MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION Federal State Autonomous Educational Institution of Higher Education
“South Ural State University (National Research University)”
School of Electrical Engineering and Computer Science
Department of Computers

THESIS IS CHECKED

Reviewer,

PhD, Associate Professor

_____ N.V. Plotnikova

“___”_____ 2021

ACCEPTED FOR THE DEFENSE

Head of the department,
PhD, Associate Professor

_____ G.I. Radchenko

“___”_____ 2021

ATTENDANCE ACQUISITION & INFORMATION MANAGEMENT SYSTEM USING BIO-METRICS AND IOT

GRADUATE QUALIFICATION WORK
SUSU – 09.04.01.2021.308-642.GQW

Supervisor,
PhD, Associate Professor
_____D.V. Topolskiy

Author,
student of the group KE-228
_____AL Abdullah Maher Safauldeen

Normative control
_____ S.V. Syaskov
“___”_____ 2021 г.

Chelyabinsk–2021

FEDRATION Federal State Autonomous Educational Institution of High Education "South Ural State University (National Research University)"

School of Electrical Engineering and Computer Science

Department of Internet of Things

APPROVED

Head of the department

Dr. Sci., Prof.

_____- _____- 2021

TASK

of the master graduate qualification work

for the student of the group KE-228

AL Abdullah Maher Safauldeen Yaseen

in master direction 09.04.01

"INTERNET OF THINGS (Master Program "INTERNET OF THINGS")

1.The topic (approved by the order of the rector from ..2021 , No.)

"ATTENDANCE ACQUISITION & INFORMATION MANAGEMENT SYSTEM USING BIO-METRICS AND IOT"

2. The deadline for the completion of the work: .06.2020.

3. Source of Data for the Work

R. Dutta, T. Tamang, P. Paul, N. Kumar, C. Chetri and P. K. Dutta, "Smart and Secure Fingerprint Attendance System using Arduino UNO with GSM Alert," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1086-1090, doi: 10.1109/ICISS49785.2020.9316127.

M. Srivastava, A. Kumar, A. Dixit and A. Kumar, "Real Time Attendance System Using Face Recognition Technique," 2020 International Conference on Power

Electronics & IoT Applications in Renewable Energy and its Control (PARC), 2020, pp. 370-373, doi: 10.1109/PARC49193.2020.236628.

K. A. Alnajjar and O. Hegy, "Attendance System Based on Biometrics and RFID," 2019 Fifth International Conference on Image Information Processing (ICIIP), 2019, pp. 596-599, doi: 10.1109/ICIIP47207.2019.8985745.

S. Chennattu, A. Kelkar, A. Anthony and S. Nagdeote, "Portable Biometric Attendance System Using IOT," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 245-249, doi: 10.1109/ISCON47742.2019.9036275.

4. List of Development Issues

- To develop an electronic system to manage student attendance.
- To develop a system to measure the performance of students.
- To develop an effective and efficient method for student roll call.
- To improve upon the taking of attendance by making it easier and faster.

Table of Contents

INTRODUCTION

Lately, there has been a high level of impersonation happening each day within the education system, both non-public and public sectors(education). Statistics is something and everything that can be measured in every creature. Fingerprints are a type of statistics identification that's distinctive and cannot be changed or modifiedin one's entire life. This paper presents associate degree increased attending management system employing a fingerprint system in a very university atmosphere. it had been developed exploitation the water methodology. this method consists of 2 procedures: entering and identification. throughout the enrollment, the fingerprint of someone is captured and its distinctive options extracted and hold on within the information in conjunction with the user's information because the model for the topic. throughout identification, the fingerprint of the person is once more captured and also the extracted feature is compared with the model within the information in a very magnitude relation of 1: N-templates, to spot a match (a user) before attending is created [21]. The identification mode operates day by day of attending, the fingerprint image is extracted from a personal and also the system conducts a one-to-many comparison to ascertain a personal identity (or fails if the topic isn't registered within the system database) with the topic having to say associate degree identity [26]. The results of the system show that the projected methodology is secured, reliable, and capable of averting impersonation.

1. Analysis of Subject Area

Any educational institute, public or private must keep precise and detailed attendance records of student or staff attendance in order to function effectively.As proven time and again, a lot of mismanagement of such attendance system is noticed in both the private and public institutions as a result of forged documents, besides faked identities like making impersonation of other students and staff. In universities and schools , keeping track of

attendance is a crucial task. Especially in case of huge strength in the number of students, any manual recording of attendance demands a lot of time as well as efforts. Generally, faculty members do not record students' attendance and instead ask them to authenticate manually by insisting on signature on a attendance file, thus making it look inaccurate and open to dispute. It is also possible to sign in place of another student. Students may falsify their signatures on attendance forms [5]. As a result, we may experience numerous problems and issues with manual attendance system. Many people try to give many solutions to overcome this problem but still they are not able to find the exact solution. Despite the advent of high-tech methods, they are not used in places of tight monetary restrictions. Our objective here is to come up with a biometric system that is not only accurate, but also affordable to the masses. Our focus here will be on fingerprint scanning and information processing [6],[7].

Biometrics

Biometrics refers to techniques for identifying people on the basis of a single or a number of peculiar or unique characteristics, be it it related to physical or behaviour. Biometrics is applied to establish identity systems to manage access and control in computer systems. Further, single persons are identified, even from large groups that are surveyed[8].

Broadly, there are only two classes under which all the Biometric traits can be classified:

- **Physiological** aspects have linkages to the body's shape. Fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition in lieu of retina, and odor/scent are just a few illustrations [3].
- **Behavioral traits** are a person's typical behaviour that is influenced by many psychological and social aspects. Typewriting rhythm, gait, and voice are just a few illustrations. This category of biometrics has been dubbed "behavioural metrics" by certain scientists [2].

  Although voice identification is mostly focused on the study of how a person talks, which is typically defined as behavioural, voice is also a

physiological attribute because every individual has a distinctive vocal tract. In terms of the following parameters, it is possible to determine whether a human characteristic can be used for biometrics [4].

- **Universality:** It means that such a trait is found in every individual.
- **Uniqueness:** On this basis, the biometric system establishes the uniqueness of one person by separating him/her from others.
- **Permanence:** This trait helps in making the biometric system overcome the limitations of age and can make the record last beyond age and time of the subjects.
- **Collectability:** It supports in making the traits easily acquired for measurement
- **Performance:** Establishes precision, speed, and robustness of the applied technologies.
- **Acceptability:** It proves the efficacy in terms of the acceptance of technology.
- **Circumvention:** Easy availability or facility for substitution by another thing.

Biometrics can be used to establish a person's identity based on their real identity over what they have, like ID card, or what in their memory or recollection in terms of a password. Biometrics can complement ID cards and passwords in some cases, adding an extra layer of security. A dual-factor authentication scheme is what this kind of setup is known as [1],[2],[3].

In essence, a biometric system offers a facility to recognize patterns that make it look like a recognition system by collecting biometric information belonging to a person. An extracted key feature set from that dataset is compared to the feature set(s) found in the database that forms the basis of a decision. A biometric system thus has the following basic

modules: a raw data acquisition module, quality improvement module (preprocessing module), feature extraction module, a matching module, and a database module [26].

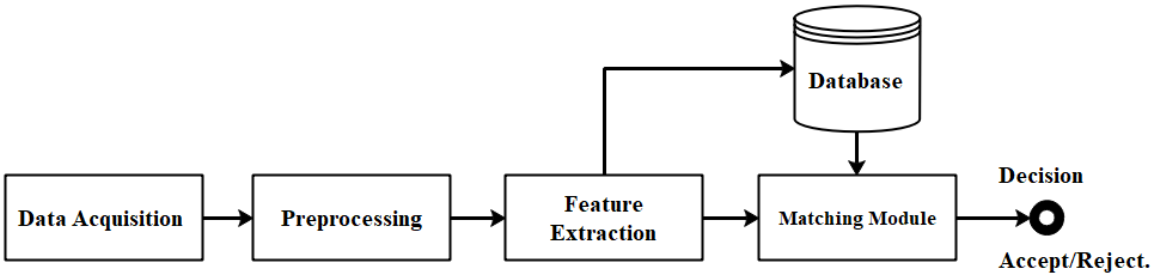

Fig.1.1Basic Block diagram of a biometric system

Data acquisition module: The raw data from the individual may be obtained by using an appropriate sensor, camera, or a scanner. This module must be capable of acquiring good quality images for the biometric system to provide good performance [4].

Feature extraction module: Next a suitable algorithm is applied on the preprocessed image to extract the features (a compact representation of the preprocessed image) that can be used to uniquely identify a person. The extracted features a restored as templates in the database [5].

Matching module: For a given test or a query image, the features are extracted and then compared with the stored templates in the database to measure the level of closeness between template and the extracted features. Decision is then made as whether the individual or the user is a genuine(authorized or enrolled user) or an impostor (unauthorized user) depending on the observed closeness measure [6].

Database module: The feature set derived from the raw biometric data (i.e., the template) is kept in the database, together with some other information about the user (such as name, PIN, address, etc.)[34].

Modes of Operation

The operation of biometric systems is done in three modes viz., Enrollment , Identification and Verification mode. They are explained as follows..

- **Enrollment Mode**: A user has to first enroll or register his/her biometric trait in the system before recognition. Here, the raw data gets sourced from user(s), preprocessed prior to extracting the features, after which they are left to store in database as master template alongside additional information like name or roll number of each of the users. This master template is compared with test template during recognition [7].

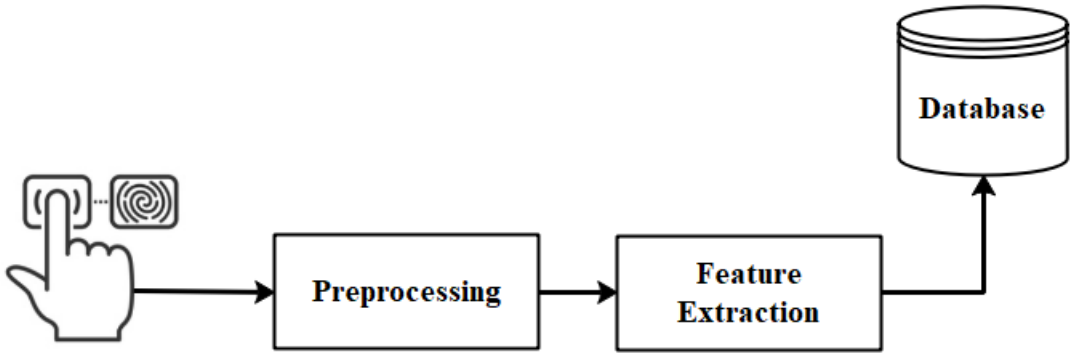

Fig.1.2. Enrollment Mode Block diagram

Identification Mode: This is defined as the identification of the user which is done by processing the unique biometric trait before gaining any information about the user identity. During the identification phase a user goes through the same procedure as mentioned in the enrollment phase to provide the template which is called the test template [10]. The test template is then compared with the master template in the database for matching or recognition. The matcher then decides to “Accept” if the test image is provided by a genuine user who has registered into the system or “Reject” if provided by an impostor who has not registered into the biometric system. This is also referred to as one-to-many matching [9].

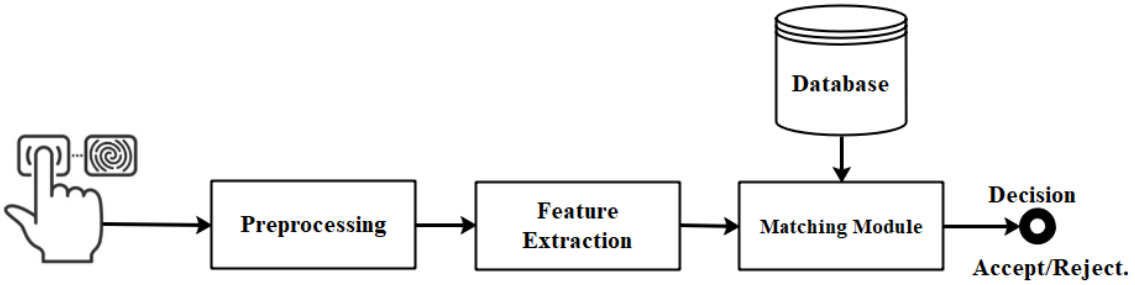

Fig.1.3 Identification ModeBlock diagram

Verification Mode: In this stage, focus is on establishing the identity of the user on the basis of the submitted identity like ID cards, smart cards or ID numbers, after which a matching of the test template is done the master for recognition. This is also known as one-to-one matching [11].

