



MULT-PATTERN FINGERPRINT SECURITY SYSTEM

A PROJECT REPORT

Submitted by

NITHYANANTHAM R

113021205036

ARVINDHAN G

113021205008

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

VEL TECH HIGH TECH

Dr. RANGARAJAN Dr. SAKUNTHALA ENGINEERING COLLEGE
An Autonomous Institution

JULY 2023

VEL TECH HIGH TECH

DR.RANGARAJAN DR.SAKUNTHALA ENGINEERING COLLEGE
An Autonomous Institution



BONAFIDE CERTIFICATE

Certified that this mini project entitled “**MULTI-PATTERN FINGERPRINT SECURITY SYSTEM**” is the bonafide work of “**NITHYANANTHAM.R (113021205036) & ARVINDHAN.G (113021205008)**” who carried out this work under my supervision.

SIGNATURE

Dr M.Malleswari M.E, Ph.D.

HEAD OF THE DEPARTMENT

PROFESSOR

Information technology

Vel Tech High Tech

Dr.Rangarajan Dr.Sakunthala

Engineering College

SIGNATURE

Ms S.Mangalapriya, M.E

SUPERVISOR

ASSISTANT PROFESSOR

Information technology

Vel Tech High Tech

Dr.Rangarajan Dr.Sakunthala

Engineering College

CERTIFICATE OF EVALUATION

College Name : VEL TECH HIGH TECH DR.RANGARAJAN
DR.SAKUNTHALA ENGINEERING COLLEGE

Degree : BACHELOR OF TECHNOLOGY

Branch : INFORMATION TECHNOLOGY

Semester : IV

S.No	Name of the Student(s)	Title of the Project	Name, Designation & Department of the Supervisor and Co-Supervisor
01	NITHYANANTHAM R	MULTI-PATTERN FINGERPRINT SECURITY SYSTEM	Ms MANGALAPRIYA.S, M.E ASSISTANT PROFESSOR Department of Information Technology
02	ARVINDHAN G		

The report of the project work submitted by the above students in partial fulfillment for the award of degree, Bachelor of Technology/Engineering in INFORMATION TECHNOLOGY for the viva voce examination held at Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College on _____ has been evaluated and confirmed to be reports of the work done by the above students

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGMENT

We would like to express our obeisance to the following persons for their invaluable help rendered.

We wish to express our sincere thanks and gratitude to our chairman Col Prof. **Dr. R. RANGARAJAN B.E. (Elec.), B.E. (Mech.), M.S(Auto.), DSC.** and vice-chairman **Dr. SAKUNTHALA RANGARAJAN M.B.B.S.**, for providing us with a comfort zone for doing this project work. We express our thanks to our principal, Professor **Dr. E. KAMALANABAN B.E., M.E., Ph.D.**, for offering us all the facilities to do the project.

We also express our sincere thanks to the professor, **Dr.M.MALLESWARI M.E, Ph.D., Head of the Department**, of department Information Technology for supporting this project work.

We also express our sincere thanks to **Mrs. M. RAMYA, M.E, Assistant Professor, Project Co-Ordinator**, Department of Information Technology for his continuous and valuable suggestions which helped us to proceed with this project work.

Our special thanks to our Project supervisor **Ms. S. MANGALAPRIYA, M.E. Assistant Professor**, Department of Information Technology, who provided us with full support at every stage of the project.

We thank our parents, friends, and supporting staff of the Information Technology Department for the help they extended for the completion of this project.

ABSTRACT

This paper proposes a multi-pattern fingerprint security system to enhance security measures. The proposed system integrates an Arduino Uno board, a fingerprint sensor, and a database to provide advanced security features. The system's design allows for multiple fingerprint patterns to be stored in the database, thereby increasing the system's flexibility and versatility.

The proposed system's architecture is based on a client-server model, with the Arduino Uno board acting as the client and the database acting as the server. The fingerprint sensor captures the user's fingerprints and sends the data to the Arduino Uno board for processing. The Arduino Uno board then sends the fingerprint data to the database for storage and authentication. The system also includes a graphical user interface (GUI) that allows users to register and manage their fingerprints.

The proposed system's main advantage is its ability to store multiple fingerprint patterns, allowing for more secure authentication. The system's design is also cost-effective and can be easily integrated into existing security systems.

In conclusion, the proposed multi-pattern fingerprint security system is an innovative solution that enhances security measures. The system's design, which includes an Arduino Uno board, a fingerprint sensor, and a database, provides advanced security features that can be easily managed through a graphical user interface. This system can be used in various applications that require advanced security measures, including banking, healthcare, and government institutions.

Keywords: Fingerprint, Arduino, SQL, Multi-pattern, Security system.

TABLE OF CONTENTS

CHAPTERS	CHAPTER NAME	PAGE NO
	ABSTRACT	v
	LIST OF FIGURES	viii
	LIST OF ABBREVIATIONS	ix
1	INTRODUCTION	
	1.1 Overview	1
	1.2 Statement of the problem	1
	1.2.1 Why the problem statement is of interest	1
	1.2.2 Objective of the Study	2
	1.2.3 Research questions	2
2	LITERATURE REVIEW	
	2.1 Finger-Knuckle-Print Recognition Using Deep Convolutional Neural Network	4
	2.2 Finger vein recognition based on Deep Convolutional Neural Networks.	6
	2.3 Biometric Authentication Using Palm Dorsal Vein Patterns.	7
	2.4 A Novel Algorithm for Secure Internet Banking with Fingerprint Recognition	8
	2.5 The Research of Double-biometric Identification Technology Based on Finger Geometry & Palm Print.	10

3	SYSTEM ANALYSIS	
3.1	Existing system	12
3.1.1	Disadvantages	12
3.2	Proposed system	12
3.2.1	Advantages	13
4	REQUIREMENT ANALYSIS	
4.1	SOFTWARE REQUIREMENTS	
4.1.1	Arduino IDE	14
4.1.2	Microsoft SQL server management studio	15
4.1.3	Windows form application (VS)	15
4.2	HARDWARE REQUIREMENTS	
4.2.1	Arduino UNO R3	16
4.2.2	Fingerprint scanner	17
5	METHODOLOGY	
5.1	Login form	18
5.2	Registration catalog	18
5.3	Fingerprint scan form	19
5.4	Fingerprint checking form	19
6	SYSTEM DESIGN	
6.1	Architectural design	21
6.2	UML diagram	
6.2.1	Use case diagram	22
6.3	Storing and receiving	23
6.4	Login form	24
6.5	Registration Form	25

6.6	Fingerprint scan	26
6.7	Fingerprint check	27
6.8	Databases	
6.8.1	Login page database	28
6.8.2	Registration page database	28
6.8.3	Fingerprint database	28
6.9	Workflow diagram	29
6.10	Fingerprint sensor pin diagram	30
6.11	Arduino to sensor connectivity	31
7	RESULT AND DISCUSSION	
7.1	Future works	32
8	CONCLUSION	33
9	REFERENCES	34

LIST OF FIGURES

FIG NO	TITLE	PAGE NO
6.1.1	ARCHITECTURAL DESIGN	21
6.2.1.1	USE CASE DIAGRAM	22
6.3.1	STORING AND RECEIVING	23
6.4.1	LOGIN FORM	24
6.5.1	REGISTRATION FORM	25
6.6.1	FINGER SCAN	26
6.7.1	FINGER CHECK	27
6.8.1.1	LOGIN PAGE DATABASE	28
6.8.2.1	REGISTRATION PAGE DATABASE	28
6.8.3.1	FINGERPRINT DATABASE	28
6.9.1	WORKING PROCEDURE	29
6.10.1	FINGERPRINT PINS	30
6.11.1	FINGERPRINT TO ARDUINO	31

