techniques, and statistics. Its initial job, as previously explained, is to transform information into an acceptable format for subsequent processing. When the audio stream is in the proper format, look for the best of the best. It achieves this by looking at the words you know, and when a signal is recognized, it provides the line of text that corresponds to it.

3.3 Suggested Solutions: -

The use of biometric verification in numerous areas of our society, businesses, and organizations has restored individual privacy while also preventing security concerns. Face Recognition and Voice Detection are two significant new technologies that provide authentication to every user while also protecting their authorization. Securing authorization

here refers to preventing duplicate identities and voices, because each human has his or her own distinct identity, even if the system is presented with two identical twins.

The first time a person uses a biometric system is during enrollment. Biometric information is acquired from the person during the enrollment process and kept in a database. In future usage, biometric information is detected and compared to the information recorded at the time of enrollment. If the biometric system is to be effective, the storage and retrieval of such systems must be secure. There are three phases to every biometric authentication or identification method:

- The first step (sensor/camera/mic device) from this we collect image, voice and finger image that acts as a bridge between the actual world and the system, collecting all necessary data.
- The second step includes the necessary pre-processing: cleaning up the acquired data, enhancing the input, and extracting the essential features. This step is critical because the right characteristics must be extracted as efficiently as possible. A template is usually out of a numeric vector or a graphic with certain properties. A template is a synthesis of the source's needed attributes. Elements of the biometric measurement that are not needed in the comparison technique are removed from the template to decrease file size, and the data is encrypted to protect the enrollee's identity.
- If a matching is accomplished, the acquired template is compared to other existing templates, evaluating the variance between them using an algorithm and a defined threshold. All three successful match results authorizes the user.

CHAPTER-4

PROPOSED MODEL

4.1 Methodology:

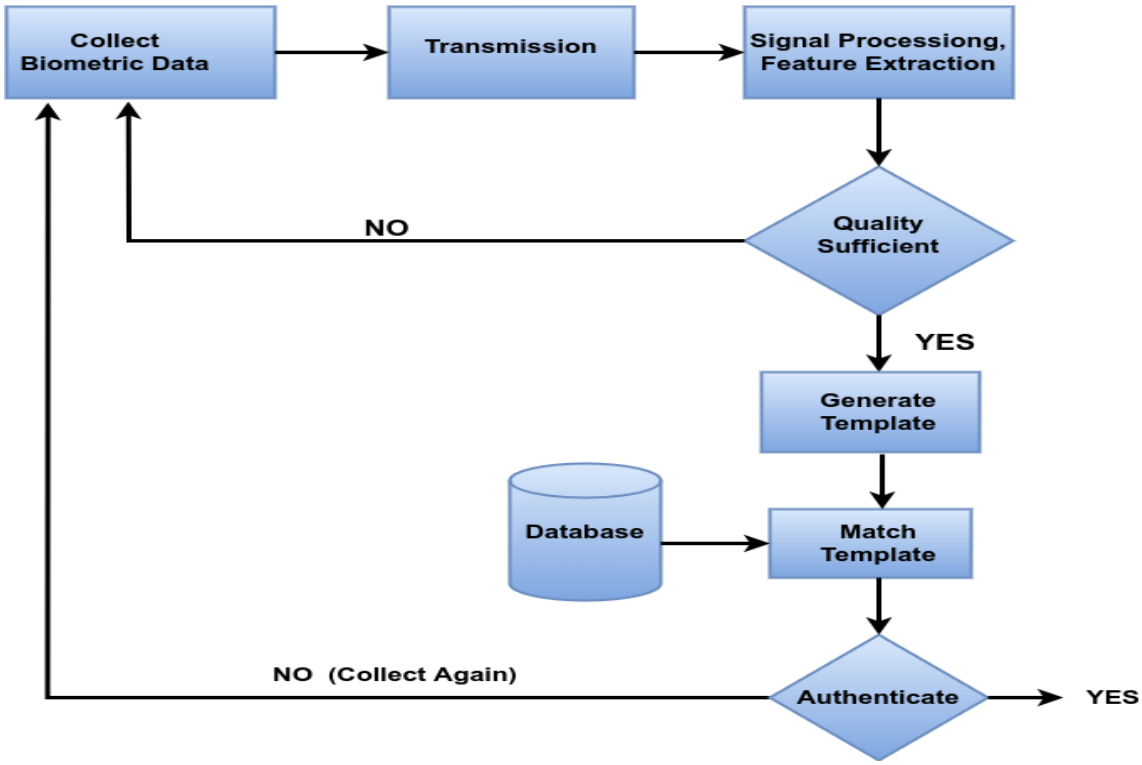

Figure 10 Methodology

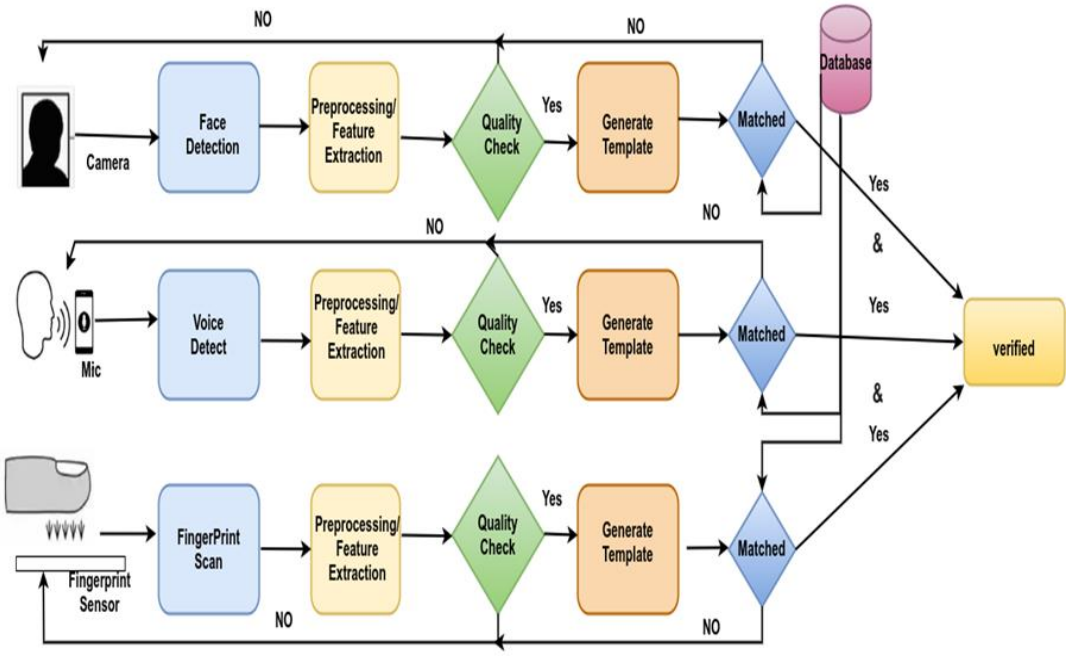

Figure 11 Three Factor Biometric Verification System

4.2 How does Face recognition Work?

You could be adept at recognising people's faces. You probably have no trouble recognising the face of a family member, friend, or acquaintance. You identify their face features, such as their eyes, nose, and mouth, as well as how they engage with others. That is how a facial recognition system operates, but on a much larger, computational scale. Recognition technology sees data where you see a face. That information can be saved and accessed.

So, how does facial recognition function? Although technologies differ, the following are the basic steps:

1. A photograph or video of your face is captured. Your face could appear alone or as part of a crowd. Your photo could show you gazing straight ahead or almost in profile.

2. The geometry of your face is read by facial recognition software. The distance between your eyes and the distance from your forehead to your chin are important considerations. The program recognizes facial landmarks – one system recognizes 68 of them – that are important in differentiating your face. As a consequence, your face signature was created.

3. Your facial signature mathematical formula is compared to a database of existing faces.

4. A decision has been made. Your faceprint might match one in a database of facial recognition systems

4.3 How does Fingerprint Work?

In fingerprint identification, pattern recognition is used to compare the arches, loops, and whorls of the fingerprint ridges to stored data. There really are three phases to the identification technique.

1. A snapshot of the fingerprint is captured. The images can be collected optically using reader's camera, electronically, or a combination of the two. The end result is a black-and-white digital version of the fingerprint ridges.
2. The fingerprint is then transformed into a numerical model, which retains the unique qualities of the fingerprint as a series of numbers, such as the arches and loops and their distance from others.

3. A recognized numerical model is compared to a stored numerical model to identify similarities (or models).
4. Fingerprint identification is used to verify a person's identity, after which the system may do the required actions, such as unlocking a door, granting access to software, or running a machine.

4.4 How Does Voice Recognition Work?

So, how exactly does voice recognition function? It uses technology to assess the biometrics of your voice. This comprises your voice's frequency and cadence, as well as your accent. Every syllable you say is split down into tonal components. This is then digitized and translated into your own distinct voice template. Artificial intelligence, machine learning, and deep learning are also used to power speech recognition. Machine learning then uses neural networks to put together the patterns and evolve from this data. This technology can be used to a wide range of systems, some of which are more sophisticated than others. However, voice recognition is capable of much more. Take, for example, Alexa. With the power of your voice, this sophisticated house aide can answer queries, play music, and switch off lights in your home.

4.5 Deployed as Mobile App: -

1. Add Face by using mobile camera
2. Image processing
3. Add Fingerprint by using fingerprint sensor
4. Add voice by using mic
5. Verify Face
6. Verify Fingerprint
7. Verify Voice

4.6 TensorFlow Lite: -

TensorFlow is a free open source software library. TensorFlow was created by Google Brain Team developers & researchers as part of Google's Ai Research group for machine learning neural network research, but the technology is flexible enough to be used in a variety of different fields! When using TensorFlow to develop and training a machine learning technique, one frequently winds up with a model file that necessitates the use of a GPU for inference.