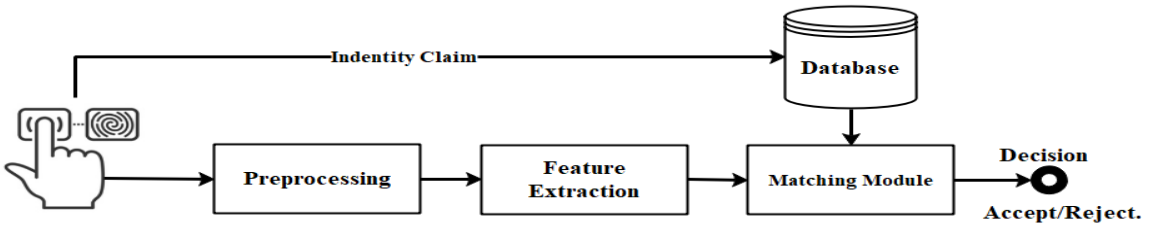

Fig.1.4 Verification ModeBlock diagram

The Table1.1 shown below summarizes the views of biometric experts on differentbiometric characteristics in terms of the factors

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand Geometry	M	M	M	H	M	M	M
Palmprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1.1 Different Biometric Characteristics Comparison

H- High,M=Mediumand L=Low ; Source:Palmprint Authentication byZhang(2004)

Performance Metrics

The measurement of how a biometric system performs is done by applying some parameters or metrics as illustrated below [1], [2], [3], [5]:

- **False Accept Rate or False Match Rate (FAR or FMR)** – It is concerned with the possibility that the system will make an inaccurate match between the input pattern and a database template that does not exist. It calculates the percentage of incorrectly accepted invalid inputs.

$$\text{FAR} = \frac{\text{Number of false acceptances}}{\text{Total no.of impostor attempts}}$$

- **False Reject Rate or False Non-Match Rate (FRR or FNMR)** – It is concerned with the possibility that the system will fail to identify matching that separates an input pattern and database template. It calculates the percentage of valid inputs that are dismissed inaccurately [12].

$$\text{FRR} = \frac{\text{Number of false rejections}}{\text{Total no.of genuine attempts}}$$

- **Receiver Operating Characteristic or Relative Operating Characteristic (ROC)** The ROC plot depicts the transaction between FAR and FRR in a visual manner. Usually, on the basis of a threshold, decision is made by a matching algorithm, thereby specifying that extent of closeness of an input to the template for accepting the match. There will be fewer false non-matches but more false acceptances in case the threshold is lowered. As a result, a higher threshold lowers the FAR but raises the FRR [4].
- **Equal Error Rate or Crossover Error Rate (EER or CER)** – Acceptance and rejection errors are accepted at the same rate. The ROC curve can easily be used to calculate the EER value. The EER is a simple method of comparing the accuracy of devices with different ROC curves. The device with the lowest EER is, in general, the most precise. The point when FAR and FRR have the same value is obtained from the ROC diagram [8].

Sensor devices are connected to some other metrics like Failure to Enroll Rate (FTE), Failure to Capture Rate (FTC), and Template Capacity. Because FAR and FRR are interconnected, plotting them against each other, as illustrated in Fig.1.6, is more informative. Each dot on the graph reflects the performance of a hypothetical system at various sensitivity levels. You may use a graphic like this to compare these rates and figure out what the crossover error rate is (Equal Error Rate). The lower the CER (EER), the more precise the system is. Physiological biometric qualities are, on average, more accurate than behavioural biometric features [1],[6].

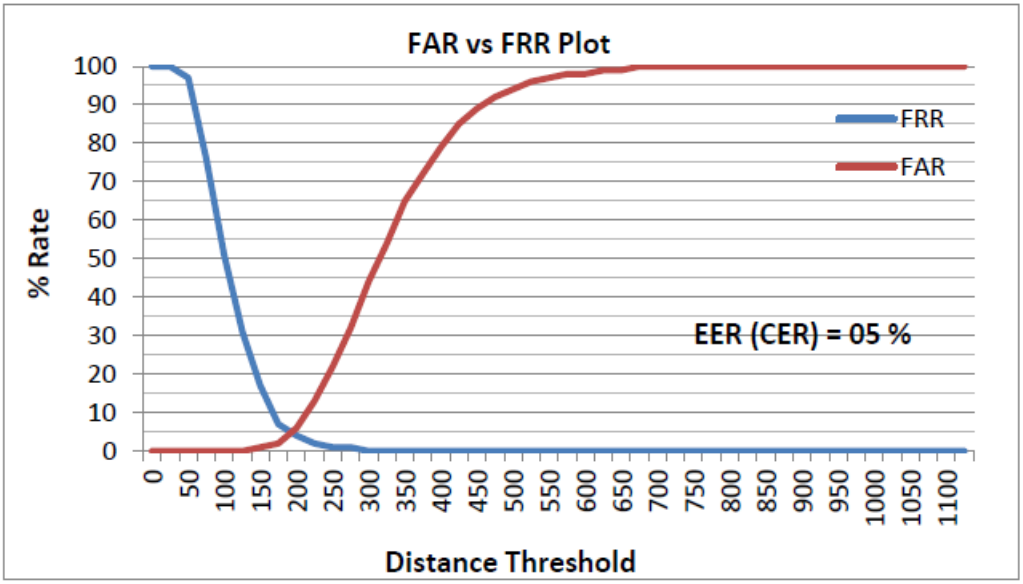

Fig. 1.5 A Typical FAR vs. FRR Plot Showing Crossover (ROC Curve)

Limitations of Biometric Systems

Although a biometric system provides many benefits over traditional methods they are not present without any limitations. Some of the issues thatlimit the performance of a biometric system are discussed here [26].

1. Noise in Sensed Data: The raw data acquired from theindividual will be corrupted by noise especially when the sensors or the datacapturing devices are defective in nature or if it is not properly handled(accumulation of dirt in the sensor, ageing) or if favorable environmentalconditions do not exist (poor illumination). A noisy data is exemplified by fingerprint images having scars

or cold-affected voice samples. In such situations a genuine person may be dismissed [24].

2. Intra-class variations: This kind of variation occurs when the individual providing the biometric trait fail to interact with the sensor in a proper way (improper placement of the hand on the scanner) or changes that occur in case of biometric traits over some time (damage caused in the fingerprint) Such implications can be avoided by storing multiple templates per individual and updating these templates over time. Template update may be necessary in case of face, hand geometry, voice, signature, or gait which is expected to change over a period of time. This results in increasing the false rejection rate [25].

3. Inter-class similarities: This type of situation arises when an overlap of the feature sets occurs between multiple classes or individuals, especially in case of a huge list of enrolled users in a biometric. This places a limit on the number of maximum users to be enrolled in a system. Thus, it is clear that it is not possible to increase the number of enrolled users by using a specific algorithm or a fixed feature set. Inter-class similarities result in increase in false acceptance rate [6].

4. Non-universality: Under certain situations the biometric system fails to generate useful data out of a small user population that is enrolled. For example, palm print recognition system may not be able to extract the line features due to the poor quality of images taken using a camera. This increases the failure to enroll rate [8].

5. Interoperability issues: Certain biometric systems fail to provide authentication of an authorized person when the characteristic isgenerated using different sensors. For example, in face recognition system itmay fail to provide matching when different cameras are used duringenrollment and identification stages [12].

6. Spoof Attacks: The biometric data may be manipulated to avoid recognition by the system or duplicated to create a fake identity. This ismainly possible when behavioral traits like voice or signature is used. It isalso possible to

duplicate physical traits like fingerprints or iris. This leads to underrating the capability of biometrics. Several mechanisms may be adopted toavoid spoof attacks [16].

Challenges inBiometric Systems

Biometric systems for personal identification have been used in lotof applications, while seeking to improve the performance of such systems. A biometric system must accurately identify a genuine user and reject an impostor. From the above discussions, it is seen how noisy data, intra and inter class variations, non-universality, user acceptance, improper user interaction and spoof attacks affect how the biometric system performs. These factors limit the accuracy or the recognition rate in biometric systems. Here, challenges imposed by biometric systems include:

Limitation of available information: The amount of informationavailable in a single trait may not be sufficient to accurately discriminatebetween individuals in the increased population. For example, the informationavailable in hand geometry like length, breadth and area could be used toidentify fewer individuals, but at the same time in biometric systems based onfingerprints or palmprint, more information like texture, minutiae points etc.,can be used to include a greater number of enrolled identities [21].

Limitations posed by feature extraction algorithms: The featureextraction algorithms must be capable of extracting all invariant anddiscriminative information from the biometric trait used. A simple algorithmwill fail to capture the rich information available in the biometric trait. Thefeature vector may contain redundant information while missing the salientfeatures. For example, a simple filter used to extract the principal lines mayhave poor performance as some individuals have a common pattern. Thiscauses an increase in the error rates (FAR and FRR) of the personalidentification system.

Limitations by the matcher and fusion method: The matchermust be capable of discriminating the feature vector generated by differentsamples of an individual. A classifier if not properly trained will fail toidentify the

individual and also the fusion technique used must effectivelyintegrate the information from different traits of an individual. These factors could limit the capacity at which biometric systems maintain recognition rate.

Many businesses are looking for precise, safe, and dependable methods to preserve access rights to their present services or operations. One solution to these issues is biometrics. Biometrics comprises methods for analysing physical and behavioural identities to extract unique qualities for identification or monitoring reasons, particularly in information technology. This technique may utilise a variety of bodily traits such as faces, eyes, fingers, hands, veins, ears, and teeth. As part of the broader biometrics research, traits such as gaits and speech patterns are also being examined and evaluated [13].

In Biometrics, finger print recognition (FR) can be expertly applied to identify individuals by comparing fingerprint features with pre-determined templates having good familiarity among users. Notwithstanding, FR-based identification or authentication suffers from three main advantages:

Despite this, identification or authentication through FR still has three main advantages:

- Low cost of deployment (cost effective)
- Simple to implement and use.
- User must be physically available at the point of identification for verification.

Why use Fingerprints?

Fingerprints have shown to be the simplest and fastest way for biometric identification at this stage of development. They are safe for using, distinct to each individual, and do not alter over time. Apart from that, using a fingerprint recognition system is very inexpensive, simple to comprehend and use, and precise enough to meet the needs. Both forensic and civilian applications have made extensive use of recognition techniques based on fingerprints. Fingerprint-enabled biometrics is the most developed approach and has the

biggest chunk of market share when compared to other existing systems that attempt feature matching using biometrics. Because these systems have been fine-tuned through time, they are not only faster than previous ways, but they also waste less energy [17].

Problem Statement

The majority of faculty members utilize manually-maintained documents for attendance to keep attendance records, according to the survey and study of the available monitoring systems.

Problems that have been discovered in using paper-based registers are:

- Impersonation is aproblem found in the old system. Some students sign/respond in somecases, for students who are absent, and this does not make the attendance credible.
- Sometimes, the attendance sheet either gets lost or misplaced by some of the students.
- It takes a lot of time to check attendance of all students available for a lecture. Students have to wait for long; before lectures begins. Lecturers have to take their time to make sure all students have checked in correctly before the lecture begins.
- Also, the tabulation of collected data of student attendance, is quite hectic and tedious.
- Designing and deploying a fingerprint-based student attendance verification system that can track attendance in classrooms, laboratories, seminars, and other areas of the institute.

  The topic for research is Biometric Authentication Systems, it consists of fingerprint biometric systems.