LIST OF ABBREVIATIONS

ABBREVIATION	DESCRIPTION
SVM	SUPPORT VECTOR MACHINE
IOT	INTERNET OF THINGS
LBP	LOCAL BINARY PATTERN
CNN	CONVOLUTIONAL NEURAL NETWORK
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEER
GUI	GRAPHICAL USER INTERFACE
SQL	STRUCTURED QUERY LANGUAGE
IDE	INTEGRATED DEVELOPMENT ENVIRONMENT
SSMS	SQL SERVER MANAGEMENT STUDIO
DIP	DUAL INLINE PACKAGE
DPI	DOTS PER INCH
FAR	FALSE ACCEPTANCE RATE
UML	UNIFIED MODELLING LANGUAGE

CHAPTER 1

INTRODUCTION

1.1OVERVIEW

The multi-pattern fingerprint security system is an innovative approach to enhance security measures. This system integrates an Arduino Uno board, a fingerprint sensor, and a database to provide advanced security features. The system's design allows for multiple fingerprint patterns to be stored in the database, increasing the system's flexibility and versatility. The proposed system is cost-effective and can be easily integrated into existing security systems. It can be used in various applications, including banking, healthcare, and government institutions, where advanced security measures are essential.

1.2STATE OF THE PROBLEM

1.2.1 WHY THE PROBLEM STATEMENT IS OF INTEREST

In the existing pattern the numeric security system (i.e.) the pin-based security system which we use in lockers, ATMs, and other sorts of protection lacks the uniqueness of the digit pattern which can be cracked easily using brute force attack, dictionary search, and many more. By entering the possibility 1234 itself we carry out 10% of the possibilities to crack a pin-based security pin so that the possibilities can be cracked easily and the values are pins cannot be unique, whereas in a people of 100 selecting the same number is 0.01% thus increasing the probability of number between 0 - 9, so this states the pin-based system is not unique and is easily crackable.

With the advancement in security system, the biometric security system was introduced which includes iris scan, fingerprint scan, face recognition, and voice recognition, and many more fingerprint security system stands out in prior which

was easy to use in automatic registration and in many bases which overcome all the disadvantages of pin-based security system, thus the fingerprint system lacks in combinations of inputs to make it strong, since these fingerprints can also be cracked using methods such as the traditional forensic method ink and glass print, master prints which is a method in common uses the possibility format named FAR(false acceptance rate) where a scanner with less FAR can be easily cracked whereas a scanner with high FAR is difficult, image scanning, forged fingerprints and exploitation of vulnerabilities which all expose the details of one person.

So far all the security systems cause disadvantages in the protection of one person which is been all these days as a state of the problem.

1.2.2 OBJECTIVE OF THE STUDY

Both pin-based and biometric security systems need advancement in security. protecting one's information by overcoming the disadvantages of both pin-based and biometric security systems.

In all aspects, both pin-based and biometric security system has some unique process or technique that is been followed to protect one's information so the objective of this paper is to correlate both the process or techniques used in a pin-based and biometric security system to overcome both systems disadvantages and make a reliable technique and secure platform.

1.2.3 RESEARCH QUESTIONS

- 1) Why do most security system uses pin even when they have biometric-based security system?
- 2) How do we prevent biometric data from more complex brute force attacks?
- 3) Does it require a more complex algorithm to store biometric data?

- 4) How to reduce time consumption for users to access our system?
- 5) How do we make a responsive and accurate scanner with the less FAR percentage
- 6) Why public organizations haven't used the biometric system primarily?
- 7) What is the type of sensor that is used?
- 8) Why fingerprint biometrics is used mostly other than other biometrics?

CHAPTER 2

LITERATURE REVIEW

2.1 LITERATURE REVIEW-1

TITLE: Finger-Knuckle-Print Recognition Using Deep Convolutional Neural Network

AUTHOR: Selma Trabelsi, Djamel Samai, Abdallah Meraoumia, Khaled Bensid, Azeddine Benlamoudi, Fadi Dornaika, Abdelmalik Taleb-Ahmed.

PUBLISHER: IEEE

YEAR: 2020

CONTEXT:

The "Finger-Knuckle-Print Recognition Using Deep Convolutional Neural Network" paper proposes a method for recognizing individuals based on their finger-knuckle prints. Finger knuckle print recognition is a relatively new biometric recognition technique that has gained attention in recent years due to its uniqueness, permanence, and ease of acquisition. Finger knuckle prints are the skin patterns that appear on the dorsal side of the finger joints, and they are as unique as fingerprints. The proposed method in this paper uses deep convolutional neural networks (CNNs) to extract features from finger knuckle print images and classify them into different classes. CNNs are highly effective in image recognition tasks and have been used extensively in various biometric recognition systems. The authors of the paper conducted experiments on two finger knuckle print datasets to evaluate the performance of their proposed method. The results showed that their method outperformed existing state-of-the-art methods in terms of accuracy, robustness, and efficiency. The application of

finger knuckle print recognition has several potential applications, including access control, identification in forensic investigations, and personal authentication in mobile devices. The proposed method in this paper provides a promising solution for accurate and efficient finger knuckle print recognition.

2.2 LITERATURE REVIEW-2

TITLE: Finger vein recognition based on Deep Convolutional Neural Networks.

AUTHOR: Lecheng Weng, Xiaoqiang Li, Wenfeng Wang.

PUBLISHER: IEEE

YEAR: 2020

CONTEXT:

The "Finger vein recognition based on Deep Convolutional Neural Networks" paper proposes a method for recognizing individuals based on the vein patterns in their fingers. Finger vein recognition is a biometric recognition technique that has gained attention in recent years due to its uniqueness and difficulty in replication. The proposed method in this paper uses deep convolutional neural networks (CNNs) to extract features from finger vein images and classify them into different classes. CNNs are highly effective in image recognition tasks and have been used extensively in various biometric recognition systems. The authors of the paper conducted experiments on a dataset consisting of finger vein images collected from 120 individuals. They used a pre-trained CNN model for feature extraction and a softmax classifier for identification. The results showed that the proposed method achieved high accuracy and robustness in identifying individuals based on finger vein patterns. The authors also compared their method with other state-of-the-art finger vein recognition methods and showed that their method outperformed them in terms of accuracy and efficiency. The application of finger vein recognition has several potential applications, including access control, personal authentication, and identification in forensic investigations. The proposed method in this paper provides a promising solution for accurate and reliable finger vein recognition using deep convolutional neural networks.

2.3 LITERATURE REVIEW-3

TITLE: Biometric Authentication Using Palm Dorsal Vein Patterns.

AUTHOR: Yutthana Pititeeraphab, Chuchart Pintavirooj.

PUBLISHER: IEEE

YEAR: 2019

CONTEXT:

The "Biometric Authentication Using Palm Dorsal" paper proposes a method for biometric authentication using palm dorsal features. Biometric authentication is the process of recognizing individuals based on their unique physical or behavioral characteristics. Palm dorsal refers to the surface on the back of the hand, and it contains unique features such as wrinkles, veins, and knuckles. The proposed method in this paper uses these features to authenticate individuals. The authors of the paper conducted experiments on a dataset consisting of palm dorsal images collected from 50 individuals. They used a feature extraction method based on Gabor filters to extract features from the images and a support vector machine (SVM) classifier for identification. The results showed that the proposed method achieved high accuracy and robustness in authenticating individuals based on palm dorsal features. The authors also compared their method with other state-of-the-art biometric authentication methods and showed that their method outperformed them in terms of accuracy and efficiency. The application of palm dorsal authentication has several potential benefits, including enhanced security, convenience, and accessibility. The proposed method in this paper provides a promising solution for biometric authentication using palm dorsal features.