When using TensorFlow to develop and train a machine learning technique, one frequently winds up with a model file that necessitates the use of a GPU for inference. Most smart phones lack sufficient storage space and GPUs. TensorFlow Lite is a machine - learning execution option for

mobile devices.

TensorFlow Lite is a one-of-a-kind feature designed particularly for embedded devices such as mobile phones. A specialized memory allocator is employed for short execution delay and low load. It also covers the unique file format that Flat Buffers supports. TensorFlow Lite optimizes old systems inside the structure of a .tflite file.

4.7 Architecture of TensorFlow Lite: -

TensorFlow Mobile is TensorFlow Lite's successor, and it is usable on mobile platforms such as Android and iOS (Operating System). It's used to construct a TensorFlow model before integrating it into a mobile environment

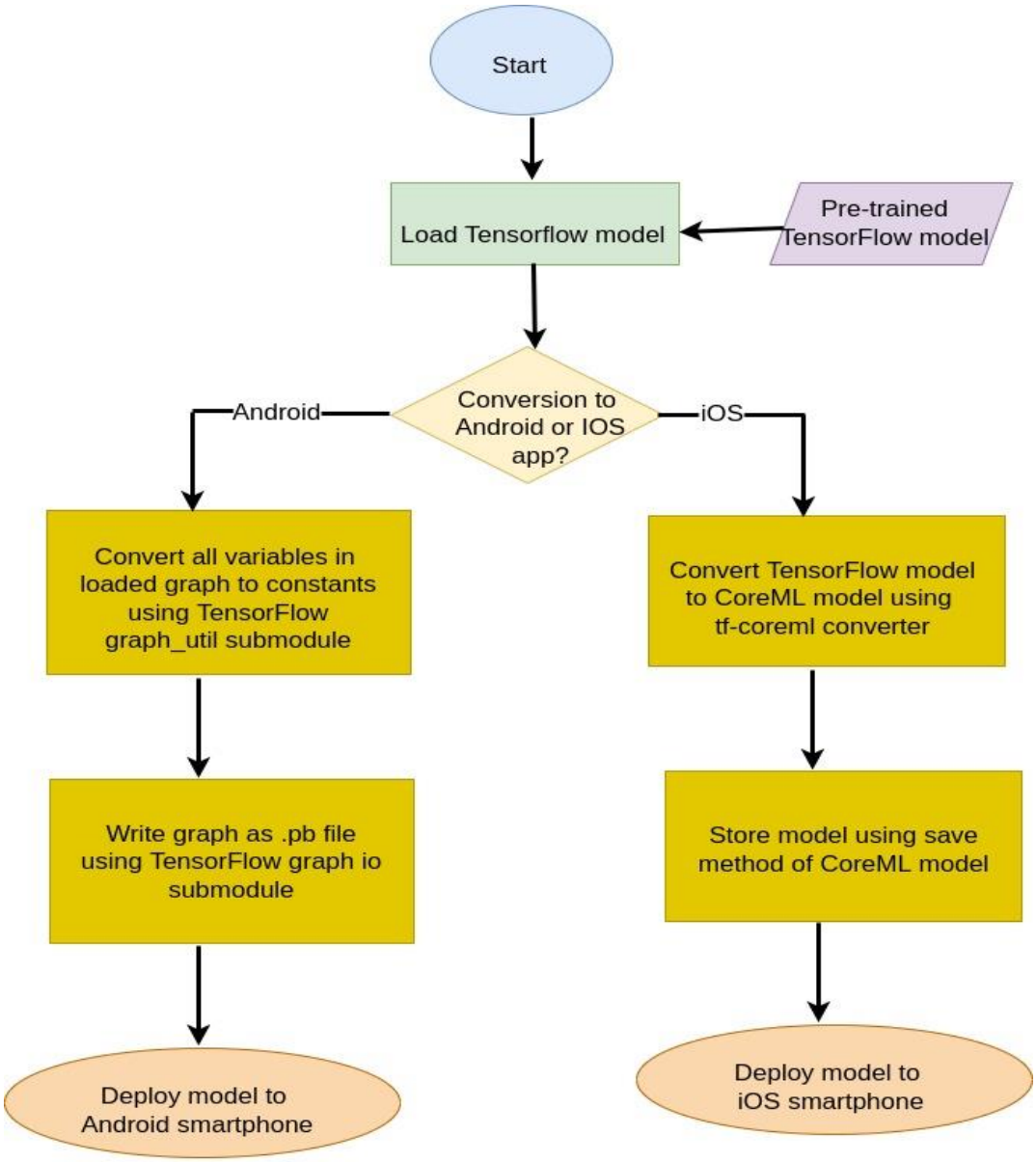

Figure 12 TensorFlow Lite Architecture

4.8 Train ML Model to .tflite file conversion:-

```
Import tensorflow as tf
# Model conversion
Converter =tf.lite.TFLiteConverter.from_saved_model(trained_model_dir)
(saved_model_dir-Trained Model Address)
tflite_model_result=converter.convert()
#Keep the model.
With open('model.tflite', 'wb') as f:
f.write(tflite_model_result)
```

4.9 Test Model in Android Studio: -

```
Model newmodel = Model.newinstance(getApplicationContext());
//Creates reference inputs
TensorBuffer intputfeature= TensorBuffer.createFixedSize(new int[]{1, 132, 132, 3},
DataType.UNIT8);
//Model inference is performed and the result is returned.
Model.Outputs getresult = model.process(inputfeature);
TensorBuffer outputfeature= getresult.getOutputFeature0AsTensorBuffer();
// If a model resource is no longer in use, it is released.
Model.close()
```

4.10 Advantage of TensorFlow Lite: -

- Convert TensorFlow models to TensorFlow lite models quickly and efficiently for mobile-friendly models.
- With simplicity, creates machine learning apps for iOS and Android devices.
- A more effective option to mobile model enablement than server-based architectures.
- Tensorflow Lite enables machine learning models to be performed directly on a smartphone, allowing users to do common machine learning tasks without the need for an external API or server. As a consequence, the models will work on devices that do not have internet access.

4.11 TensorFlow Lite's Drawbacks:-

- In the TensorFlow Lite procedure, the cost of reliability and optimization is a trade-off with model accuracy. As a result, TensorFlow Lite models are less accurate than their full-featured equivalents.

- It's doesn't improve the model's size. As a result, mobile devices may need extra storage space.

4.12 TensorFlow Mobile Use Cases-

The three most important use cases for TensorFLow Mobile are as follows:

- **TensorFlow Gesture Recognition:** By analyzing sensor data, it may run apps or do any unique task supported by the hands or other gestures.
- **TensorFlow Picture Recognition:** It is used to recognize or extract information from an image captured using a mobile device. If users take images to interpret information or to apply effects (filters) to the photos, Images Recognition plays a critical role in accurately recognizing the photos. Camera, Image Editor, and so on.
- **TensorFlow Speech Recognition:** Using Tensorflow, various speech-related applications can be built using a speech-driven interface. Speech Recognition is used to correctly recognize the voice. Google Translate, Google Assistant, and other prominent applications that use the Speech Recognition System are listed here.

4.13 Requirement Analysis: -

- **Hardware Requirements**
  1. Processor: Dual core or above
  2. RAM: 4 GB or above
  3. Hard Disk: 320 GB or more
  4. Monitor: Color (for best result)
  5. Keyboard: 108 Key normal
  6. Mouse: 3 Button normal mouse
- **Software Requirements**
  1. Operating System: Windows10,11
  2. Knowledge of M.L
  3. Android Studio