Motivation

The practice of keeping track of student attendance has been around for a long time. With the emergence of new technologies, the method for maintaining

these data has become more efficient over time. The goal of this project was to create a better attendance management system for students so that records could be kept with convenience, openness, and accuracy. The accuracy of attendance records will be enhanced since it will remove the inconveniences of roll calling, which involves a person physically observing and verifying attendance. This will save time for both students and instructors. There are a variety of image processing approaches for recognizing fingerprint patterns. They are quite developed in terms of technology currently, and hence highly accurate. As a result, a rapid and precise attendance system is created, devoid of the risk of impersonation.

Aims and Objectives.

The goal of this project is to develop a new way to tracking student attendance and build an application for it by combining fingerprint comparison with an innovative hybrid strategy to increase reaction speed and accuracy in identifying the best fit in a large fingerprint databases.

The primary objectives include:

- To create an electronic system for management of student attendance.
- To design a system that measures how students perform.
- To build an effective and efficient method for roll call among students.
- To enhance attendance system and make it easy and fast.

The Practical Significance

The Fingerprint Attendance specifications are described in this project thesis. In this software, we have attempted to build a graphical interface for allowing system users to perform various activities like saving, preserving, updating, and retrieving Student data. The goal is to assist developers in choosing a design that can support application at full scale level. Some personal information of a student as well as details about classes, lectures, and courses can be recorded in the system that can further be updated and retrieved as and

when require, thus saving time and enhancing accuracy. Students can enter their fingerprints into the device to kick start the entire operation.

- Students enter their fingerprints into the device.
- Every fingerprint has a special id for every record. This id takes the other step, which is matching with database.
- The system checks on the fingerprint and sends to the circuit and the student database.
- In this database file, the system checks this print for the identification.

Justification

This problem is a real-time issue that is affecting the school currently, records of student's attendance is kept in a sheet of paper or notebook. This is dangerous because the paper or the notebook can easily get lost because it is not protected. Undertaking research and gathering information to build this Automated Fingerprint Attendance System (AFAS) will also go a long way to help the organization grow, because this system can be used for so many years. It is open for upgrades of its features.

Structure of the Thesis

The thesis consists of seven chapters, Introduction, Literature Survey,Software Requirements,System Analysis and Design, Implementation Testing, Results, and references

- In the first Chapter, the problem statement is given in details, as also a comparative analysis of the existing applications. Also, a description of biometrics use is given.
- In Chapter two, a detailed Literature Survey is given and also the gaps identified in the previous works.
- Chapter three describes functional and non-functional requirements.

- In Chapter four, there is a description about System Analysis and Design i.e. use case diagram, database scheme and the design of the application’s interfaces.
- In Chapterfive, we show several fragments of source code for implementing the basic functionality of the system.
- Chapter six is devoted to the testing of the application. It contains the results of functional, and usability testing.
- Chapter seven gives some comparative results for this project.

1.1. REVIEW OF ANALOUGES

S.No	SegmentationAlgorithm	MeasuringParameters	ComputationalComplexities	Limitations	Advantages	Applications
[1]	Adaptive TotalVariationModel.	λ=FidelityWeightCoefficient andfeatures such asmean, varianceandcoherence	In selectingdifferent valuesofλindifferentfingerprintimageregion.	Accurateperformanceis notachieved forworst (authorsays ugly)latentfingerprints	Provides verysatisfactorysegmentationresults.	(i) Fingerprint Segmentation. **(ii)** ImageDecomposition
[2]	Directional TotalVariationModel.	$\vec{a}(x)$ spatially varyingorientationvectoranduse variancefeature.	Inkeeping $\vec{a}(x)$ spatially varyingand well alignedwith localfingerprint ridgeorientation	_	Goodperformanceas comparedto [1]'smethod.	Decompositionof images withorientedtextures.

[3]	Method based oncombination of ridgeorientation andfrequencyfeatures.	Ridge frequencyor Ridge densityandmeanvalue	Orientation andfrequencyfeatures aredetermined foreach printseparately andthen theirintersectionistaken.	Need a robustconfidencemeasure forsegmentation output	Satisfactoryresultsasfaras visualinspection isconcerned.	Detection andSegmentation ofLatentFingerprint
[4]	Combined Method.Orientation fieldinformationcombined withstatisticalcharacteristics ofgray.	Meangrayvalueandvariance.	-	Not so goodforimagethatis too wet ortoodry.	**(i)**Improvesaccuracy **(ii)**Savesprocessingtime	FingerprintImageSegmentation
[5]	Ridge TemplateCorrelation.	Image mean andvariance	Lengthyalgorithm needs to be followedin	Whenfingerprintsilage andmissedminut	Reduces theaveragedetectedfingerprintareafr	FingerprintSegmentation

			order toachieveeffectivesegmentation	iae ishigh, thesegmentation incorrectlylabels thebackground asforeground	om60.7% of thetotalimageto33.6%.	

1.2. Analysis of Basic Technological Solutions

Before comparing the applicability of FR with that of other biometric approaches, research was conducted to establish the needs of any biometric system, and especially of a FR system for usage inside the University context. A choice of FR device had to be considered, and consideration given to the role of identifying or verifying credentials for deciding the best possible technique for application. It also studied the various methods in analysis of the used image and an approach was chosen which could be tested in the context of this project with currently available equipment. A measure of performance had to be discovered and decided upon, before benefits and concerns of FR systems could be considered.

1.2.1. Fingerprint

Fingerprint, biometric traits with textural richness are chosen, while its extraction is done to generate a feature vector. We need to capture the data first and then preprocess the data. These stages are common in almost every biometric trait and in case of fingerprint, palmprint and finger knuckle print they tend to be similar [21].

1.2.2Types of Fingerprint Patterns

The patterns on fingerprint have three broad classifications:

1.2.2.1. Arches

Fingerprint patterns with ridges that go straight from one side to the other. In general, Without a delta point inside an arch pattern, the re-curving ridge does not come in between the core and the delta point. Also, arches are classified under four categories [26]:

- Plain Arche
- Radial Arche
- Tented Arche
- Ulnar Arche

1.2.2.2. Loops

Loops are a type of loop that is used to allow Ridges to flow inwards and return in the direction of the origin in these patterns. Ridges enter the impression from each side, recurve, and end in the direction of the ridges' entry [5]. There are four different kinds of loops:

- Plain Loop.
- Lateral Pocket Loop.
- Central Packet Loop.
- Twinned Loop

1.2.2.3. Whorls

Ridges occur in a circular pattern around a central point in whorls patterns. Whorl patterns are any patterns with two or more delta points [7]. There are four different whorl designs to choose from:

- Plain Whorl.
- Central Pocket Loop Whorl.
- Double Pocket Loop Whorl.
- Accidental Whorl.

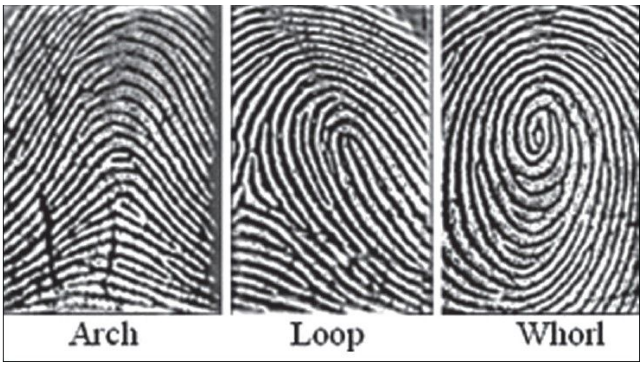

Fig.1.6Types of Fingerprint Patterns

1.2.3. Fingerprint Recognition Systems

In order to analyze a fingerprint for granular detection or matching, Automatic Fingerprint Recognition Systems need to have a clear, noise-free finger print[29]. This is done by preprocessing the finger print image [8].

1.2.4. Fingerprint Preprocessing

To reduce the effects of noise, dryness, wetness of the finger, and differences in applied pressure when scanning the fingerprint, the fingerprint must be pre-processed. Pre-processing involves a number of steps [18]. The following are the many pre-processing stages.

1. Smoothening Filter
2. Normalizing Intensity
3. Estimating orientation Field
4. Segmenting Finger print
5. Ridge removal
6. Thinning

Depending on the application and feature extraction methodthese steps may vary. Wu and Govindarajan [32] have proposed anadaptive image filtering method for singularity (minutiae)preservation. They first estimated image quality by Fourierspectrum of the image, in this paper, fingerprint imagespreprocessing is performed based on the discriminant frequencyand statistical texture features. Later Gaussian filtering is used toenhance the ridge structure and gradient field coherence strength isused for segmentationof region of interest (ROI).

According to Madhuri and Richa Mishr (2012), who did a study on "Fingerprint Recognition using Robust Local Features", a host of human recognition approaches that are based on fingerprints have been developed in recent times. For fingerprint representation and matching, a major proportion of such approaches employ minutiae points. When a person's enrolled picture is compared with a rotated test picture, these procedures fail, and they also fail when incomplete fingerprint pictures are matched. This work provides a fingerprint matching and representation methodology based on strong local features [23].

In the paper entitled, “Fingerprint Recognition Using Minutiae Extractor”, Manisha Redhu and Dr.Balkishan identified the utility of biometrics in authenticating the fingerprints of individuals on the basis of unique features that are permanent as well. The automated ways of validating a match between two human fingerprints is known as fingerprint recognition. Because of its practicality, distinctiveness, persistence, accuracy, dependability, and acceptance, fingerprints have been widely employed in daily life for more than a century. The authors have used the Minutia Score matching approach to project Fingerprint Recognition in their research work.

In the paper entitled, “A Review on Fingerprint-Based Identification System”, Ritu and Matish Garghave defined biometric fingerprints as the personal identification tools due to their peculiarity, uniqueness, and dependability. Valleys and ridges on human fingertips make up a fingerprint impression. Fingerprint authentication is arguably the most advanced biometric approach available. Authentication of fingerprints has been rigorously confirmed using a variety of applications. Either one or many methods from the known three methods i.e. minutiae-based, correlation-based, or hybrid are applied in most of the fingerprint-based human recognition systems. This paper covers a generic minutiae-based fingerprint identification system after providing an overview of several fingerprint recognition approaches [17].

In the paper entitled, “Fingerprint Identification System”, Priyanka Rani and Pinki Sharmahave highlighted the significance of Fingerprint authentication as the most suitable biometric technique, which has great implications in many applications. Obvious traits like a person's face or signature may evolve over time and can be forged or duplicated. A fingerprint, on the other hand, is unique to each person and remains unchanging throughout their lives. The many elements and procedures to be employed for the fingerprint-based identification system are defined in this study [14].

In the paper entitled, “Fingerprint Recognition: Minutiae Extraction and Matching Technique”, Gurpreet Singh and Vinod Kumarhave also highlighted the more recent advancements that have occurred in the field of fingerprint identification and authentication. It has in fact, soured many others to carry out further studies in this emerging area. Fingerprint identification is evolving into a new arena for user authentication. In big enterprises that use fingerprint identification systems, fingerprint categorization is very significant. Fingerprint identification is particularly useful in authenticating when two fingerprints do not match, and it also minimizes on the amount of time it takes to identify someone. This study provides a comprehensive analysis of available classification algorithms for fingerprint identification challenges. The numerous evaluation parameters utilized by AFIS classification techniques are explained in this work [18].

Anil Jain et al. developed a matching system for 1000dpi fingerprint matching that uses Level 3 features such as pores and ridge outlines. Wavelet transform and Gabor filters are used to automatically extract Level 3 features, which are then put to local matching by applying ICP method. Level 3 traits convey considerable discriminating information, according to their research on a medium-sized database [22].

Based on the response of eight oriented Gabor filters, Alonso, Fierrez, et al. suggested an improved methodology for segmenting fingerprints. This approach yields a larger foreground region and a much smaller background region, allowing for the recovery of blocks with minutiae and legitimate but poorly defined zones. A shortcoming of this method is that the thresholding is not automatic, and a manual threshold needs to be selected empirically. We have proposed automatic thresholding based on Gabor filters; the process is automated by generating a threshold by Otsu’s methodapplied on Gabor magnitude histogram. In Correlation-based fingerprint recognition system we need to determine a registration point as a reference; this is called as core point.

Core point detection is a non-trivial task. In our research we are discussing correlation-based fingerprint recognition; now we discuss some methods for core point detection [24].