2.4 LITERATURE REVIEW-4

TITLE: A Novel Algorithm for Secure Internet Banking with Fingerprint Recognition

AUTHOR: R. Priya, V. Tamilselvi, G.P.Rameshkumar.

PUBLISHER: IEEE

YEAR: 2014

CONTEXT:

"A Novel Algorithm for Secure Internet Banking with Fingerprint Recognition" paper proposes a secure algorithm for Internet banking that incorporates fingerprint recognition for user authentication. Online banking has become increasingly popular in recent years, but security concerns remain a major challenge for financial institutions and users. The proposed algorithm in this paper uses fingerprint recognition to authenticate users and ensure secure access to their online banking accounts. The algorithm involves a multi-stage process, starting with the capture of the user's fingerprint using a biometric sensor. The fingerprint is then processed and matched with a pre-stored template in a database, and if a match is found, the user is granted access to their account. The authors of the paper conducted experiments on a dataset consisting of fingerprint images collected from 100 individuals. They used a feature extraction method based on minutiae points and a support vector machine (SVM) classifier for identification. The results showed that the proposed algorithm achieved high accuracy and robustness in authenticating users based on fingerprint recognition. The authors also compared their algorithm with other state-of-the-art authentication methods and showed that their algorithm outperformed them in terms of accuracy and security. The application of fingerprint recognition in online banking has several potential benefits, including enhanced security,

convenience, and accessibility. The proposed algorithm in this paper provides a promising solution for secure Internet banking using fingerprint recognition.

2.5 LITERATURE REVIEW-5

TITLE: The Research of Double-biometric Identification Technology Based on Finger Geometry & Palm Print.

AUTHOR: Lang Zhai, Qi Hu.

PUBLISHER: IEEE

YEAR: 2011

CONTEXT:

The "Research of Double-biometric Identification Technology Based on Finger Geometry & Palm Print" paper proposes a method for biometric identification using both finger geometry and palm print features. Biometric identification is the process of recognizing individuals based on their unique physical or behavioral characteristics. The proposed method in this paper combines two types of biometric features: finger geometry and palm print. Finger geometry refers to the shape and size of the fingers, while palm print refers to the unique patterns on the palm. By combining these two types of features, the proposed method aims to improve the accuracy and reliability of biometric identification. The authors of the paper conducted experiments on a dataset consisting of finger geometry and palm print images collected from 100 individuals. They used a feature extraction method based on local binary patterns (LBP) to extract features from the images and a support vector machine (SVM) classifier for identification. The results showed that the proposed method achieved high accuracy and robustness in identifying individuals based on both finger geometry and palmprint features. The authors also compared their method with other state-of-the-art biometric identification methods and showed that their method outperformed them in terms of accuracy and efficiency. The application of double-biometric identification technology has several potential applications,

including access control, personal authentication, and identification in forensic investigations. The proposed method in this paper provides a promising solution for accurate and reliable biometric identification using multiple features.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

There are many services and providence through fingerprint security systems such as biometric door locks, time and attendance systems, mobile devices, payment systems, and border control which are prolonged sustained in use for specific purposes and in security which is termed to be the existing system, meanwhile which also has a lot of drawbacks namely accuracy, privacy and hygiene concern and limited applications. To resolve all the issues we tended to create the proposed system.

3.1.1 DISADVANTAGES

- 1) lack of combinations and uniqueness
- 2) low affirmation of protection or security
- 3) security can be easily breached or biased using some known techniques such as brute-force attacks, master prints, etc...

3.2 PROPOSED SYSTEM

The proposed system “Multi-pattern fingerprint security system” improvises the method of fingerprint recognition which includes combinations of multiple fingerprints that results in a complex pattern. Thus the system uses an Arduino UNO board to access the data, where the data is collected from the fingerprint scanner from the user of different fingers in series is been and applied or saved onto the data in the database (SQL server), thus the modification of

finger data requires verification of the person who is been the user in this case, the following images and code explain the proposed system briefly. Thus this advancement also tends to cost-effectiveness, security of one's data, and accessibility. The system also significantly makes the security system different from the usual or existing system where in simple words "four unique patterns for a single use er". In the existing system, a user has only single biometric data, whereas in the proposed multi-pattern fingerprint security system the user will have four unique biometric identification thus providing better protection than the existing system.

3.2.1 ADVANTAGES

- 1) Justifies possible protection by including both the causes in the existing method that is uniqueness and combination
- 2) Could affirm high-rated protection and security
- 3) Not easy to breach one's data because requires a lot of data to breach itself

CHAPTER 4

REQUIREMENT ANALYSIS

4.1 SOFTWARE REQUIREMENTS

4.1.1 ARDUINO IDE

An Arduino integrated development environment (IDE) is an open-source software used for development purposes in terms of uploading programs to any programmable circuit board that can do a specific task. It consists of layouts including a sketchbook used to sketch or write programs in text using a variant of C++ language, library management is used to manage, find and update both internal and external libraries to be included in the sketches, the serial monitor is used to monitor the serial output, the serial plotter is used to track different data, board manager is used to managing the different boards that are connected to the uploading device and debug used to find and resolve problems in the sketch which makes an IDE markable in developing programmable circuit board projects.

In specific, libraries in Arduino IDE are used in vast areas including two sections type and topic where type consists of what type of the library is required whether that is installed, updated, or pre-built, and topic includes on what basis such as communication, sensors, data processing and many more.

In Arduino sketch the language used is C++ programming language but a slight variant in it for circuit boards which is compatible, fast, and stable thus a good choice for microcontrollers, here the compiler is used to transform the code into object files (i.e) avr-g++ and the program is uploaded into the microcontroller using the program avrdude which can be collected from the library or that is prebuilt in Arduino itself where sketches in Arduino are saved using the extension .ino.

4.1.2 MICROSOFT SQL SERVER MANAGEMENT STUDIO

The Microsoft SQL server management studio (SSMS) is an open-source integrated environment used to manage, access, configure and develop all needed components of a Microsoft SQL Server, Azure database, Azure VM, and many more thus this studio is prolonged especially to manage databases for any server or collection of databases.

An SQL is termed a structured query language used to manipulate, define, and control records in databases and an embedded SQL is the computing power of a programming language such as c programming language in this case it is C++ with the data manipulation, definition, and controlling of SQL, where SQL statements can be written inline to the source program (i.e) the correlating programming language.

SQL server also has several authentication prompts, thus it is a series of encrypted messages to authenticate SQL users use two methods to authenticate the user one is the Windows authentication mode and another is the mixed mode where in Windows authentication mode windows authentication is enabled and the SQL server is disabled whereas in mixed mode both the windows authentication and the SQL server are enabled.

In all factors above from basic, SQL has a lot of advantages for this project to be engraved in to make this project clarify and to reveal the data that is been stored for only the administrators or the creators.

4.1.3 WINDOWS FORM APPLICATION

Microsoft visual studio is an open-source integrated environment development tool used to develop computer programs in this case we use visual studio to develop a form page and registration page for the data entries and manipulation of the user.

With the help of visual studio, we managed to create a form page by Windows form page application (.NET framework) which can take data from the user and store them in the database that we created, it also has a variety of languages that can be accommodated a variety of platforms such as android, IOS and much more and variety of project types such as IOT, cloud desktop, games and many more, where visual studio also provides applets for all aspects of projects and has many designing properties for visual understanding of the user.

In our project, we used many properties and data sources for each page to collect the details of the user on various pages such as the login page, registration page, and fingers can page.

To create this form page we used c# language which is an object-oriented type-safe programming language. c# language is used to develop more robust applications that run if .NET framework where .NET framework is used to create and run applications.

Connecting form page inputs in the database to the Arduino can be done via serial port serialization where the exact inputs ports and output ports are to be set in place of code in c# and c++ so.