❖ Sequence Diagram

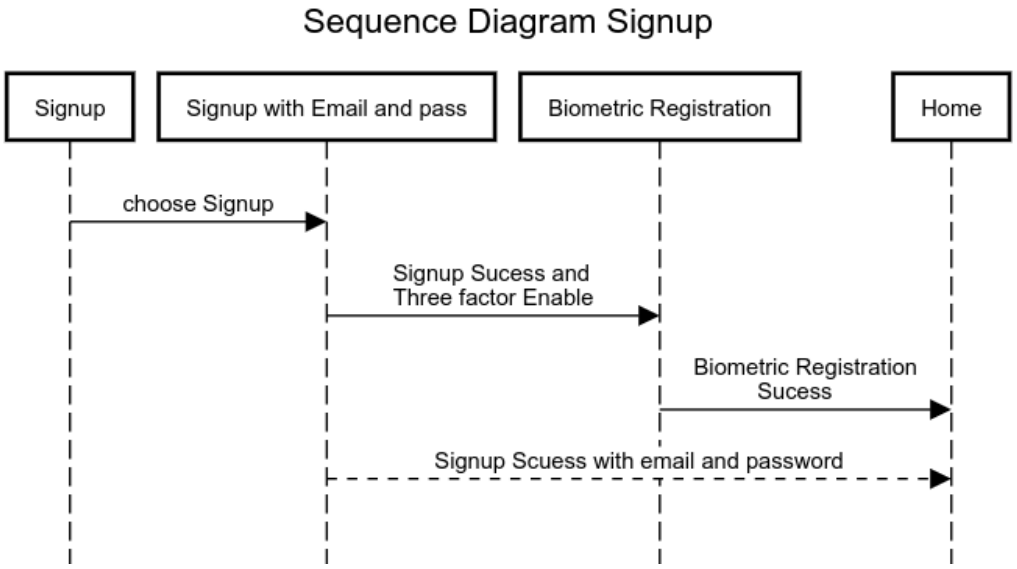

Figure 13 Signup Sequence Diagram

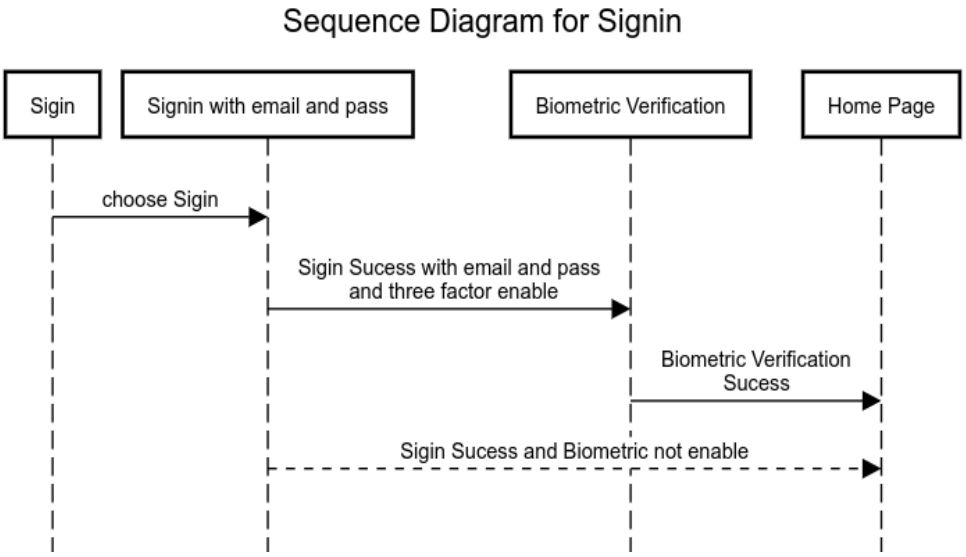

Figure 14 Sign in Sequence Diagram

❖ USE CASE Diagram

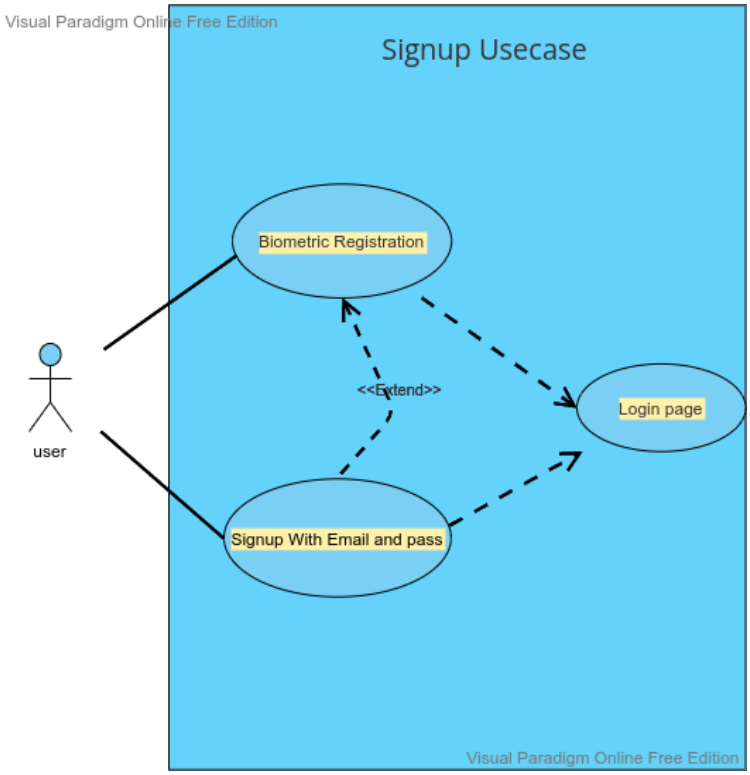

Figure 15 Signup Use case Diagram

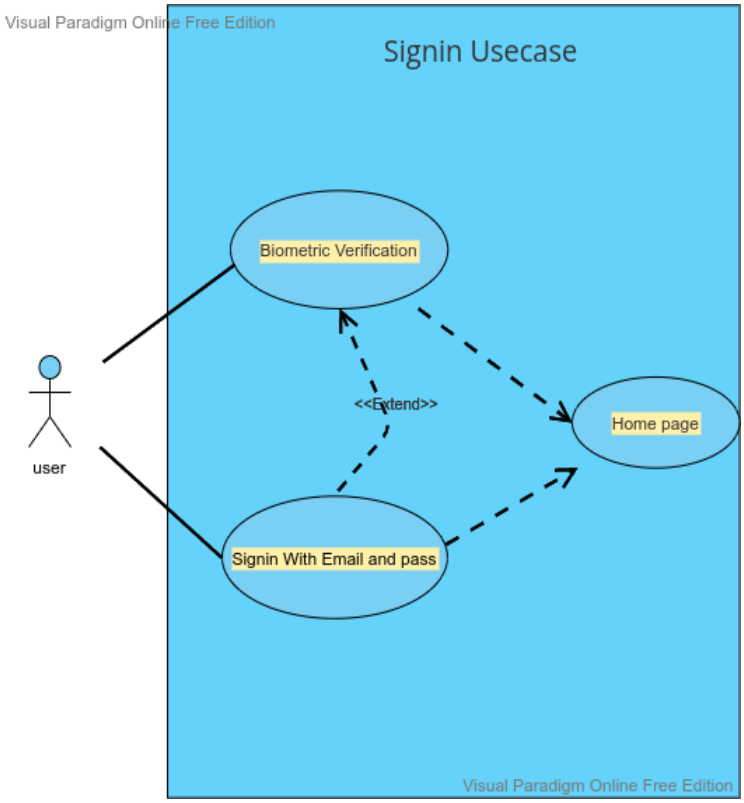

Figure 16 Signin Use case Diagram

❖ **Flow Chart: -**

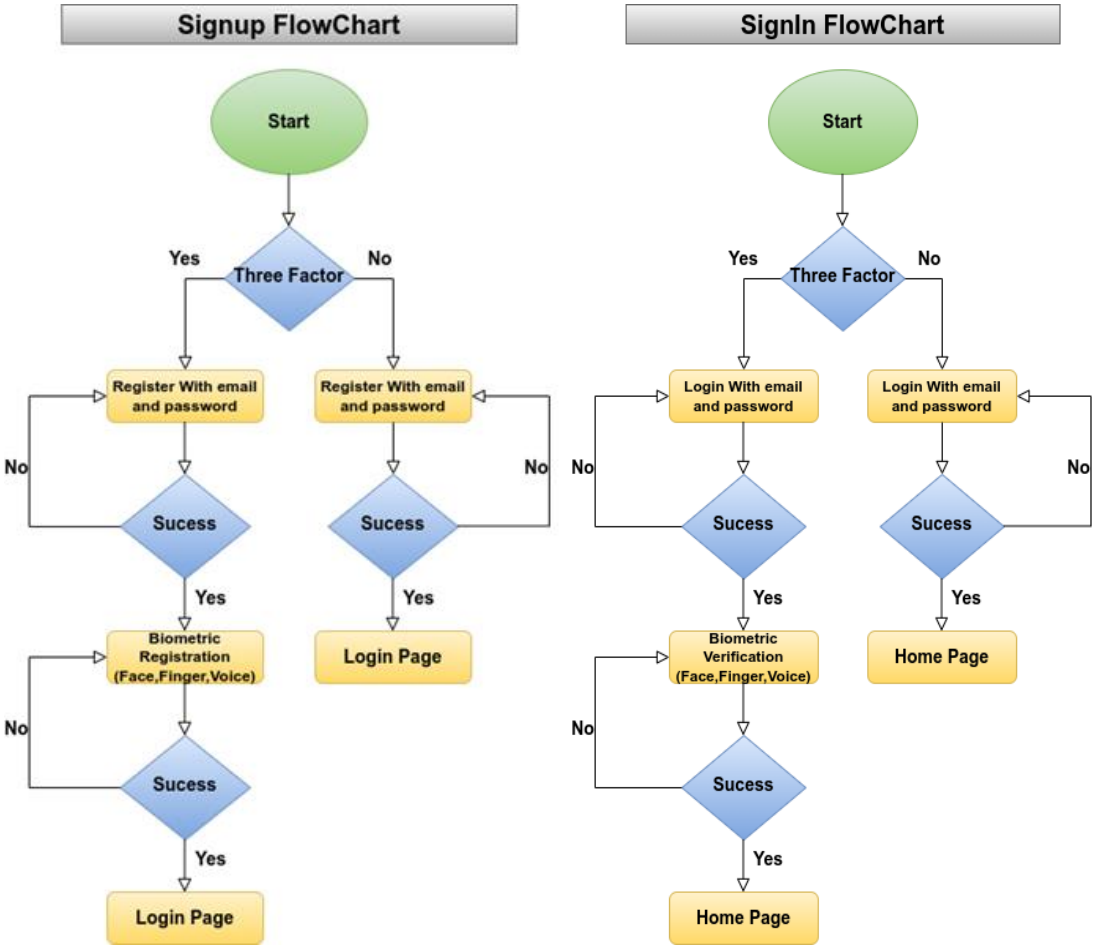

Figure 17 Flow Chart for Sign in and Signup

CHAPTER-5

RESULT AND ANALYSIS

Overall, our system performed admirably, as seen by our 98.2 percent success rate. One of the main reasons for our high success rate was that our photos were both pre-normalized and pre-cantered. trying to create an effective cantering algorithm in the past has generally proven to be the demise of many groups; there just isn't any method out there right now that dependably finds the centre point of an image. As a result, the fact that this step had already been completed for us simplified our duty.