Weiping Chen and Yongsheng Gao proposed a phase correlation-based minutiae-based fingerprint matching technique. They proposed a Minutiae direction Map as a novel approach. They began by converting minutiae sets into two-dimensional picture spaces. Furthermore, using phase correlation between two MDMs, the transformation parameters are generated to make alignment between two fingerprints, which is defined by the distance separating two minutiae sets [19].

1.2.5. Importance of Biometric Systems

Uniqueness: Individual biometrics systems have been developed based on their distinct properties. It's almost impossible for two persons to have the same biometric data.

Cannot be Shared: A biometric property is exceedingly hard to emulate or share since it is nothing but an intrinsic trait that a person possesses.

Cannot be Copied: The Biometric features are almost unviable to fabricate or spoof, especially with emerging technologies that prove that a detected biometric image actually belongs to a living person.

Cannot be Lost: Except, in case of only a major accident can cause an individual's biometric property to be lost.

1.2.6. Limitation of Previous Work

1. **Not User Friendly:** The current system is inconvenient for users since data retrieval is sluggish and data is not well-maintained.
2. **Difficulty in Report Generating:** To create the reports, we may need further computations.
3. **Manual Control:** Since all of the calculations for the report were done by hand, there is a higher risk of mistakes.

4. **Lots of Paperwork:** The current method necessitates a great deal of documentation. Because all of the documents are required to make the reports, even the loss of a single register/record created a problematic scenario.
5. **Time Consuming:** Because all of the work is done by hand, we are unable to produce reports in the midst of the semester or as needed due to the time commitment.

1.2.7. Strength of Current Work

- It was able to be keeping some records of students which could be used to assess the students' attendance at the end of the semester.
- It was very helpful when the class size because with a large number of class, calling the names of every student would take time, which is meant for lectures.

1.3. Conclusions

In this chapter an introduction to Biometrics is discussed, while identifying some research gaps found in the previous models.This chapter also gives some basic technologies used to develop this project. A Problem statement has been presented with some of the limitations of previous works is also been discussed in this chapter.

2. DEFINITION OF REQUIREMENTS

2.1. Functional Requirements

A formal declaration of an application's functional needs is the Functional Requirements Document (FRD), which is similar to the goal of the agreement. The developers have agreed to provide the alternatives that have been requested. If the product meets the FRD's specified criteria, the client agrees to consider it acceptable. The function of software or a component is defined by a functional requirement. A set of inputs, behaviour, and outputs is referred to as a function. Calculations, technical details, data manipulation and processing and other particular tasks that specify what the system should do are examples of functional requirements. The use case reflects behavioural requirements that characterize all scenarios where the system employs functional needs. The system's design includes a thorough strategy for implementing the functional requirements [29],[30].

After obtaining and validating a set of functional requirements, the requirements analyst may produce use cases. The user / stakeholder request function user guide business rule is the hierarchy of functional needs. Through one or more functional requirements, in every examined use case, we notice behavioural occurrences. Nonetheless, the analyst frequently begins by creating a collection of use cases from which the functional requirements that must be executed to enable the user to accomplish each use case may be derived [31],[32].

The functional requirements document has the following characteristics:

Characteristics ofFunctional Requirements Document
It demonstrates that the application provides value to the State in terms of the business objectives and business processes in the 5-year plan
It contains a complete set of requirements for the application. It leaves no room for anyone to assume anything not stated in the Functional Requirements Document.

It is solution independent. Functional Requirements Document is a statement of what The application is about what to do, not how to accomplish it. The developers are not bound by the design in Functional Requirements Document. As a result, any mention of a specific technology in a Functional Requirements Document is completely improper.

2.1.2.Functional Requirements of Biometric System

R.1: Login Management

Login Management
Description: To access the database and verify the student's attendance, the user must first provide their login id and password. Only the head of department and other staff members have access to the database since it is accessed at the management level.
Input: Login_id and Password. **Output:**Main form opens.

R.1.1 Failed to Login

Failed to Login
Description: If a user's attempt to access the database fails, it is assumed that the user has entered incorrect information, such as a faulty password or id, or both. In such a scenario, the database will notify the user.
Input: EnterLogin_id and password. **Output:** Invalid information. Please try again.

R.2. Main Form

R.2.1:Manage Personal Details

Manage Personal Details
Description: After filling student's information, such as name, phone number, address, age, and gender, a roll number is assigned to the student, which serves as a unique student id . Finally, the student is assigned to a department in which he or she wishes to enrol.
Input: Student_id **Output:** **S**tudent details stored successfully

R.2.1.1: Enrollment Scan

Enrollment Scan
Description: After scanning the fingerprints of the user, it is linked to the user's identification in the system. This is usually a supervised procedure to prevent the development and spread of fraudulent identities. Enrolment at colleges and universities is done at the moment a student applies for admission to the institution and only has to be done once.
Input: Fingerprint scan and image of the Student. **Output:** Successfully saved the biometric data of the Student.

R.2.1.2: Update Student Details

Update Student Details
Description: In case a student wishes to update his or her personal information, he or she may do so since the database automatically enables it. Thus, nothing is permanent or static, except a student's fingerprint scan, which cannot be modified once it is placed in the database.
Input: Student_id. **Output:** Updated details saved successfully in the database.

R.2.1.2.1: Reset Student Details

Enrollment Scan
Description: This option can be utilized if all of the details need to be changed; it will simply clear all of the student's personal information. You will be given the opportunity to enter the information again if you do so.
Input: Student_id. **Output:**Student information cleared from the database.

R.2.1.3: Delete Student Information

Delete Student Information
Description: Delete record of student who has left the institute or who is passed out.
Input: Student_id. **Output:**Student information delete.

R.3: Attendance Report

Description: It records every student's attendance in every subject or course offered by the department in which he or she has chosen to enrol.

R.3.1: Attendance Report of Particular Student

Attendance Report of Particular Student
Description: It indicates a student's attendance in every subject or course offered in the department he or she has chosen to enrol.
Input: Enter Student_id. **Output:** Attendance of the student is displayed for every course.

R.3.1.1: Attendance Report of All Students of Class

Attendance Report of All Students of Class
Description: It indicates all students' attendance in every subject or course offered in the department in which they have chosen to enrol.
Input: Class_id.

Output: Complete attendance report of all students in a class

R.3.2 Attendance Report of a Course

Attendance Report of a Course
Description: A report displayed that details the course's status, including those students who are eligible for tests and those who are not.
Input: Course_Code. **Output:** Displays a report that details the course's status, including eligible students as well as those who are not eligible for exams.

R.4: Display Report for Eligibility Criteria

Attendance Report of Particular Student
Description: As each course's report is prepared, the total number of students for each attendance is provided, along with their associated status. If their attendance falls below a certain threshold, such as 60% or any other criteria you choose, a report will be generated indicating whether or not they are qualified to take the test.
Input: Enter Status of eligibility. **Output:**Corresponding to the eligibility, report is displayed.

2.1.2System Design

2.1.2.1. Use Case Diagrams

The utilisation case graphs have the task to assess the framework's requirements from an abnormal condition perspective. As a result, when we study these requirements, we can determine the features in these use scenarios. As a result, we can say that usage case outlines are nothing more than a collection of framework features expressed in a logical order. The performing artists, who are anything that communicates with the framework, are the second important aspect of a usage scenario. Humans, applications, computers,

and artificial intelligence may all be used as actors. So, here we are, designing our system's use case diagrams. We are attempting to assess the many user interactions that are conceivable with our system, as well as how each of these use cases is significant to our system's operation [20].

a) Use Case Diagrams for Student

The easiest of the use cases found are of the student. The student will be handed over the attendance module in order to only insert their respective biometrics into the sensor. This can be observed in the diagram above. Once the finger is inserted, the student has to wait for the system to confirm validity. Once the identification is matched, the student has to just pass along the device to other students to perform the same operations. At the end of the session, the database shall be updated according to the user entry. The users can be either the student or the faculty member. In order to accomplish the student entry, the faculty member has to perform some operations. These operations can be summarized by the use case diagram below [30],[31].

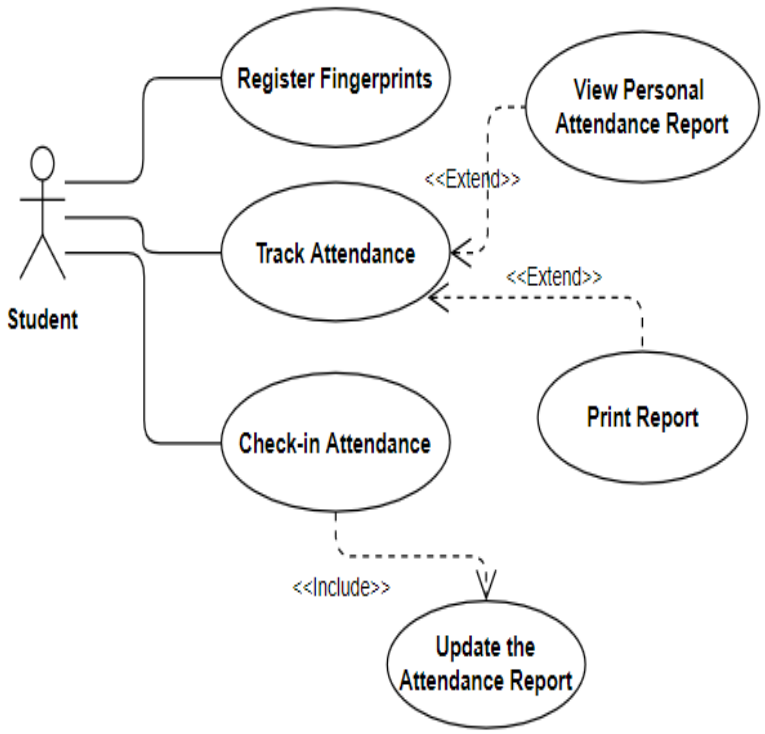

Fig.2.1. Use Case Diagrams for Student

A. Use Case Diagrams for Register Fingerprint
Primary Actor: Student
Stakeholders and Interests: Student – seeks to place his/her fingerprint. Admin – seeks to save the student fingerprint into system.
Brief Description: Here, how a student registers own fingerprint into the system with assistance from admin is described.
Trigger: After making requests for registration of his fingerprint, a student enters into the system. **Type:** External
Relationships: Association: Student. Include: Extend: Generalization:
Normal Flow of Events: 1. Entry by student into the system following his/her requests for registration of fingerprint 2. The request for login is received by admin. 3. The system navigates to login page. 4. The ID & password is entered in the system by admin. 5. The admin validates admin ID & password in system from database. 6. The admin searches student information 7. Student registers fingerprint 8. The admin registers student data in the system. 9. Student registration information is saved by system.

10. The result of the transaction is provided by admin to student.

11. The system ends.

B. Use Case Diagrams for Track Attendance

Primary Actor: Student

Stakeholders and Interests:

Student – Seeks to monitor his/her own attendance record.

Brief Description:

In this use case, student monitors his/her personal attendance record by verifying report photo copy.

Trigger: The student wants to monitor own attendance record.

Type: External

Relationships:

Association: Student.

Include:

Extend: View Personal Attendance Report, Print Report.

Generalization:

Normal Flow of Events:

1. The student seeks to monitor own attendance record.
2. Login request by student.
3. The system navigates to login page.
4. The ID & password is entered into system by student.
5. Validation of student's ID & password by the system after checking database.
6. Request from student for permission to check own attendance report.
7. The personal attendance report is displayed by the system.
8. The report analyzed by student.
9. Seeks print out of the report.
10. The printed report comes out

11. The system ends. 12. Else 13. The system ends.
C. Use Case Diagrams for Check-in Attendance
Primary Actor: Student
Stakeholders and Interests: Student – wants to check in his/her attendance status.
Brief Description: Description of handling of the process of attendance check-in by students in this use case.
Trigger: The student seeks to check own attendance status. **Type:** External
Relationships: Association: Student. Include: Update Database. Extend: Generalization:
Normal Flow of Events: 1. The student seeks to check own attendance status. 2. The student attends the class. 3. The attendance is verified by student after applying fingerprint. 4. Student fingerprint matches the system. 5. Checks if fingerprint is matched or not. 6. Updates the attendance status of student. 7. The email transaction result is shared by system to student.**(E1)** 8. The system ends. 9. Else 10. The system ends.