4.2 HARDWARE REQUIREMENTS

4.2.1 ARDUINO

The Arduino is a programmable circuit board that has several variants in it, in this project we have used the ARDUINO UNO R3 board based on a removable, dual inline package (DIP) and an ATmega328 microcontroller. The Arduino uno r3 microcontroller has 20 digital input/output pins where 6 pins are PWM and another 6 pins are analog. To make this microcontroller work the power source can be either from an AC - DC adapter or a battery of 6-20V(volt) where the

microcontroller Atmega328 itself consumes 80mA at peak during the writing phase.

The ATmega328 microcontroller is an 8-bit AVR RISC-based microcontroller of 32kb flash memory and 2kb of SRAM which has a maximum CPU speed of 20MHz. The ATmega328 has its variants namely ATmega328p and ATmega329PB.

4.2.2 FINGERPRINT SCANNER

The optical fingerprint scanner is a scanner that captures a 2D image with good high resolution which is measured by dots per inch (DPI) takes 2D image of a fingerprint using a digital camera where an illuminate light is passed on the space to keep the fingerprint and the camera captures the fingerprint in the 2D image and stores it in the allocated storage medium.

In specific, the storage capacity of a fingerprint sensor is 127 print locations and the type of data stored in the fingerprint sensor is a finger image in turn a 2D image.

A fingerprint sensor consists of 6 pins where the first pin is allocated to the power supply and the second pin is allocated for the ground signal to avoid shock and other instances of earth wiring to electrical appliances, the third and fourth pin is used to transfer and receive finger image and the next fifth and sixth pin are not mandatory can be used in case of the finger detection signal and touch indication power supply.

CHAPTER 5

METHODOLOGY

5.1 LOGIN FORMS:

Here in the login form section, we collect data from the user that is the details from the user such as username and preferred password. By development, we used the path of the SQL server management studio to store the data of the user in the created login database in the server and a connection is been created between the login page and database under the login function which is been coded to collect the data from the user. Without login completion, the user cannot enter the security panel which is the authentication section.

Refer figure(6.3.1)

5.2 REGISTRATION CATALOG:

From successful login, the user can enter the registration catalog, which has three primary sections namely the registration section, database grid view, and the task section where each section has its priorities and specification. From the registration section, the user has to enter his details included on the page. To newly include data the registration can be completed by adding a combination of a fingerprint concerning the ID of the user which will be followed, after enrolling the user data will be visible in the database grid view and the data of some specific users can be searched using the search bar. In the task section, there will be two buttons one to save, and another to modify where this modification includes the updation of data and deletion of data. Once the data is been enrolled it has to be saved to be viewed in the grid view if any changes have to do means the modify button helps here, even though to modify the data the system authenticates your

fingerprints to make the user modify such as update or delete his\her data from the database.

Refer figure(6.4.1)

5.3 FINGERPRINT SCAN FORM:

After completion of registration with a unique ID, now the user will be able to add his fingerprint to the system through the optical fingerprint sensor. Here in this fingerprint storing form, the ID mentioned in the registration form will be visible in the biometric data pallet, then as said this is the combination and uniqueness of the security system the user will be mentioning his unique number in different aspects below the Redbox available and after entering data onto the textbox the user will be requested to enter his different combination of fingerprints to complete his enrollment by clicking the scan button below the textbox for each different biometric data, after successful entry of fingerprint, the Redbox will turn into green-boxes which resembles in a successful entry of fingerprint and by clicking the submit button the given biometric data of the user will be stored into the database as per the ID given concerning each byte code saved in the sensor by itself.

Refer figure(6.5.1)

5.4 FINGERPRINT CHECKING FORM:

This form is used in the modification section, where if a user needs to modify his data the user will be authenticated with his biometric data concerning the combinations given by the user himself so then the user will be able to modify the details which will be resembled into the database. The process of checking is also similar to storing method, for each biometric data the scan button has to be

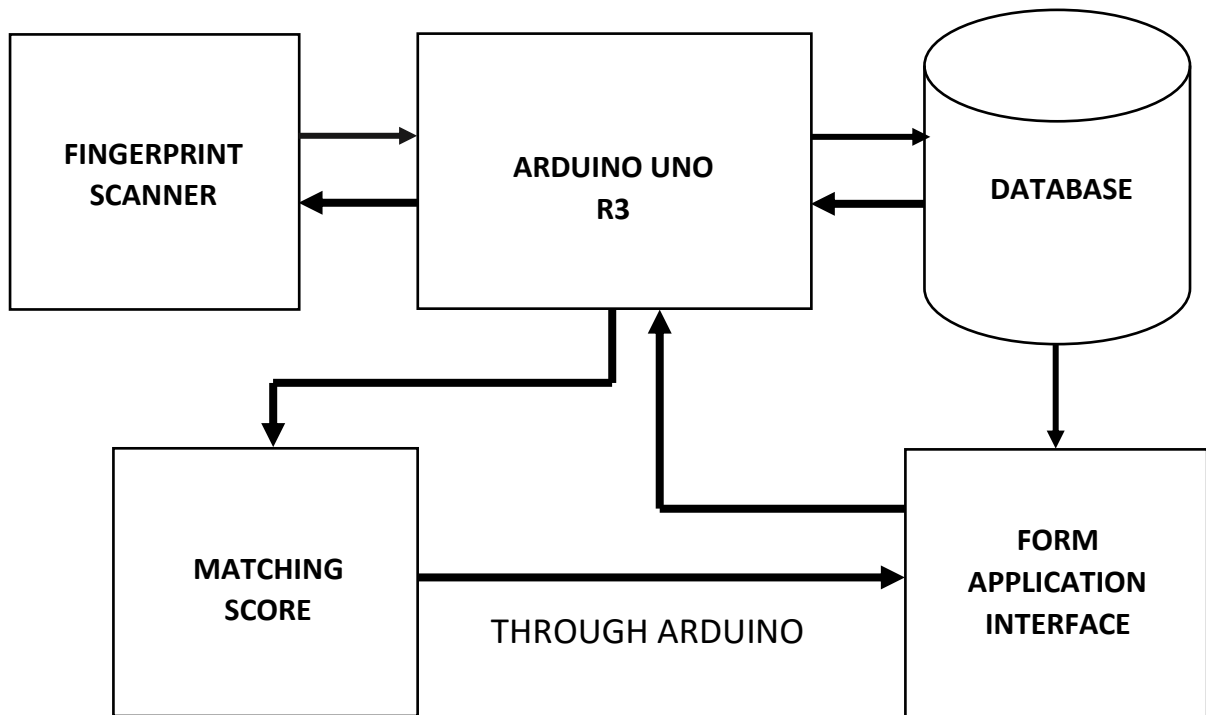
clicked to authenticate the user's biometric combination and to be verified for further processes such as updating new data or deleting the existing data.