We have taken sufficient test set photos and a training set photo in database. Our programme correctly verified that each user was who he or she claimed to be. We put our algorithm through rigorous testing, and it passed all of them

5.1 Result of Biometric Verification: -

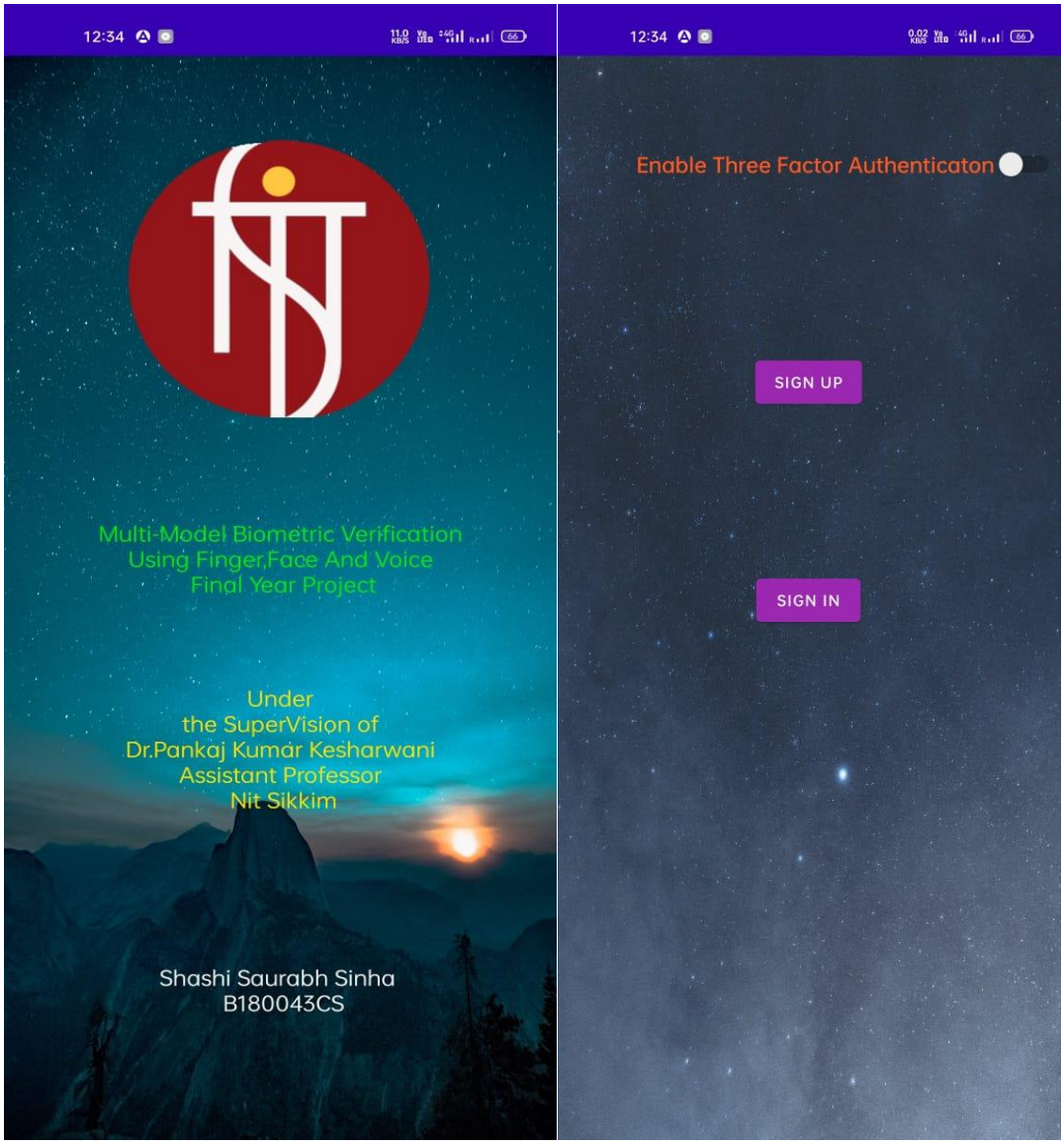

Figure 18 Splash Screen and Signup/Signin without Biometric enable

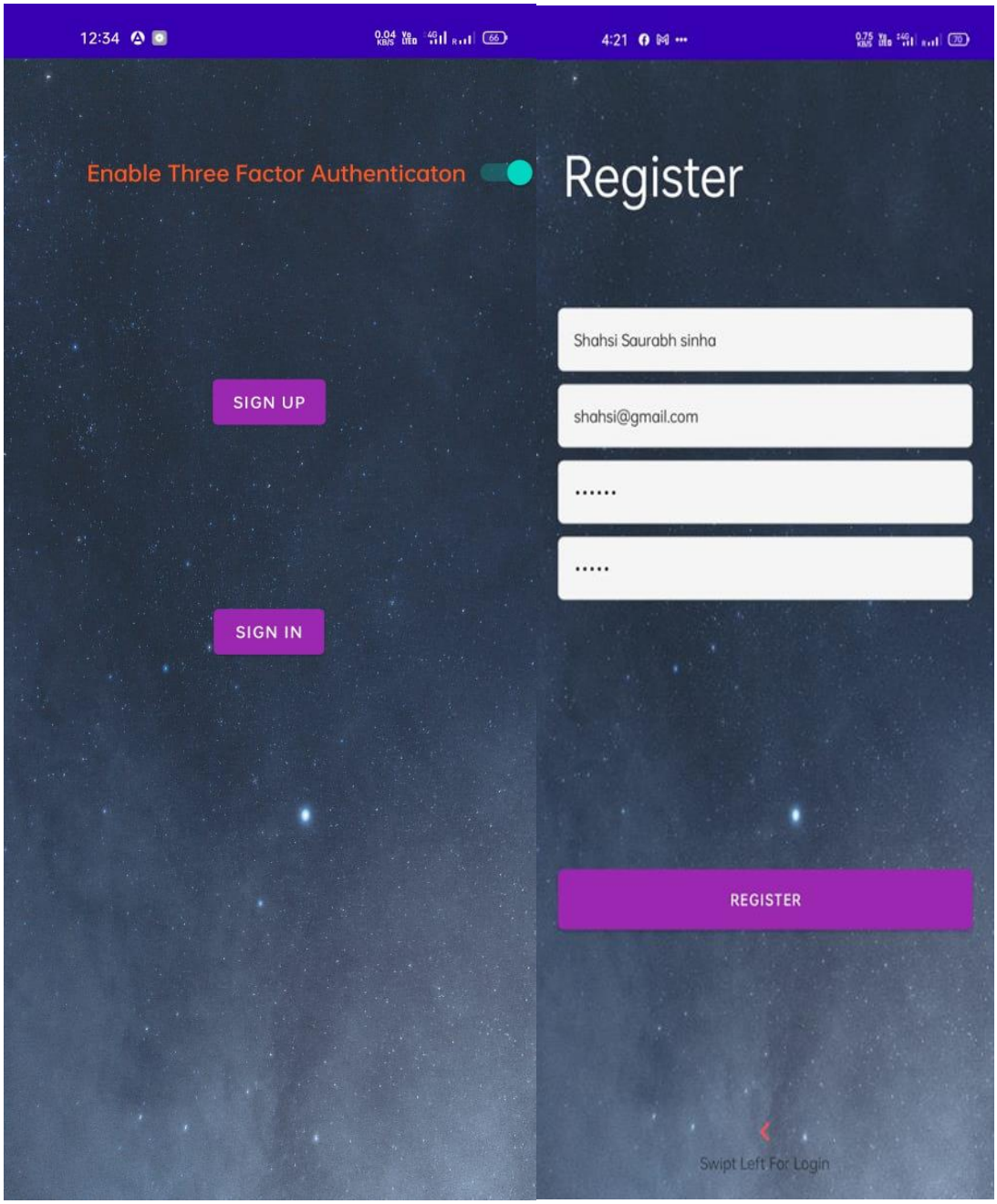

Figure 19 Signup/Sign in With Biometric Enable and Registration page

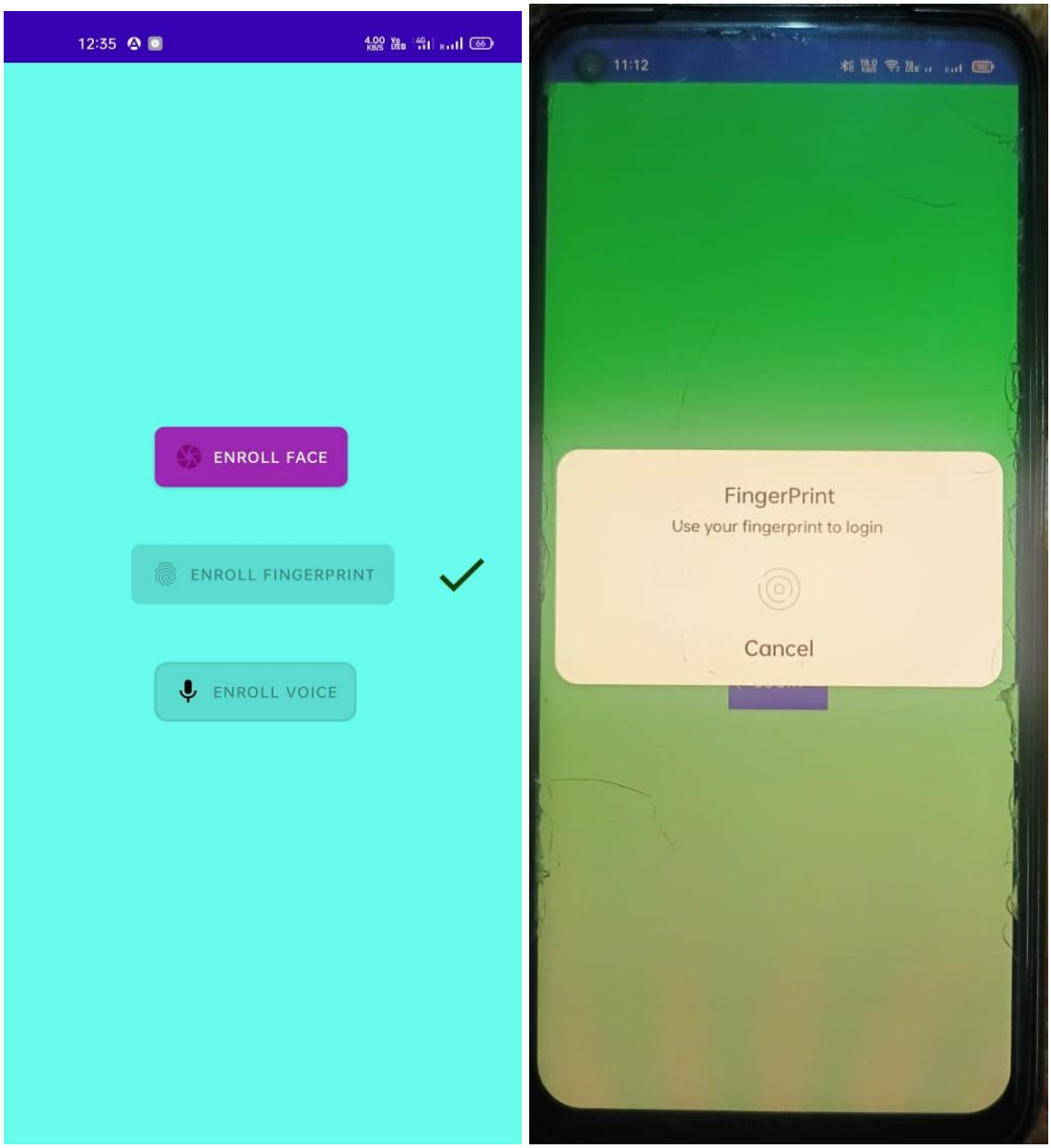

Figure 20 Fingerprint Enroll

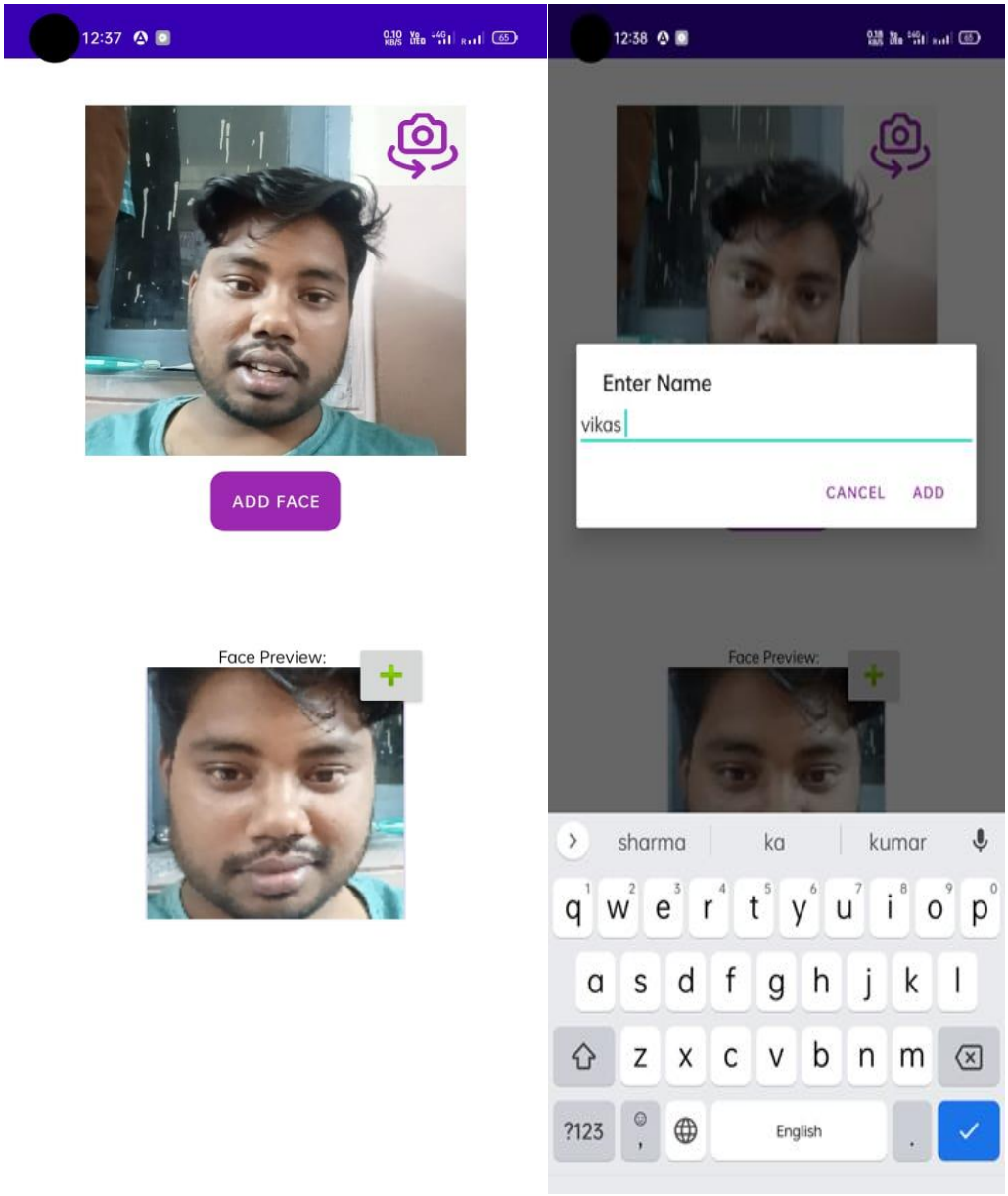

Figure 21 Face enroll and level

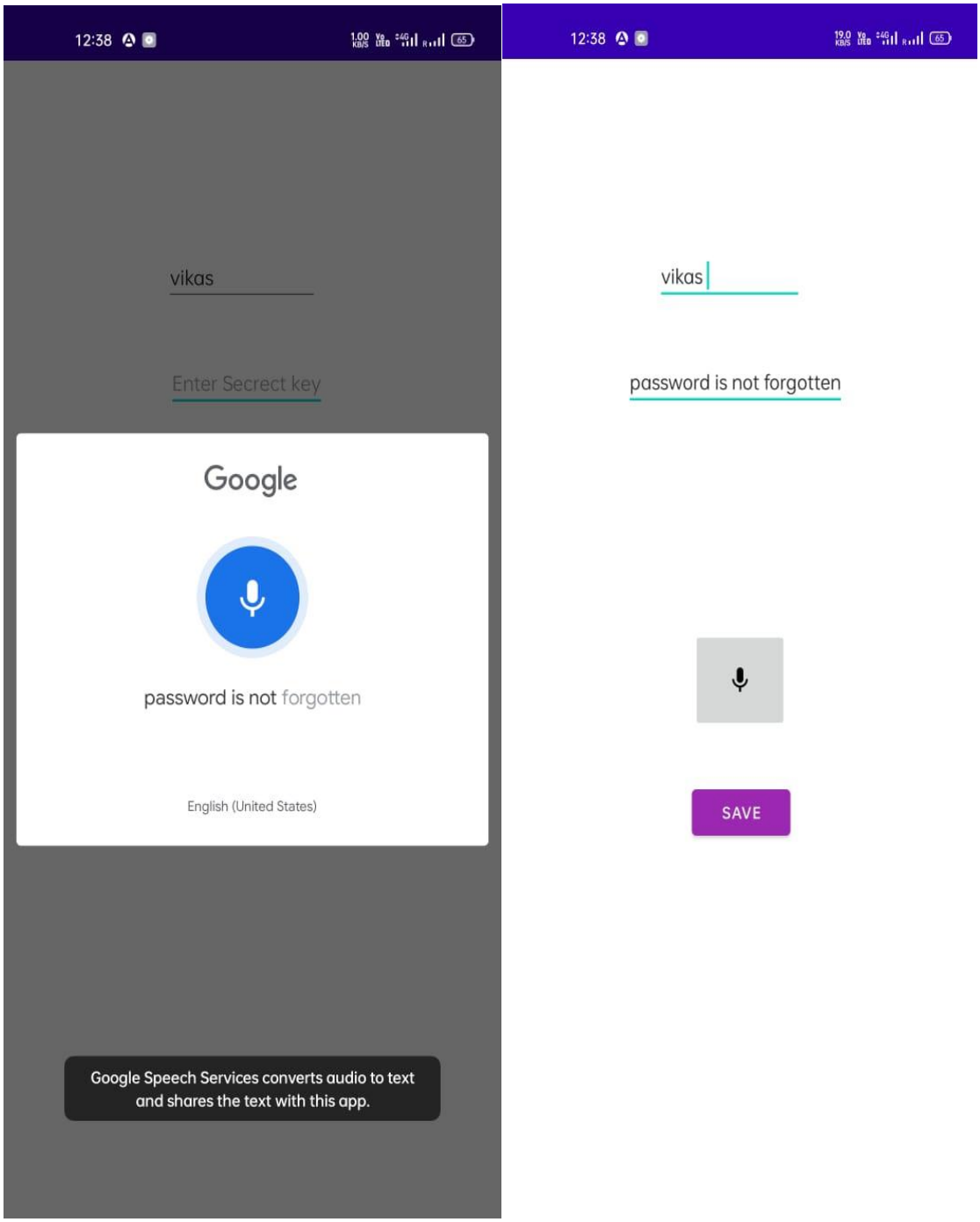

Figure 22 Voice enroll and Level

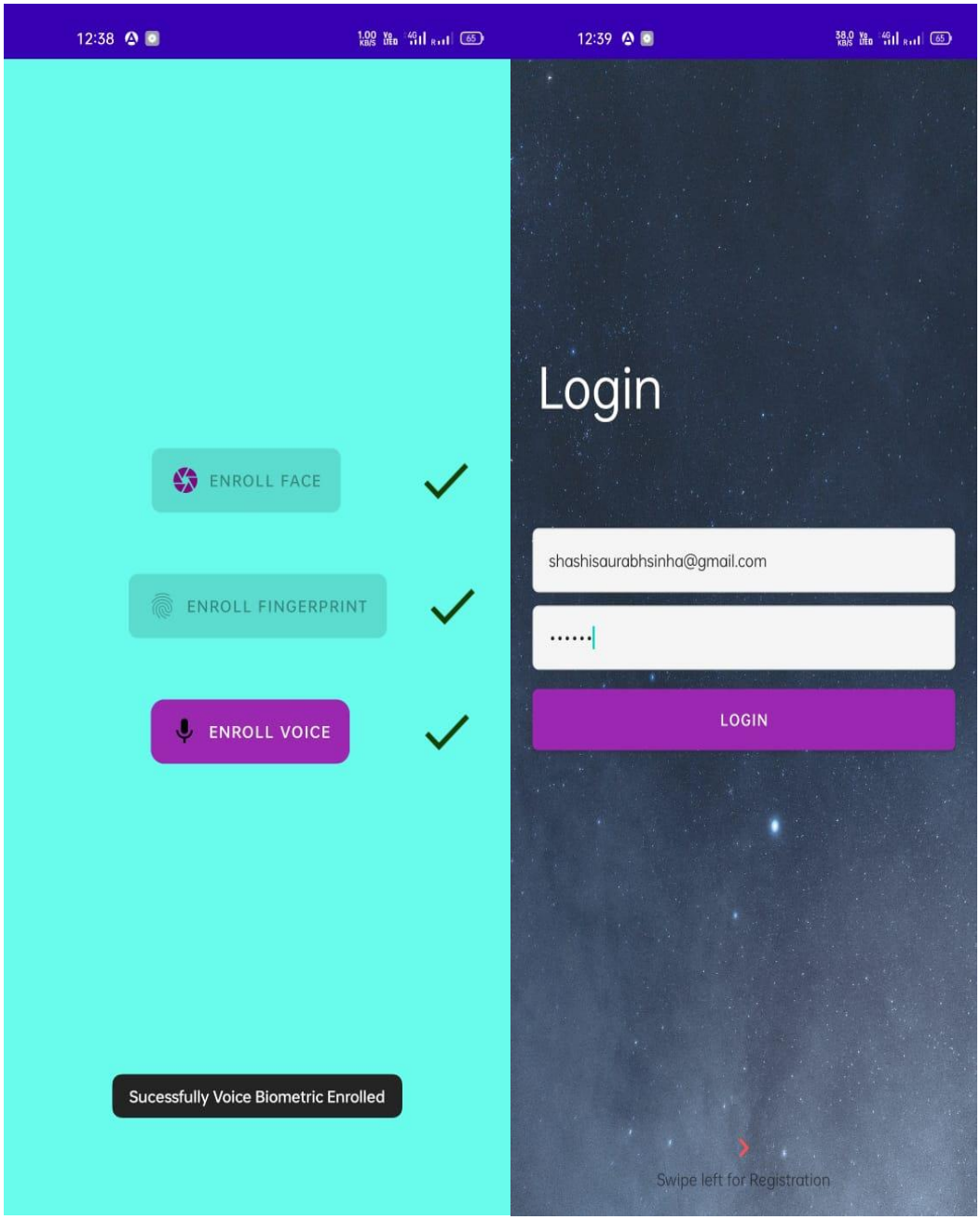

Figure 23 Three Factor Biometric Enrolment Success and Login Page

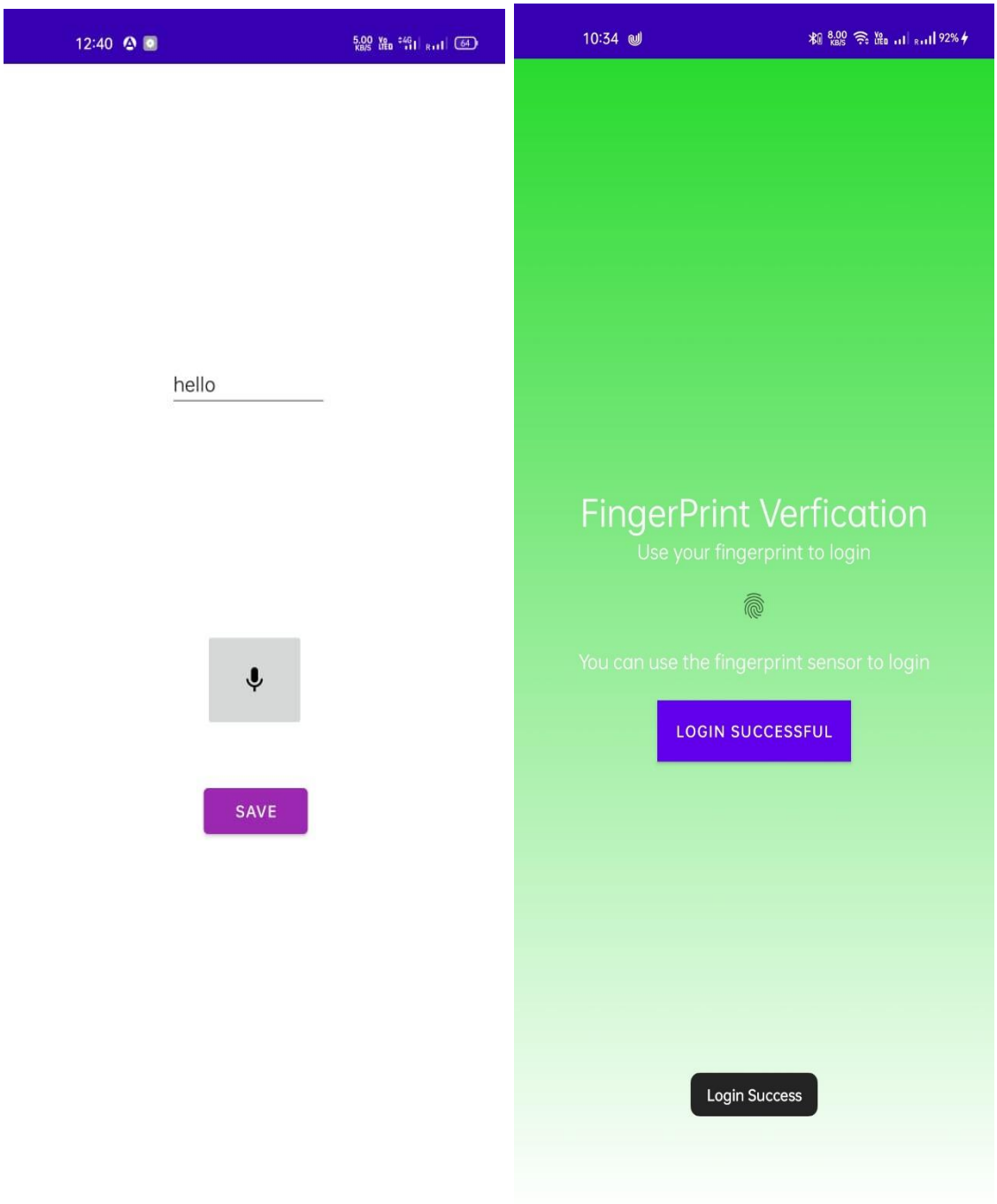

Figure 24 Voice Verification and Fingerprint Verification