Alternative/Exceptional Flows:
E1: In case student fails to verify own attendance, no mail is sent to student by the system, thus ending the process.

B) Use Case Diagrams for Admin/Faculty

The Admin/Faculty authentication system is the primary authentication system in the model. The Admin/Faculty starts off by inputting the password required to open the functionality interface. This password is only known by the Admin/Faculty members. Once the entry is correct, the user interface (UI) displays the various operations supported and programmed into the Arduino. On fresh start, the Admin/Faculty must enrol all the students in class. This can be easily done using the enrol operation. But to do this, the Admin/Faculty must have access to the enrol authentication password. The other operations include matching ID's with existing ID's and deleting an ID, if required. To delete an ID, the deletion authentication must be done. Again, the Admin/Faculty member has access to this.

c) Arduino Use-Case

The basic operations of the Arduino are to connect and control the R305 fingerprint sensor. Using the NodeMCU component, the Arduino can transmit the data captured on the device to the respective database of the user. The module also has inbuilt LCD that is programmed to render the UI appropriately. The user can observe the LCD and respond through the keypad provided [23].

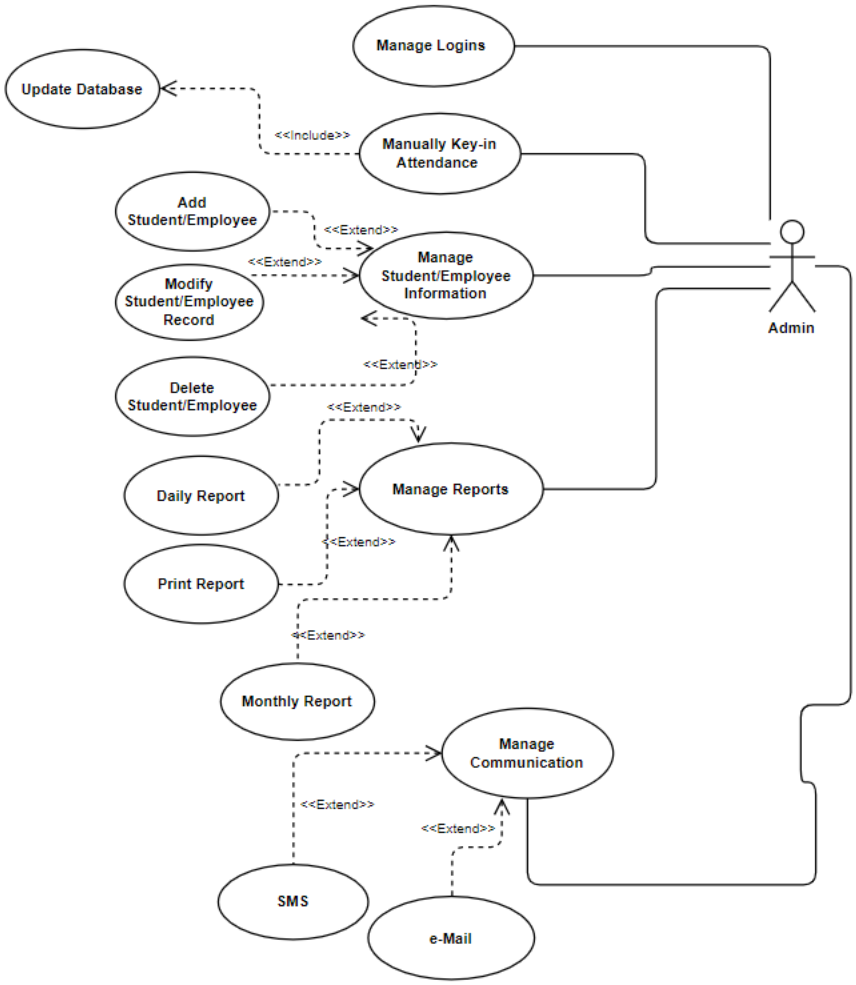

Fig.2.2. Use Case Diagrams for Admin/Faculty

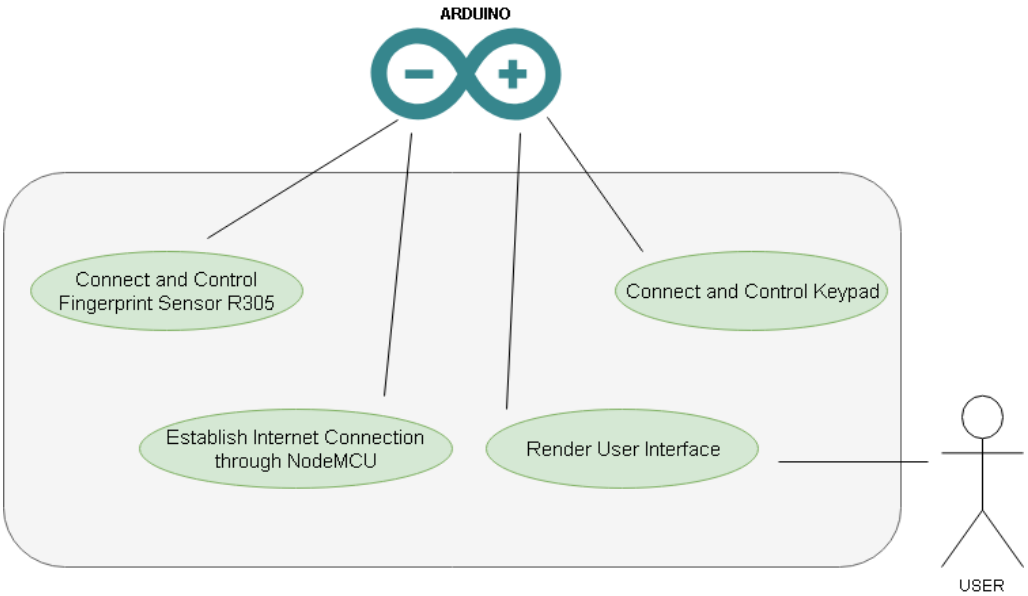

Fig.2.3. Arduino Use-Case

Use-Case Description(Admin)

D. Use Case Diagrams for Manage Student Information
Primary Actor: Admin
Stakeholders and Interests: Admin – seeks to manage the student information in system.
Brief Description: This use case deals with admin's handling of the process of student information management.
Trigger: The admin seeks to manage the student information in system. **Type:** External
Relationships: Association: Admin. Include: Extend: New Student Information is added, Edit Student Information, Delete Student Information. Generalization:
Normal Flow of Events: 1. The student information is managed by admin in system. 2. Log in request by admin. 3. Navigation of the system to login page. 4. ID & password entered in system by admin. 5. The admin ID & password system is validated from database. 6. The action selected by admin to be performed. 7. If the admin wants to add new student information 8. The S – 1: Add new student info performed. 9. If the admin wants to edit existing student information 10. The S – 2: Edit student info performed.

11. If the admin wants to delete existing student information 12. The S – 3: Delete student info performed. 13. The result displayed by system. 14. The system ends.
Sub Flows: S – 1: New student information added. 1. The required information entered into system by admin. 2. The record saved in the system by admin. S – 2: Edit student information. 1. Specific student information is searched and navigated by admin. 2. The student information is edited by admin. 3. The record saved in the system by admin. S – 3: Delete student information. 1. Specific student information is searched and navigated by admin. 2. The student information is edited by admin. 3. The record saved in the system by admin.
E. Use Case Diagrams for Manage Communication Methods
Primary Actor: Admin
Stakeholders and Interests: Admin – Seeks to manage the methods for contact/mail the student/parent.
Brief Description: Deals with admin's handling of the process of email or SMS to the student/parent.
Trigger: The admin seeks to manage the methods to contact/mail the student/parent. **Type:** External
Relationships: Association: Admin.

Include: Extend: Email, Short Message Service (SMS). Generalization:
Normal Flow of Events: 1. The admin seeks to manage the methods to contact/mail the student/parent. 2. Log in request by admin. 3. Navigation of system to login page. 4. The ID & password entered by admin into the system. 5. Validation of the admin ID & password from database. 6. The generation of email/SMS to parent/student by admin. 7. The forward methods selected by admin. 8. If email method selected. 9. E mail sent to student/parent through email service by system. 10.The system ends. 11. Else 12. SMS sent to student/parent by system through phone service. 13.The system end.
F. Use Case Diagrams for Manage Report
Primary Actor: Admin
Stakeholders and Interests: Admin – Seeks to manage and analyze report on student attendance record.
Brief Description: This use case deal with management of the process of report analysis and generation by admin.
Trigger: The admin seeks to manage and analyze report about the student attendance record. **Type:** External
Relationships:

Association: Admin. Include: Extend: Sort Report by Types, Print Report. Generalization:
Normal Flow of Events: 1. The admin wants to manage and analyze report about the student attendance record. 2. Log in request by admin. 3. Navigation of system to login page. 4. The ID & password entered into the system by admin. 5. Validation of admin ID & password by system from database. 6. The required information provided to the system by admin. 7. The attendance report of all students in a class created by admin. 8. The report result displayed by system. 9. The attendance record result analyzed by admin. 10. If admin choose to sort report. 11. Category-wise sorting of report by the system. 11. If admin chooses to print the report. 12. The report printed out by system. 13. The system ends.
F. Use Case Diagrams for Manually Key-in Attendance
Primary Actor: Admin/Faculty
Stakeholders and Interests: Admin/Faculty – seeks to do manual key-in of the student attendance.
Brief Description: Deals with manual key-in attempt by faculty to enter the student attendance into the system.

Trigger: The Admin/Faculty seeks to do manual key-in the student attendance. **Type:** External
Relationships: Association: Faculty. Include: Update Database. Extend: Generalization:
Normal Flow of Events: 1. Manual key-in of student attendance sought by the Faculty. 2. Request for manual key-in into student attendance by Faculty. 3. Navigation to identity verification page by system. 4. The Faculty password to verify its identity. 5. The Faculty password is validated by system from database. 6. Attendance of selected student is modified by Faculty. 7. The Faculty assigns the reason for modifying attendance. 8. The modified attendance record status is saved by faculty. 9. The system displays result. 10. The system ends.

2.1.3.Activity Diagram

Making cutting edge technology in the field industries, schools, and colleges to automate attendance at cost effective prices aimed at the betterment of the society. The proposed system can be used to keep track of the log time of students or workers to process attendance. Therefore, it can be used in schools, colleges, and industries where an attendance registry is to be maintained. The system provides high accuracy and is reliable since it cannot be manually manipulated. Thus, it is helping the society in general [32].

a) Enrolling a New Fingerprint

In order for our model to work, the system should allow for easy and convenient way of inserting finger scans, besides detailed user information. User enrollment through the fingerprint scanner is the manner in which we accomplish this. We explicitly type in the details of the user and link it to the enrolled scan. Once the user details is in our database with the respective fingerprint, attendance can be easily managed [30].

b) Scanning an Enrolled Fingerprint

After the user has enrolled himself, we can now start to log the attendance every time he/she scans their finger. The log will contain the details about the entry, such as, name, id and time of entry.

c) Storing Details

The details about the user will be stored onto our computer/server. The log entry will be made automatically once the user's fingerprint is verified. If the scan fails to identify the fingerprint, attendance will not be provided.

This log is used as the attendance managing software to extract, process and disseminate information regarding attendance statuses for a respective student.

d)Deleting Ids

Certain cases such as student transfer or quitting, the exiting ID is no longer needed. Therefore, we can free-up space by removing it. The following are some the activity diagrams [31].