Refer figure(6.6.1)

CHAPTER 6

SYSTEM DESIGN

6.1 ARCHITECTURAL DESIGN:

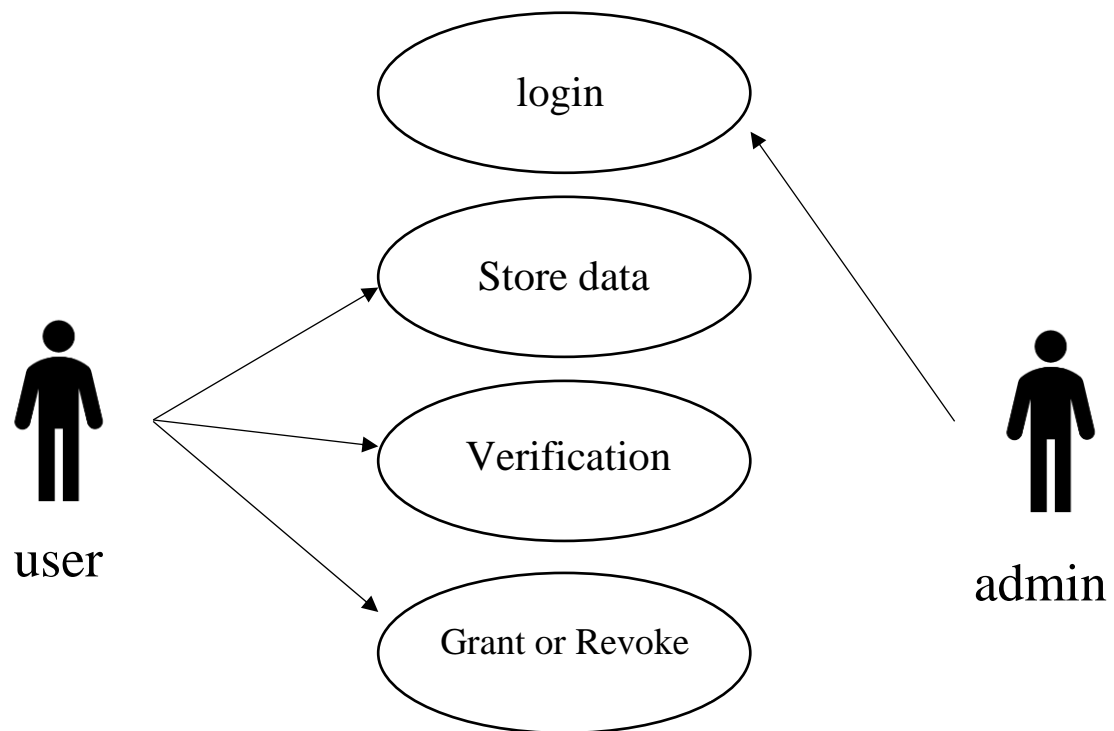


6.1.1 Workflow of the system

Here this is the architectural or model design of the project. This resembles the workflow of the process, where the data comes from the user as a fingerprint and is been processed in the Arduino the data will be stored in the database for each process such as updation and deletion the process opens up to authenticate the user by moving to the previous process, in which all these instructions to the user is carried out by the form application interface.

6.2 UML DIAGRAM:

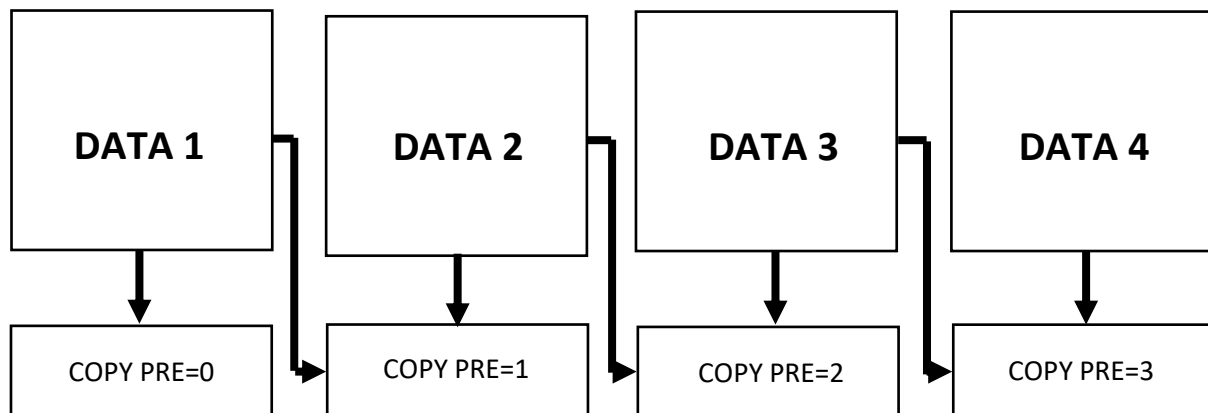
6.2.1: USE CASE DIAGRAM:



6.2.1.1 Use case diagram

The above use case diagram is an implementation of our project, it consists of login, store data, verification, grant or revoke process. Here admin can only access the login page which enables another user to process consecutive operations. In the remaining phases, the user can store the data, which later can be used on verification, then grant and revoke access to the user based on the result of verification.

6.3 STORING AND RECEIVING THROUGH FINGERPRINT SCANNER:

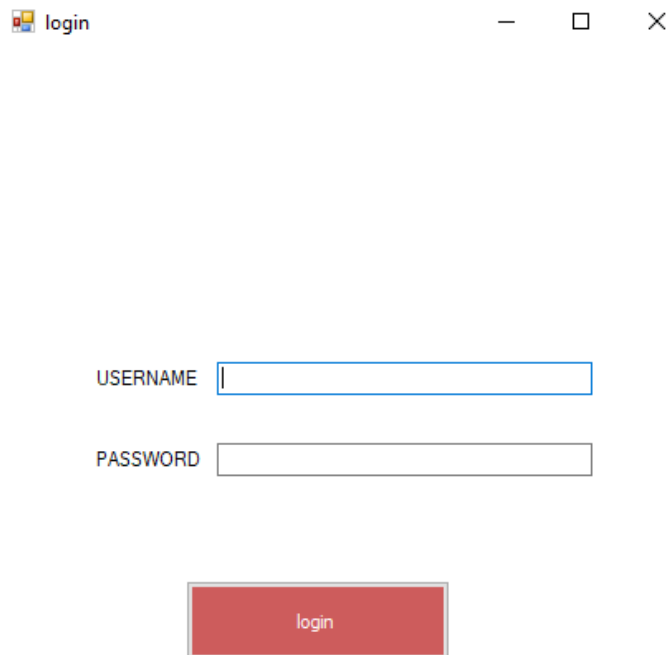


6.3.1 Working of the fingerprint

This is the schema of how the fingerprint store and fingerprint check will work. Here the data entered by the user is the data 1 which will be pre-copied as 0 for identification in the optical fingerprint sensor, and when the data (i.e) the biometric data is approved then the data will turn green symbolizing the biometric data is accepted by the system and thus follows for all the data 1, data 2, data 3 and data 4. Thus this is the functionality of the finger scan and finger check page which is shown on page 24 and page 25 (images 6.5.1 and 6.6.1).

All the data 1,2,3 and 4 are resembled in color red and copy pre-data are resembled in green where the workflow is followed by the directions provided in the system.

6.4 LOGIN FORM:



The image shows a screenshot of a Windows-style application window titled "login". The window has a title bar with a minimize button, a maximize button, and a close button. Inside the window, there are two input fields: one labeled "USERNAME" and another labeled "PASSWORD". Below these fields is a red button labeled "login".

6.4.1 Login

This is the login page form where the user has to give his username and appropriate password to be logged in. This is the authentication portal where the system recognizes any the users that have been assigned to the system and thus the data of the user (i.e) the username of the user and the password of the user is stored on the database which is shown in page 26 (image 6.7.1.1).

These applications are designed through the visual studio which is termed as Windows applications where each page is designed specifically for a certain purpose.

6.5 REGISTRATION FORM:

The screenshot displays a web application interface titled "LOG". It is divided into two main sections: "REGISTRATION" and "TASK".

REGISTRATION Section:

- NAME:** A text input field.
- FATHER NAME:** A text input field.
- DESIGNATION:** A text input field.
- EMAIL:** A text input field.
- ID:** A text input field.
- GENDER:** Radio buttons for "male" and "female".
- ADD FINGERPRINT:** A button.
- UPLOAD IMAGE:** A button.
- SEARCH:** A text input field.

TASK Section:

- A large empty white box for a profile picture.
- SAVE:** A red button.
- MODIFY:** A green button.
- UPDATE:** A red button.
- DELETE:** A red button.