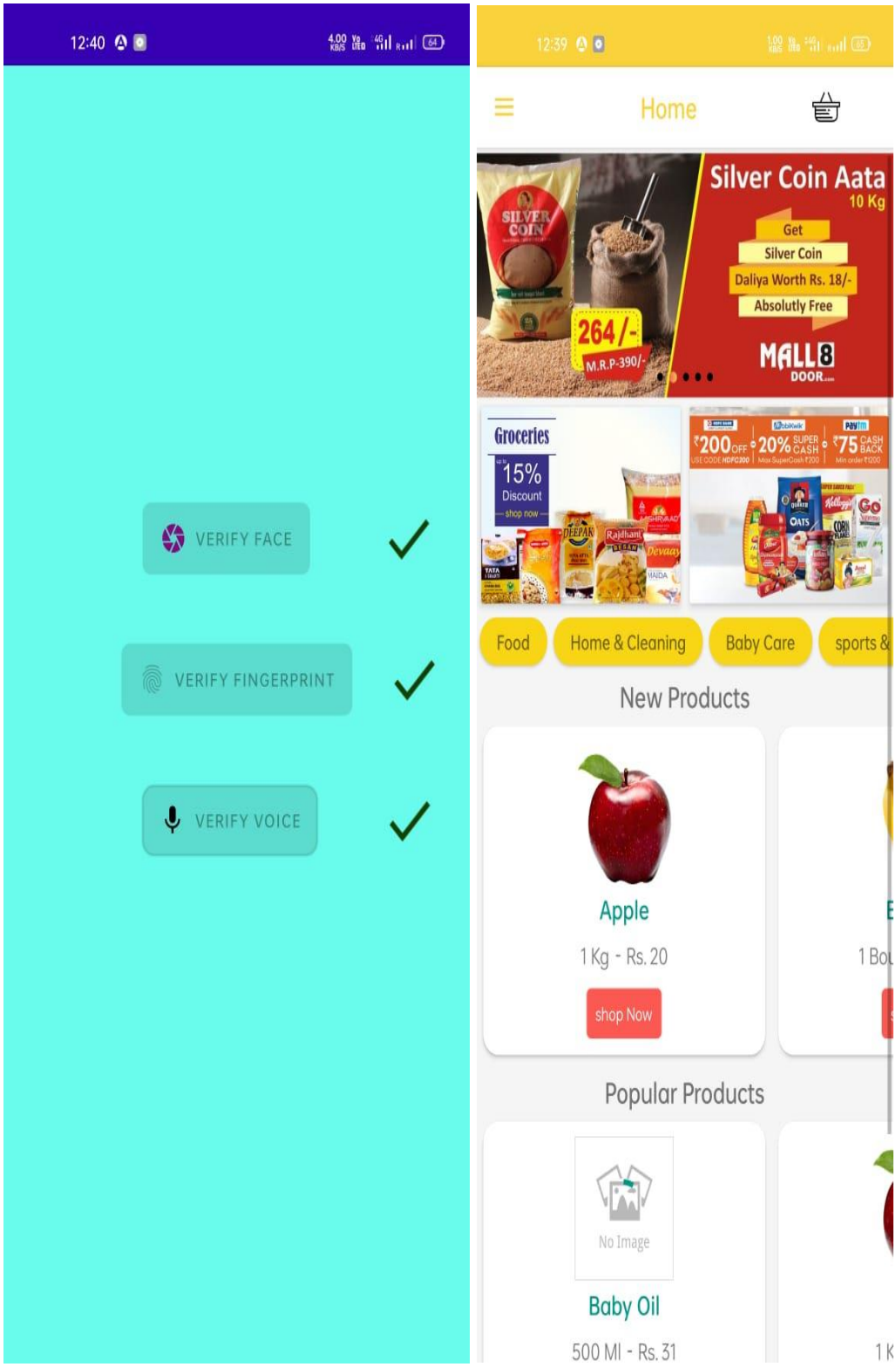

Figure 25 Three Factor Biometric Verified and Home page

5.2 Database: -In this project used two databases.

1. **Firebase: -**It Developed by google and it a type of No-SQL database which store data in form of document and collection. I used this for authentication when user login by email and password or register with email and password.

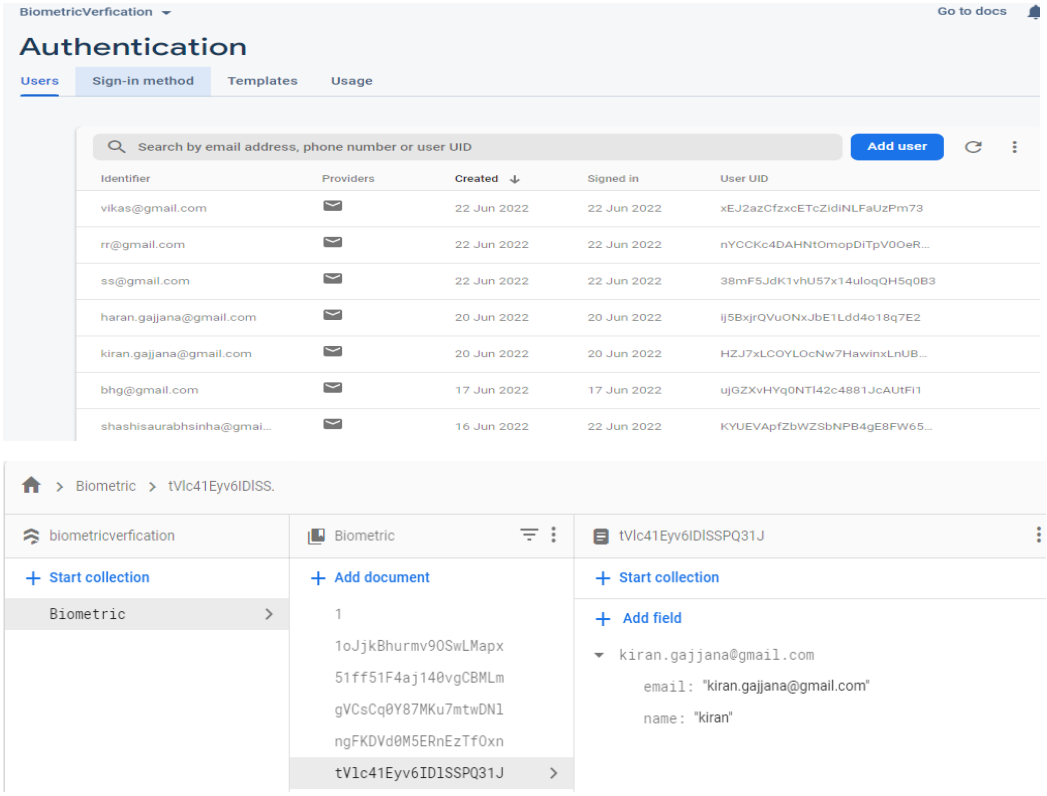

Figure 26 Firebase User Authentication data

2. **Shared Preferences: -**It is a type of xml file. Which store the value in the form of key and value. It is used for store the small data. We use shared preferences in this project for store data of user and retrieve data of face and voice.

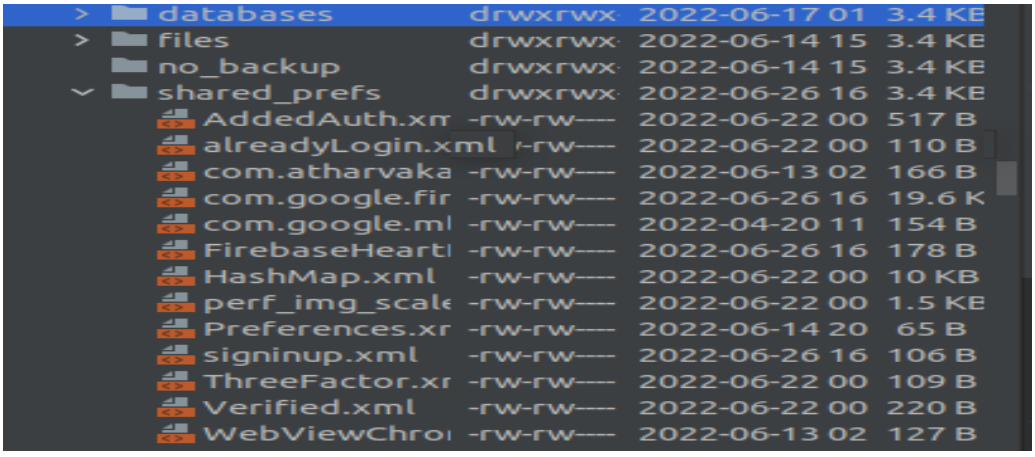

Figure 27 Local Storage

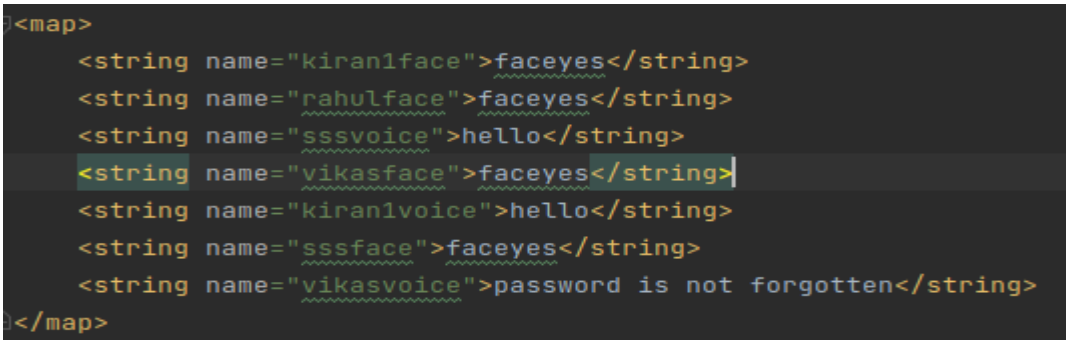

Figure 28 Register User Data

5.3 Analysis