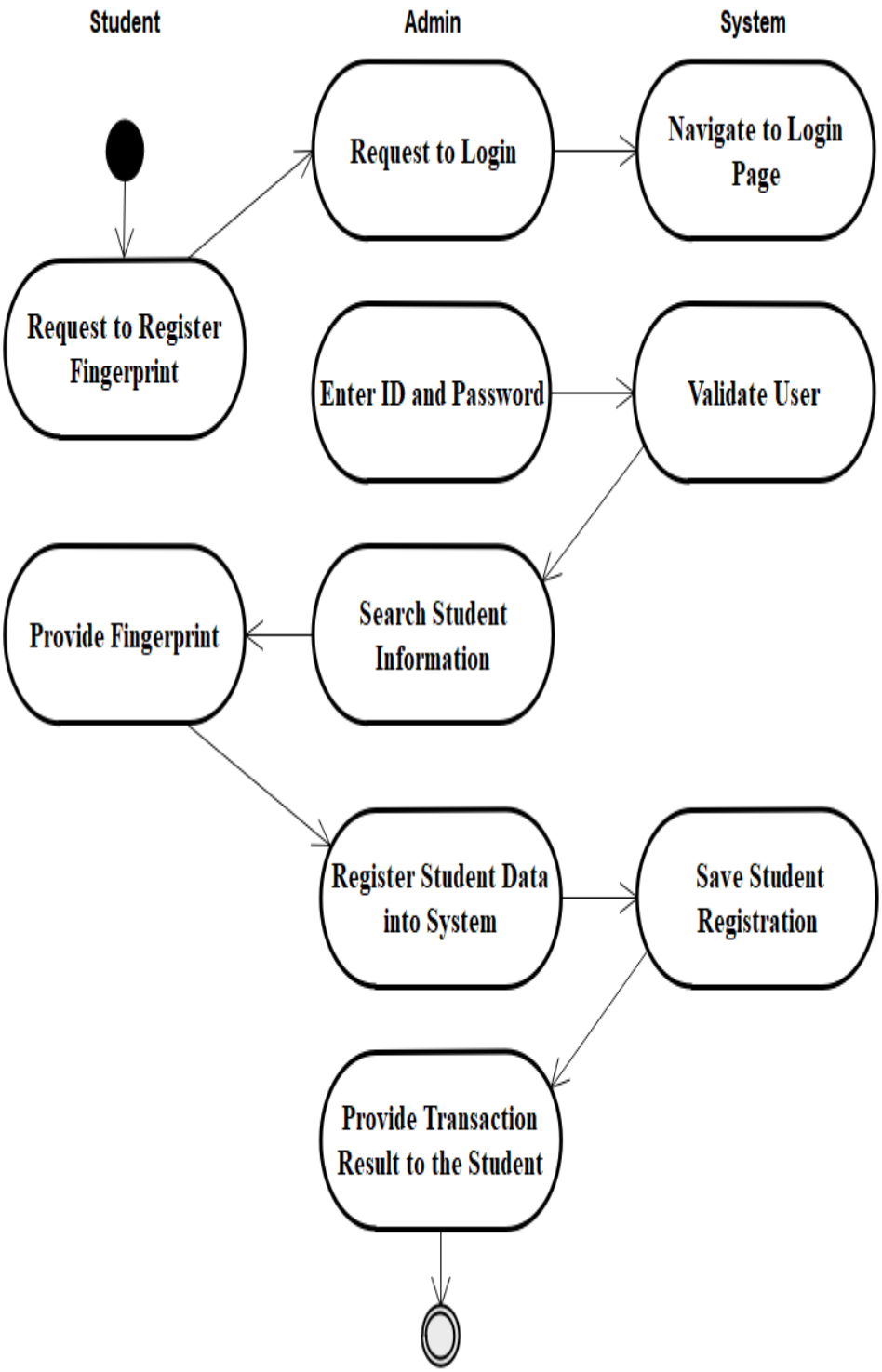

Fig.2.4. Activity Diagram for Register Fingerprint (Student)

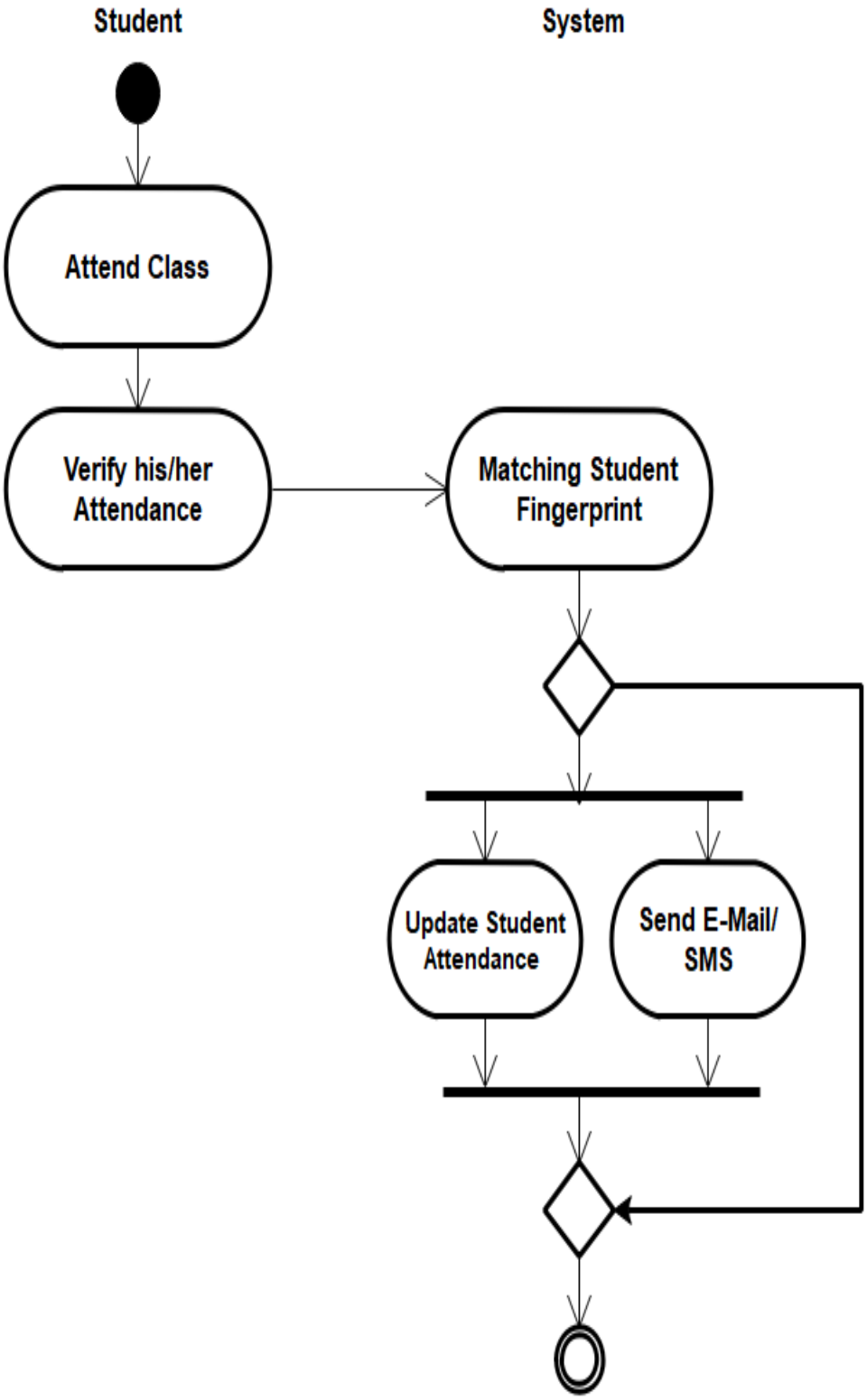

Fig.2.5. Activity Diagram for Check-in Attendance (Student)

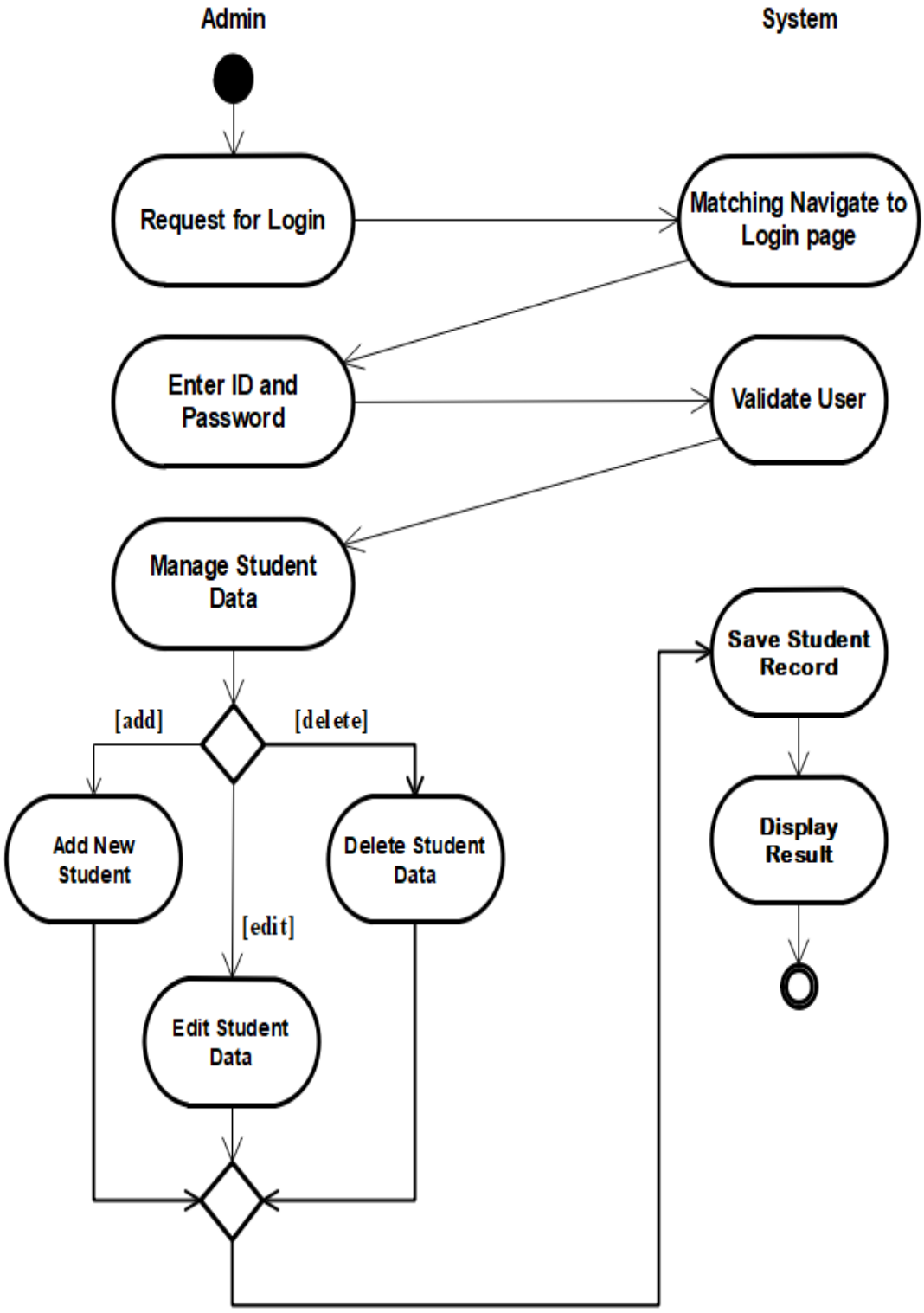

Fig.2.6. Activity Diagram for Manage Student Information (Admin)