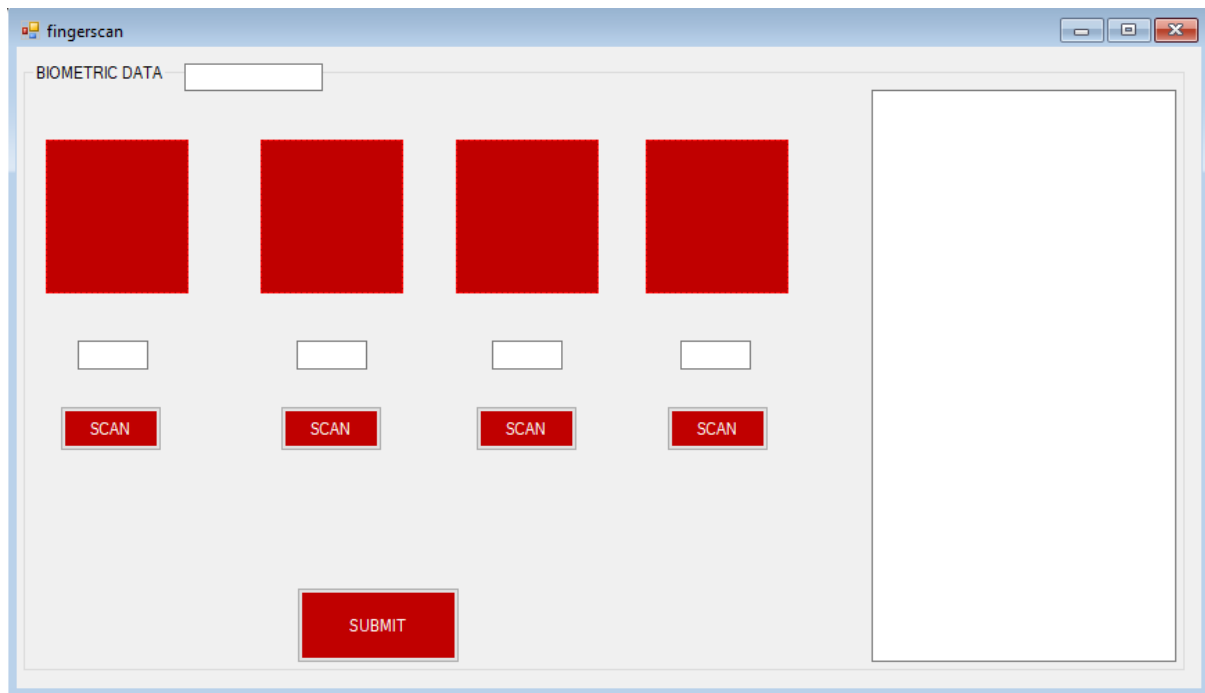
Database Grid View:

	p_id	p_name	p_fname	p_email	gender	p_designation
*						

6.5.1 Registration interface

This is the registration form page where there are two primary phases the registration phase and the task phase. Which also includes the database grid view and other components mentioned in the registration catalog. The registration phase is the application (image 6.4.1) which is the interface that enhances the user experience. On this page, the user has to provide his name, father's name, designation, mail-id, gender, and a specific ID to know the registered details of the users. Whereas the task phase (grid view) shows the number of users registered to the system where the data in the task phase is connected to the database where each data registered through the registration phase is logged onto the task phase and also through the registration phase itself the user's image will also be applied to verify the user.

6.6 FINGERPRINT SCAN:



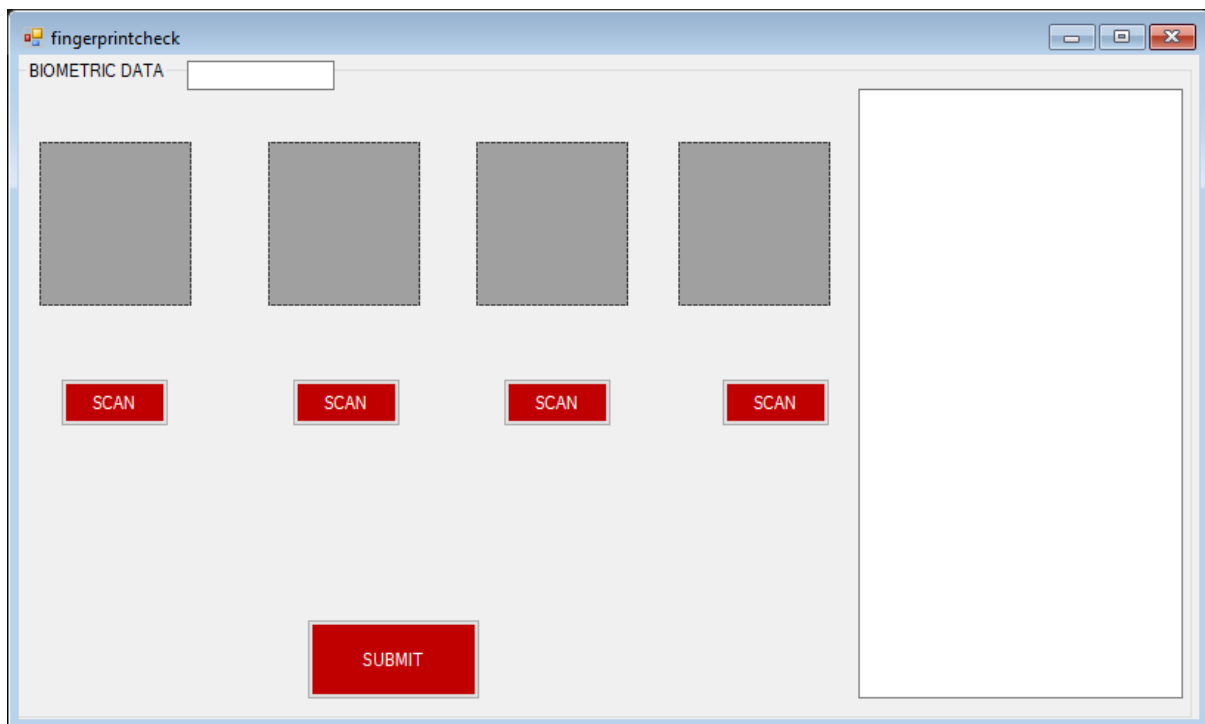
The screenshot shows a web browser window titled 'fingerscan'. Inside the window, there is a form with the following elements:

- A label 'BIOMETRIC DATA' followed by a text input field.
- Four red square buttons arranged in a horizontal row.
- Below each red square button is a small white rectangular input field.
- Below each white input field is a red button labeled 'SCAN'.
- At the bottom center of the form is a large red button labeled 'SUBMIT'.
- On the right side of the form is a large, empty white rectangular area.

6.6.1 Finger scan page

This is the fingerprint scan page where the biometric data will be collected from the registration pages and by clicking on the scan button user will be able to enter his biometric data has four different data each. This page is followed after registering the basic details of the user, also the specific ID provided by the user will stand as the biometric data ID for the user. Each biometric data has to be entered by the user after acceptance of the biometric data by the system the data will be stored in the database in byte format according to the biometric data provided by the user itself. So the data can be viewed by the admin in the database as bytes and the data can be further accessed on the registration page only.

6.7 FINGERPRINT CHECK:



The screenshot shows a window titled "fingerprintcheck" with a standard Windows-style title bar (minimize, maximize, close buttons). Inside the window, there is a label "BIOMETRIC DATA" followed by a text input field. Below this, there are four square gray boxes representing fingerprint scan areas. Each box has a red "SCAN" button centered below it. At the bottom center of the window is a red "SUBMIT" button. On the right side of the window is a large, empty white rectangular area, likely for displaying a user's photo or additional information.