5.3.1 Advantage of Biometric Verification: -

1. **Less Processing time-** Biometrics verified systems are typically referred to as one-to-one processes and require shorter processing time than other identifying systems. This is due to the fact that in other recognizing systems, the information is compared to all previously stored data in the database.
2. **Increased Security-** When compared to traditional authentication techniques, biometric technology has delivered a higher level of security. It is chosen over traditional procedures for a variety of reasons, including the requirement for the authorized person's physical presence at the point of identification, which means that only the authorized person has access to specified resources.
3. **Ease of work-**You no longer have to type the passwords over and over. Or even the necessity to remember complex passwords. Unlike a phone or office punching machine, your electronic gadgets can be opened or updated with just a fingerprint. The tools are now retina and voice sensitive.
4. **Accuracy-** Biometrics validated systems are also more accurate because they simply need to compare an individual's data against his or her stored data in the database rather than hundreds, thousands, or even millions of comparisons as identifying systems require.
5. **Screening-**Most tourists travelling on visas will have two fingerprints scanned by an inkless device and a digital image taken as part of the upgraded procedures. All of the information and data is then used to help the border inspector decide whether or not to accept the traveler. These upgraded procedures will add merely seconds to the overall processing time of the visitor. The computerized fingerprint scanner will allow inspectors to cross-reference visitors' IDs with those on terrorism watch lists.