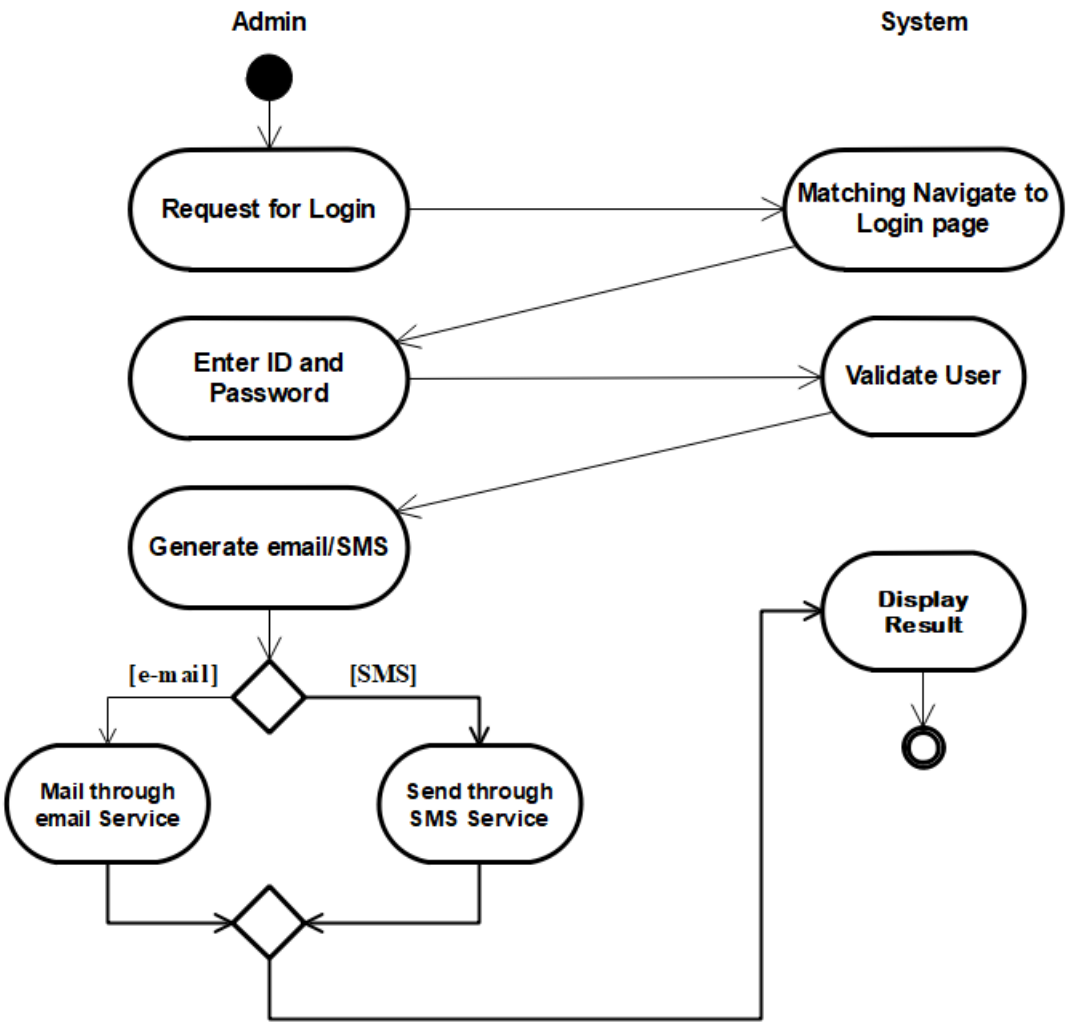

Fig.2.7.Activity Diagram for Manage Communication Methods (Admin)

2.1.4. Class Diagram

In the Unified Modeling Language, a class diagram depicts the connections and source code dependencies between classes (UML). A class specifies the methods and variables in an object, which is a specific entity in a programme or the unit of code that represents that entity in this context. The diagram depicts the various interconnections created to make this model function. The classes shown here range from the Arduino UNO base model controller to the smaller, more concise classes such as the fingerprint module (R305).

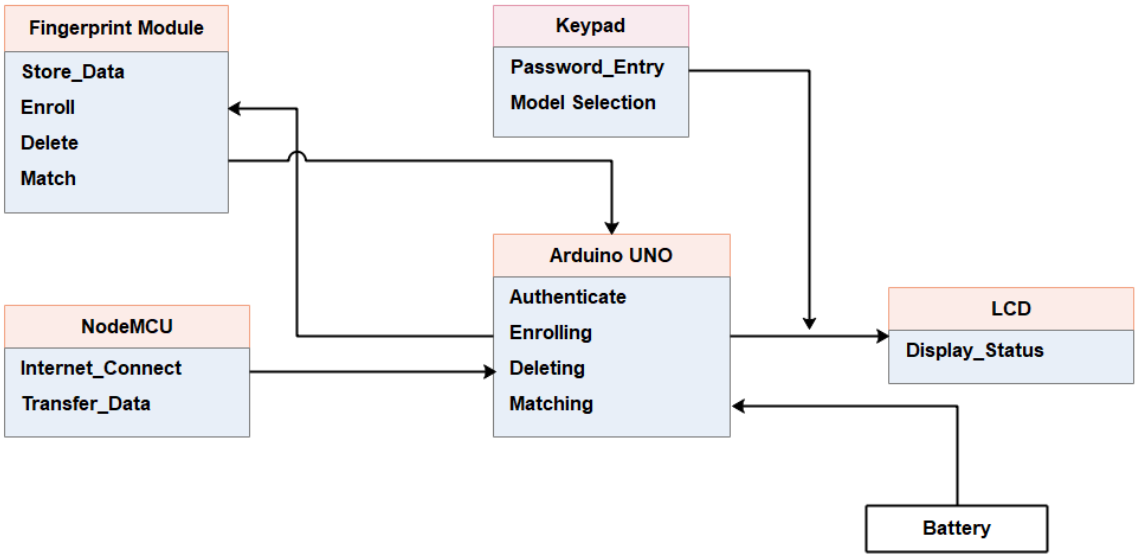

Fig.2.8.: Class Diagram(Level-0)

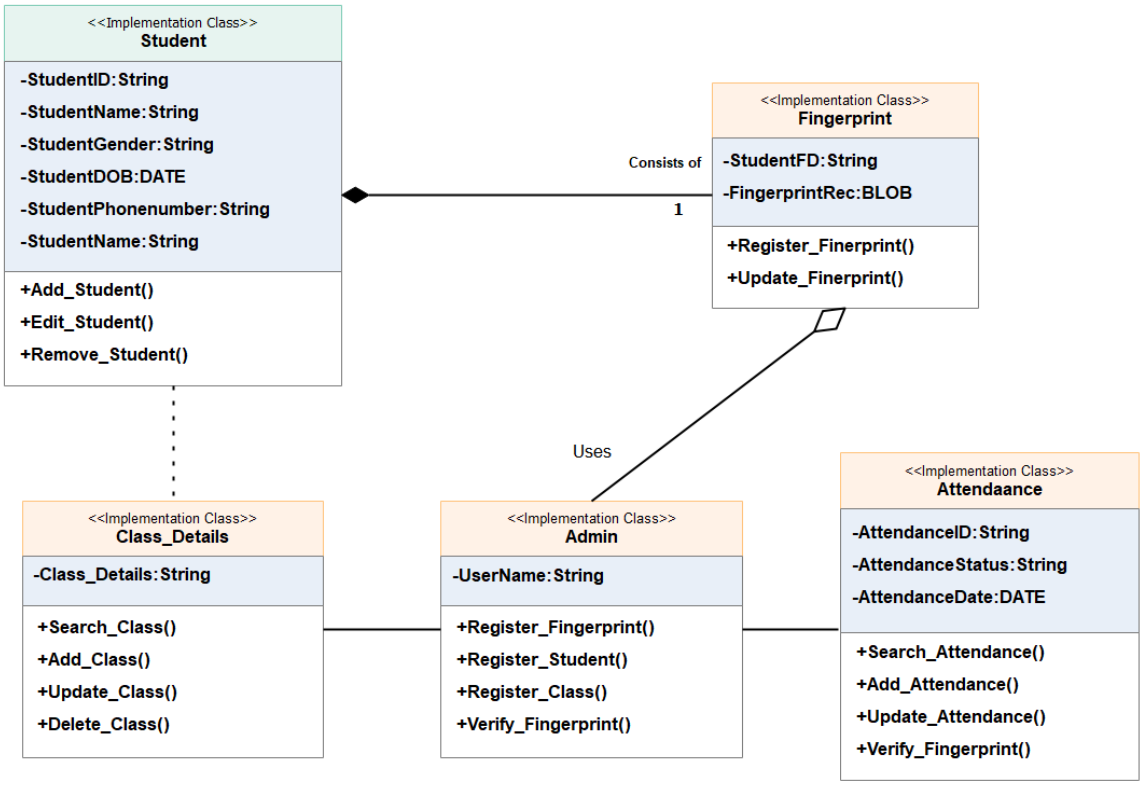

Fig.2.9.: Class Diagram(Level-1)

2.1.5.Entity-Relationship Modeling

To model the notions described, an E-R diagram needed the usage of a number of

notational rules. The E-R diagrams was developed using a smart drawing package (Concept Draw Office Package). This tool provided easy to use functions that facilitated consistency of the data workflow diagram. Object classes (called entities) are represented as rectangles, relationships are represented as diamonds and attributes of the entities are represented as ovals. The diagrammatic depiction of a database design is also known as an entity relationship diagram. The purpose of this entity relationship diagram is to show data for an organization or business sector in a thorough, graphical, and logical manner. They're frequent diagrams that explain how data in an information system is structured. They are very essential to create smooth modes of communication in project development. Some examples of tables are listed below [19].

2.9.1. Data Tables

A) Student_Table

S.No	Field_Name	Data_Type	Description
1	Student_ID	var_char	Unique Student ID
2	Student_Roll No	Number	Student Roll Number
3	Student_Name	var_char	Student Name
4	Student_Gender	var_char	Student Gender (Male/Female)
5	Student_DOB	DATE	Student Date of Birth
6	Student_Phone No	var_char	Student Mobile Number for sending SMS
7	Student_E-mail	var_char	Student E-mail Id for sending mails
8	Student_Class	var_char	Student Class

B) Admin_Table

S.No	Field_Name	Data_Type	Description
1	Admin_ID	var_char	Unique Admin ID
2	Password	var_char	Admin password
3	Admin_Phone No	var_char	Admin_Phone Number
4	Admin_E-mail	var_char	Admin_E-mail id

C) Fingerprint

S.No	Field_Name	Data_Type	Description
1	Student_FPID	var_char	Unique identifier for Fingerprint
2	Fingerprint_Rec	Nvarchar(MAX)	Templates of fingerprint
3	Student_ID	var_char	Identifier for Student

D) Attendance Entity

S.No	Field_Name	Data_Type	Description
1	Attendance_ID	var_char	Unique identifier for Attendance
2	Attendance_Status	var_char	Status of Attendance
3	Attendance_Date	DATE	Date of Attendance
4	Student_ID	var_char	Identifier for Student's class

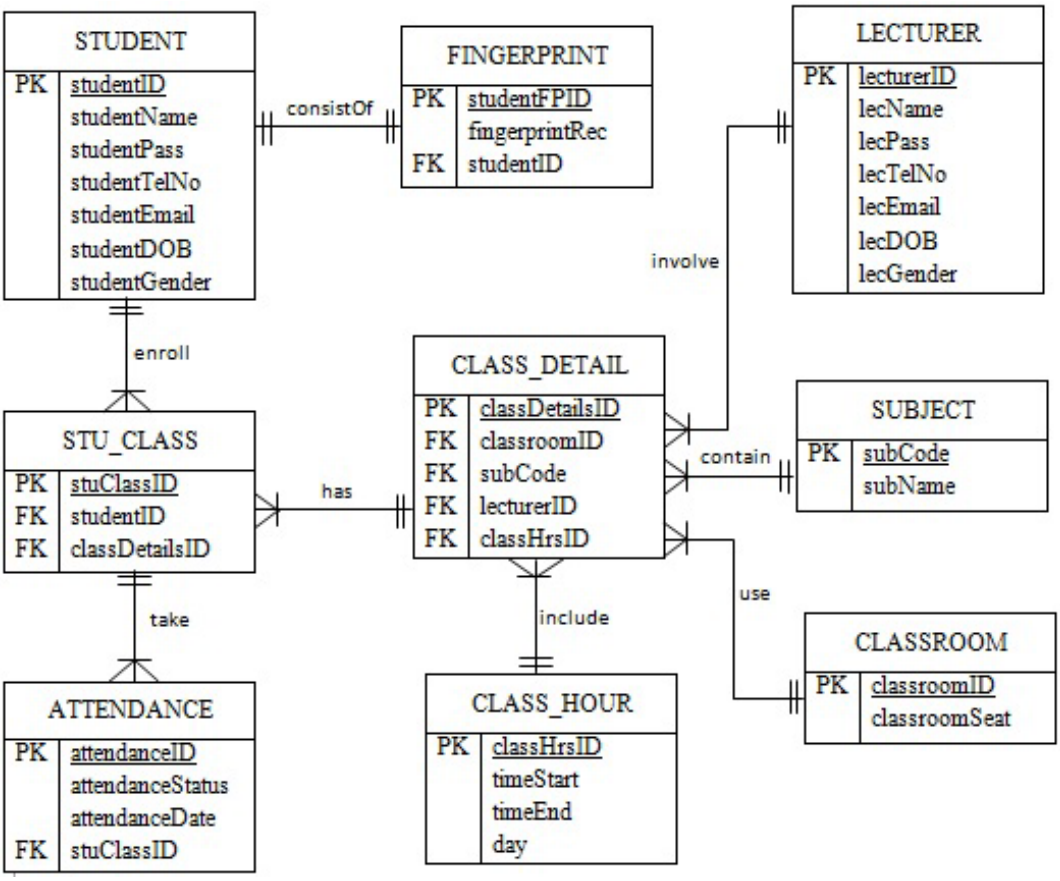

Fig.2.10. E-R diagram for Bio-Metric Attendance System

2.2 Non-Functional Requirements

2.2.1 Performance

It is possible to keep track of records and update them easily. The section below contains all of the requirements for the system's performance characteristics. There are two kinds of specifications [20].