6.7.1 Finger verification page

Check form used to detect the identity of the user through patterns of biometric data stored already. At first, the user enters their respective pins for fingerprint data on each text box. when the user hit the scan button of the respective finger I'd, it sends the response to the fingerprint scanner to detect biometric data. On consecutive entries of biometric data, if all four data are checked and verified successfully, submission becomes available to the user and allows the user to further processing. The form contains an I'd box which contains the respective I'd of the user details. Here I'd box used as a mapping attribute to four fingerprints I'd stored in the finger data table.

6.8 DATABASES:

6.8.1 LOGIN PAGE DATABASE (sample):

	u_id	u_name	u_pass
1	1	anand	key
2	2	aravindhana	key

6.8.1.1 Login database

Each column resembles the details of the user from the login page.

6.8.2 REGISTRATION PAGE DATABASE (sample):

p_id	p_name	p_fname	p_email	gender	p_designation	p_idcode	pic
------	--------	---------	---------	--------	---------------	----------	-----

6.8.2.1 Registration database

Each column resembles the details of the user from the registration page.

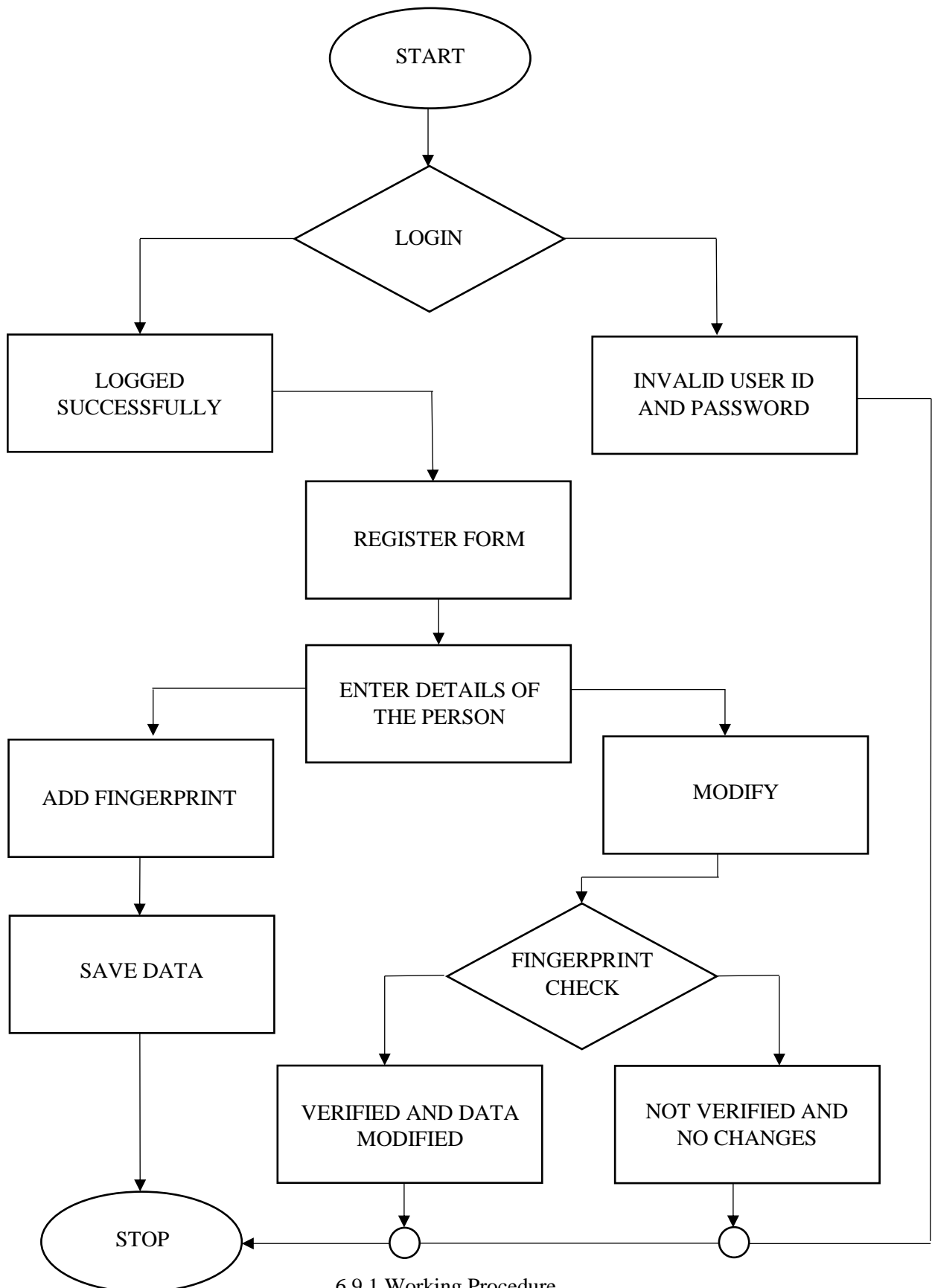
6.8.3 FINGERPRINT DATABASE:

	f_id	f_idcode	f_id1	f_id2	f_id3	f_id4
1	1	1234	3	4	5	6

6.8.3.1 Finger code database

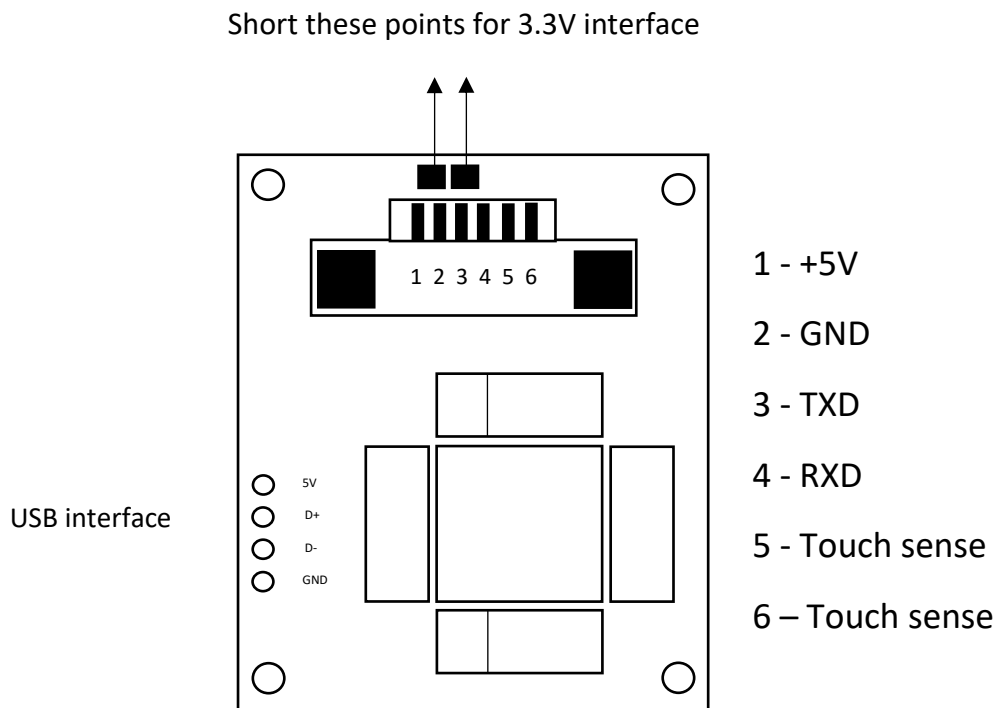
Each column resembles the fingerprint data of the user from the fingerprint scan page.