5.3.2 Biometric Verification Has a Drawback: -

Biometrics, like all other security solutions, has limits and risks that might impair its efficacy and efficiency, which are as follows:

- Intra-class variability and inter-class likeness
- Classification
- Noisy input & population coverage
- System performance (error rate, speed, cost)
- Individuality of biometric characteristics
- Fusion of several biometric variables
- Scalability
- Biometric - based attacks Concerns About Privacy

5.3.3 Biometric Applications: -

Biometric applications are classified into horizontal and vertical markets. The following horizontal categories make extensive use of biometrics:

a) **Identification of a citizen:** Citizens who work for government agencies must be identified and verified.
b) **Network Access:** Safeguard access to computers, networks, and other computer services.
c) **Time and Travel/Physical Access:** Avoid future access to a specific area.
d) **Monitoring and evaluation:** Identify and confirm the existence of specific individuals in a given area.
e) **For Sale / Sales Area/ATM:** Personal identification and verification of products and services
f) **E-Commerce / Telephone:** Provide remote identification / verification of goods / services
g) **Crime Detection:** Identify / verify certain people in legal applications.
h) **Public Sector:**
   → Transport and Travel
   → Financial Industry
   → Medical Care
   → Voting

Among the technologies is fingerprint scanning, which is dominated by a non-competitive leader with a market share of far more than 50%.

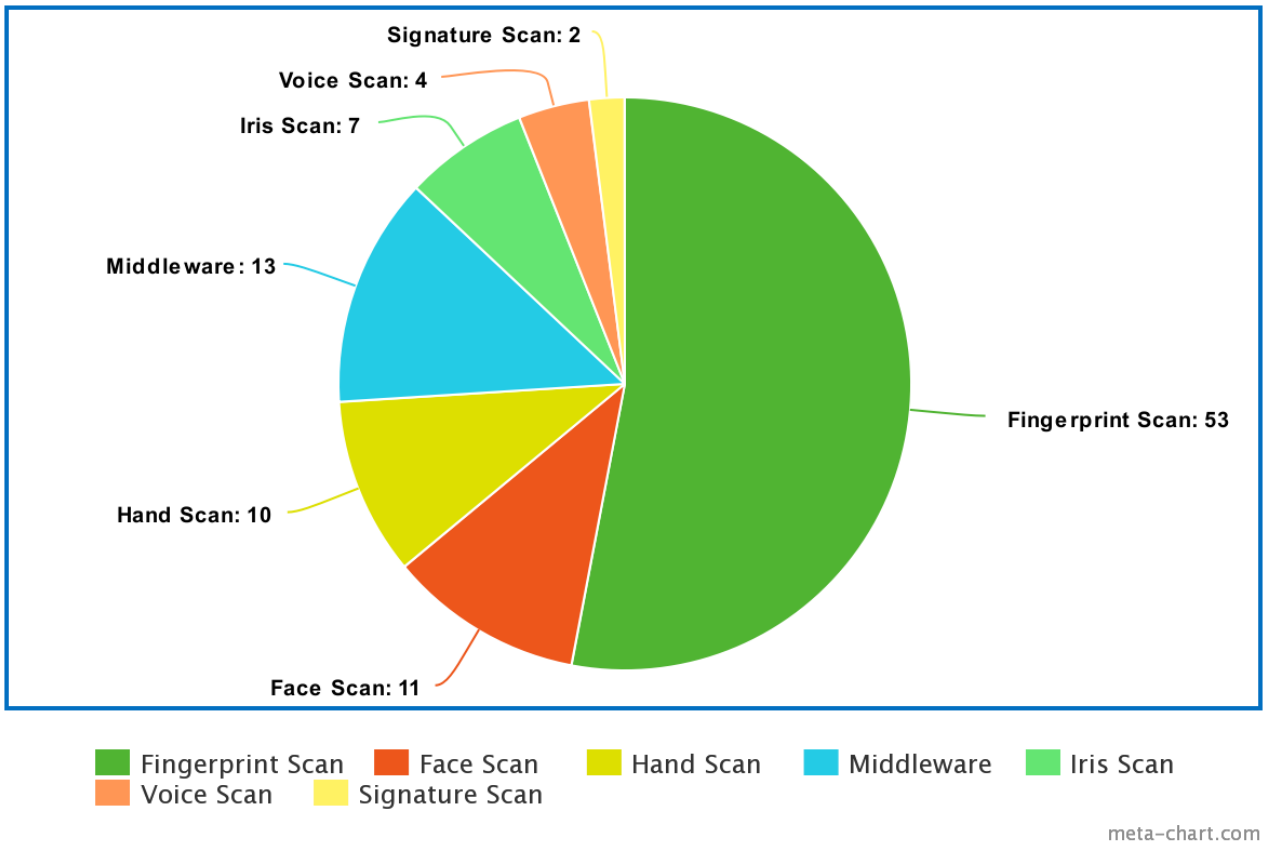

Figure 29 Biometric Uses in Real life

CHAPTER -6
CONCLUSION AND FUTURE WORK

6.1 Conclusion: -

Even if the accuracy of biometric approaches is limited, there are already several mature biometric systems available. The proper integration of a biometric system, particularly smartcard-based solutions, can improve overall security. Creating secure biometric systems, on the other hand, is not as simple as it may appear. The term biometrics is frequently used to mean full safety. This is a deceptive viewpoint. When creating a safe biometric system, there are numerous aspects to consider. First and foremost, biometrics are not a well-guarded secret. This means that biometric measures cannot be used as power tokens and that generating cryptographic keys from them is not secure. Second, you must have faith in the installation device and safeguard the communication link. Third, the input device must be doing check for the estimated human life and validated, for example, using a demanding response protocol.

6.2 Future Work: -

Given that the most significant shortcoming in the existing implementation of this project is the lack of speed, that would be the top priority of any changes. Even if only the paging to memory functioned, it would result in a 10x improvement in the Gabor section, reducing the runtime of a single experiment from six minutes to less than one minute. Following that, we would attempt DMA transfers from the board to the on-chip memory, employing a threaded method to ensure that data was continually being processed and relocated.

The following are the upcoming works:

1. Improve the most recent way for providing a high level of security.
2. Make biometric verification more secure so that it cannot be easily faked.
3. Introduce another form of biometric verification that can aid in its detection. If one of the methods fails, such as the heart-bit, DNA verification can be used to validate.
4. The use of biometric systems in different areas of our society, businesses, and organizations has restored individual privacy while also preventing security concerns. Face Recognition and Voice Detection are two significant new technologies that provide authentication to every user while also protecting their authorization. Securing authorization here refers to preventing duplicate identities and voices, because each human has his or her own distinct identity, even

if the system is presented with two identical twins.

5. Biometrics System- Face Recognition is on the verge of becoming more advanced. Security limitations are required for almost any software. We intend to replace traditional security constraint approaches with Biometrics Systems—Face Recognition, Voice Identification, or both.
6. The future potential of our software CONNOISSEUR-the Expert Judge is vast. It can also be embedded into practically every piece of software that we use on a daily basis. For instance, in an attendance management system, an employee management system, or a library management system.
7. With the addition of sensor connectivity, our program CONNOISSEUR-the Expert Judge may be further developed to automatic detection. The security code can also be substituted by a voice recognition system.

6.3 Reference

1. Prasad Pawar 1 , Shreyas Datar 2 , Nilay Ranade 3 , Kunal Thorat 4 , Prof.A.N.Gharu 5(2019),Biometric Security Using Cryptography for Insurance
2. International Journal of Recent Technology and Engineering (IJRTE), Mohammed, Bayan Omar. "Mean-Discrete Algorithm for Individuality Representation." *Journal of Al-Qadisiyah for computer science and mathematics* 13, no. 1 (2021).
3. Al-Nima, R.R.O., Abdullah, M.A., Al-Kaltakchi, M.T., Dlay, S.S., Woo, W.L. and Chambers, J.A., 2017. Finger texture biometric verification exploiting multi-scale sobel angles local binary pattern features and score-based fusion. Digital Signal Processing, 70, pp.178-189.
4. de Freitas Pereira, T. and Marcel, S., 2021. Fairness in biometrics: a figure of merit to assess biometric verification systems. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(1), pp.19-29.
5. Sawhney, S., Kacker, K., Jain, S., Singh, S.N. and Garg, R., 2019, January. Real-time smart attendance system using face recognition techniques. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 522-525). IEEE.
6. Kaur, N., 2021, March. A study of biometric identification and verification system. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 60-64). IEEE.
7. Ibrahim, S., Egila, M.G., Shawky, H., Elsaid, M.K., El-Shafai, W., El-Samie, A. and Fathi, E., 2020. Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. Multimedia Tools and Applications, 79(19), pp.14053-14078.
8. Kaur, N., 2021, March. A study of biometric identification and verification system. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 60-64). IEEE.
9. Połap, D. and Woźniak, M., 2018. Voice recognition by neuro-heuristic method. Tsinghua Science and Technology, 24(1), pp.9-17.
10. Herbadji, A., Guermat, N., Ziet, L. and Cheniti, M., 2019, November. Multimodal Biometric Verification using the Iris and Major Finger Knuckles. In 2019 International Conference on Advanced Electrical Engineering (ICAEE) (pp. 1-5). IEEE.
11. Alarifi, A., Amoon, M., Aly, M.H. and El-Shafai, W., 2020. Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system. IEEE Access, 8, pp.221246-221268.

12. Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G. and Yearwood, J., 2016. Protection of privacy in biometric data. IEEE access, 4, pp.880-892.
13. M. Arsenovic, S. Sladojevic, A. Anderla, and D. Stefanovic, “FaceTime - Deep learning based
14. face recognition attendance system,” SISY 2017 - IEEE 15th Int. Symp. Intell. Syst. Informatics,Proc., pp. 53–57, 2017