6.9 WORKFLOW DIAGRAM:



6.9.1 Working Procedure

6.10 FINGERPRINT SENSOR PIN DIAGRAM:



6.10.1 Fingerprint pins

Description of connection:

1.+5v

The 5-volt port is used to supply power supply to the fingerprint scanner, as it used in the optical sensing method to detect and store fingerprint data

2. gnd

GND is a ground pin on the fingerprint sensor which is then connected to the ground pin Arduino Uno rev 3. This balances the power supply between Arduino and the sensor.

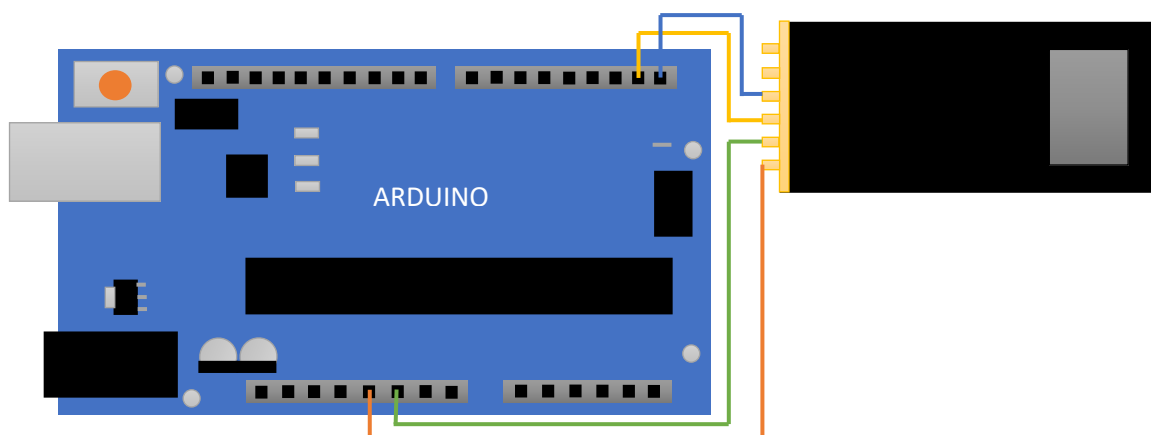
3.txd

The txd pin is the transfer data pin on the fingerprint sensor which is connected to the receiving data pin on the Arduino board. it provides communication between the board and the sensor

4.rxd

Rxd is a receiving data pin on the fingerprint sensor in which another end is connected to and pin on the Arduino board .it provides communication between the board and the sensor

6.11 ARDUINO TO SENSOR CONNECTIVITY:



6.11.1 Fingerprint to arduino

As we can see in the above connection, the Arduino board contains 14 digital inputs/outputs out of which 6 can be used as PWM outputs), 6 analog inputs, and a 16 MHz ceramic resonator, here we connected a 5v pin sensor to a respective 5volt socket in Arduino, ground pin in sensor connected to respective ground in Arduino Uno, transfer data pin fingerprint connected to respective receiving data pin, Receiving data pin in sensor connected to transfer data pin in Arduino Uno.

CHAPTER 7

RESULTS AND DISCUSSION

7.1 FUTURE WORKS:

1. Enhancing the UI and UX design
2. Including gestures that make the work of the user easy and convenient.
3. Optimizing the data collection much faster.
4. In the purpose of automation and the use of machine learning is to predominantly reduce the time complexity even more.
5. Surpassing the use of databases by cloud storage because databases might cost large amounts of data.
6. Increase in use of this security system in various fields such as home security and many more.
7. Enhancement of fingerprint scanner with high FAR (false acceptance rate).
8. Development of mobile applications for different use cases.
9. Integrating the same methodology with other biometric modalities.

CHAPTER 8

CONCLUSION

In this advanced technological world, the data of one individual can be shared over the network very easily even though with many security systems, but they all have certain limitations of work which can be easily biased which leads to leakage of data. So we collectively gathered information on the protection enhancement of data and we developed the multi-pattern fingerprint security system which can stand as a firewall for the data that are been stored in any kind of database. This is the more enhanced, improvised security system that we deliver for the privacy of one individual.

CHAPTER 9

REFERENCES

- [1] BENSID, Khaled, SAMAI, Djamel, LAALLAM, Fatima Zohra, et al. Deep learning feature extraction for multispectral palmprint identification. *Journal of Electronic Imaging*, 2018, vol. 27, no 3, p. 033018.
- [2] Eryun. L, Jain A.K, and Jie.T, "A Coarse to Fine Minutiae-Based Latent Palmprint Matching," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 35, no. 10, pp. 2307-2322, Oct. 2013.
- [3] FAKHAR, Khalid, EL AROUSSI, Mohamed, SAIDI, Mohamed Nabil, et al. Fuzzy pattern recognition-based approach to biometric score fusion problem. *Fuzzy Sets and Systems*, 2016, vol. 305, p. 149-159
- [4] JAMDAR, Shradha D. et GOLHAR, Yogesh. Implementation of uni-modal to multimodal biometric feature level fusion of combining face iris and ear in a multi-modal biometric system. In: *2017 International Conference on Trends in Electronics and Informatics (ICEI)*. IEEE, 2017. p. 625-629.
- [5] Kun Ling; Yingjie Lei; "Research on palm vein recognition algorithm based on improved AlexNet convolution neural network". *Modern electronic technology*, 2020 (7): 43-56.
- [6] Li Gu, Zhenquan Zhuang, Shuchao Wan and so on. An Algorithm of Hand Geometry Authentication Based on Template Matching [J]. *Computer Project and Application*, June 2005:85-88.
- [7] Liu T.; Xie J.; B.Yan; W., et al. "An algorithm for finger-vein segmentation based on modified repeated line tracking" *The Imaging Science Journal*, 2013, 61(6):491-502 [6] Miura N.; Nagasaka A.; Miyatake T. "Extraction of [1]

- [8] Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles” IEICE Transactions on Information and Systems, 2007,90(8):1185-1194
- [9] Li. W, D. Zhang, and Xu. Z, "Palmprint Identification by Fourier Transform," International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 4, pp. 417-432, Jun. 2002.
- [10] Mingxing, HE, HORNG, Shi-Jinn, FAN, Pingzhi, et al. Performance evaluation of score level fusion in multimodal biometric systems. Pattern Recognition, 2010, vol. 43, no 5, p. 1789-1800.
- [11] Meiru Mu, QiuQi Ruan, and Yongsheng Shen, "Palmprint Recognition Based on Discriminative Local Binary Patterns Statistic Feature," Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, pp. 193-197, 9-10 Feb. 2010.
- [12] Sanchez-Reillo. R, Sanchez-Avila. C, and Gonzalez-Marcos. A, "Biometric identification through hand geometry measurements," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 22, no. 10, pp. 1168-1171, Oct 2000
- [13] Saropourian. B, "A new approach of finger-print recognition based on neural network," Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, pp. 158- 161, 8-11 Aug. 2009.
- [14] SOVIANY, Sorin et JURIAN, Mariana. Multimodal biometric securing methods for informatic systems. In: Proceedings of the 2011 34th International Spring Seminar on Electronics Technology (ISSE). IEEE, 2011. p. 447-450.
- [15] TAO, Qian et VELDHUIS, Raymond. Threshold-optimized decision-level fusion and its application to biometrics. Pattern Recognition, 2009, vol. 42, no 5, p. 823-836.

[16] Vikram Singh and Kalpna Kashyap, “A survey paper on “hybrid system for fingerprint identification”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 1, Issue 4, November – December 2012, ISSN 2278-6856

[17] Wu Chao; Shao Xi;” Study on finger vein recognition based on deep learning” Computer Technology and Development, 2018, V. 28; No.250(02):206-210.

[18] Zhang Z; Ma S.; Han X. “Multiscale Feature Extraction of Finger-Vein Patterns Based on Curvelets and Local Interconnection Structure Neural Network” 18th International Conference on Pattern Recognition 2006:145-148