A. Static Requirements

Such requirements have no capacity to put any constraints on the implementation aspects of the

System, which is detailed below:

1) Number of Terminals

The software makes use of an underlying database that will reside at the server, while the front end will be available online to the administrative and departmental computers as well as students and teachers.

2) Number of Users

The number of users may vary, as this software finds applications in almost all department of the organization.

B. Dynamic Requirements

Such aspects impose limitations on the system's ability to execute. They usually cover reaction time as well as the system as a whole. Because these parameters do not apply to the proposed programme, it will suffice provided the reaction time is high and transactions are completed accurately and fast.

2.2.2. Reliability

If the college LAN goes down, or if the server goes down due to hardware or software problems, the programme will be unable to connect to the centralized database.

2.2.3. Availability

Only approved college users will have access to the programme, such as professors who will be able to grade students' attendance, students who will be able to view their registered courses, and administrators who will be able to add and change student data.

2.2.4. Security

The primary security is addressed by the security protocols. Only the administrator and authorized users ought to have access to the software. Permissions such as establishing new accounts and generating passwords may only be assigned by the administrator. With a user name and password, only authorized users may access the system.

2.2.5. Maintainability

Maintenance on any system should be an easy task. Any difficulties that arise should not cause extensive harm, and any repairs should be simple to carry out. This model makes performing maintenance look quite easy. Modifications can be made to the Arduino code running at the heart of the system. Once updated, the hardware should reflect the changes made..

2.2.6. Portability

One of the most significant advantages of any system is its portability.Our model is small enough to be carried by the faculty from class to class. It is not hindered by the use of any wire as the model is capable of sending data through the wi-fi.

2.2.7. Correctness

It's critical to pay attention to the values presented in the system and the accuracy of the results shown. If the system does not produce the desired results, it fails the fundamental operability test. Here, we use digital systems to transmit data, therefore, the core of the system is strong. The chances of an external stimulation producing a failure are virtually next to nothing. External disturbances are unlikely to occur since the sensors are housed within the rigid box construction.

2.2.8. Usability

Usability focuses on ease of use. The system has been made in order to function on a number of times on a daily basis. Therefore, the UI is created in such a fashion that it runs on the intuition of the user (faculty/student).

2.2.9. Efficiency

The main quality aspect of a system is its efficiency. The objective of presenting a remedy to a problem becomes irrelevant if the system is inefficient. The model is built using the best resources, each more efficient that the other while running. They have been integrated in such a fashion that it allows overall efficiency to prevail.

2.2.2 Software Requirements

Server/Domain Name: Used to connect, verify, and store information regarding the user inputs. Initially, the dummy server uses the “thingspeak.com” server to store

information (ID). The final server is set to the domain of institution on which the whole process is set. In our case, we use the BIMS server to upload the data from the module.

Arduino IDE: The Arduino Software (IDE) includes a text editor for writing code, a message area, a text terminal, a toolbar with buttons for basic operations, and a series of menus. It links to Arduino and Genuino hardware in order to publish and interact with programmes. ESP8266, Adafruit Arduino Libraries were used for interfacing the Wi-Fi module as well as the fingerprint reader [29].

2.2.3. System Requirements

Fingerprint Scanner: Used to scan different finger to find the respective prints. We use the R307 Fingerprint reader for our project. Arduino Uno: The basic controller for our prototype. It will control the various parts in our model, such as the fingerprint scanner, database upload etc. based on the code provided.

NodeMCU: Provides wi-fi connectivity along with data transmission and reception.

Display Module: To display the status of fingerprint analysis. This project uses the JHD162A display module.

Electronic Components Kit: To provide a common interface to connect the various electrical components through a breadboard, connecting wires, LEDs, and resistors [30].

The compatibility specifications are:

- **Processor: -** Dual Core minimum
- **RAM: -** 512MB minimum
- **Hard disk:** -80 GB minimum
- **Monitor: -** 14” VGA
- Mouse, keyboard having 101 keys

2.3. Conclusion

In this chapter, we identified the requirements of this project. All the relevant requirements were discussed in detailed in this chapter. The system requirements

including fingerprint, NodeMCU, Display Module, **(**JHD162A), Electronic Components Kit, Processor specifications have been mentioned in detail. The BIMS server was used to upload the data from the module. Dynamic Requirements like Reliability,Availability, Security and Maintainability has also been discussed in this chapter. The use case diagram , activity diagram, class diagram and ER-diagram have been applied to the system design.

3. DESIGN

3.1. ARCHITECTURE OF THE PROPOSED SOLUTION

The implementation of the system is based on the above mentioned solution and the problem of the aforementioned and planned problems in the process of logging the specific requirements of the application process. In other respects, the requirements of this resolution are determined by the composition of the resolution and the specific requirements of the application. The system is utilized by the compromise and the different modes of the system and can be described in the same way as the system. The design of the system is utilized for the purpose of the communication and the implementation of the specifications and the implementation [13]. The system design is based on the difference between the system and the system usage of the programmer.

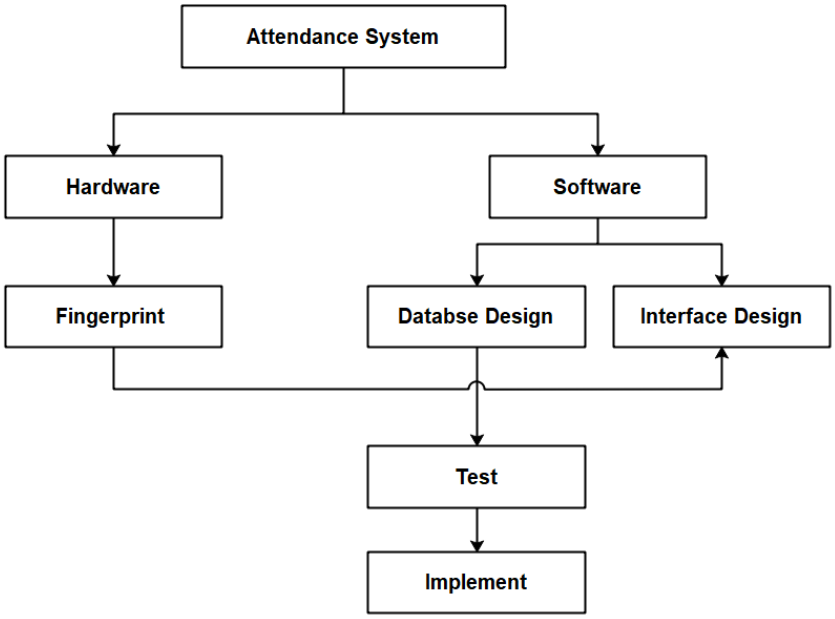

Fig.3.1 Proposed System Architecture Module

In our system design we have two modules, and they are:

- Hardware module
- Software module (Mobile application)

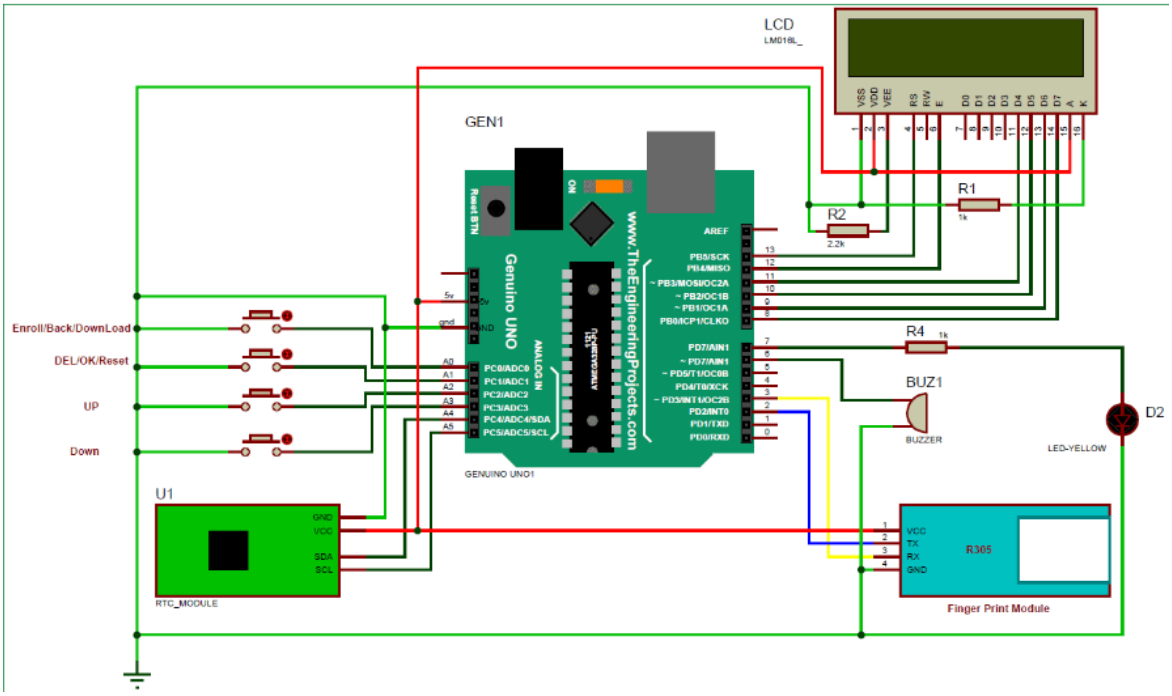

Fig.3.2 Proposed System Architecture

The architecture of the system encompasses multiple connections. We start with the Arduino UNO motherboard. Connections through its pins are made to every other device used [14]. The keypad, LCD Display, the NodeMCU(ESP8266) and the fingerprint scanner is connected via connecting wires held together with the use of a breadboard.The platform chosen for the user to send data is cloud platform. The reason for choosing this platform was the ease of use and in today's world where cloud can be used to store and retrieve data safely makes the best of use of this project. To implement this platform, we are using Thingspeak and the reason for choosing Thingspeak is because it is one open source that helps to build IOT based applications and to receive and send data from IOT based equipment's [17]. Another platform we are using is Adruino. As a free and open source platform, Arduino is suitable to carry out electronic projects. Arduino is made up of a hardware programmable circuit board (commonly called as a microcontroller) and software (IDE) running on a computer that helps in writing and uploading computer code on the physical boards [18].

The Arduino platform has grown in popularity among those who are just getting started with electronics, and for good cause. Unlike most prior programmable circuit boards, the Arduino does not require a separate piece of hardware (known as a programmer) to load new code into the board; instead, a USB cable is all that is required. Furthermore, the Arduino IDE makes programming simple by using a simplified form of C++. Finally, Arduino offers a standard form factor that separates the microcontroller's tasks into a more manageable packaging. .All interfacing part gets done through Adruino IDE [23]. Data is taken from user and sent to Adruino which reads the data serially. All the read serial data is sent to Thingspeak through NodeMCU. Adruino also provides the interface for interaction between NodeMCU and Thingspeak [24].

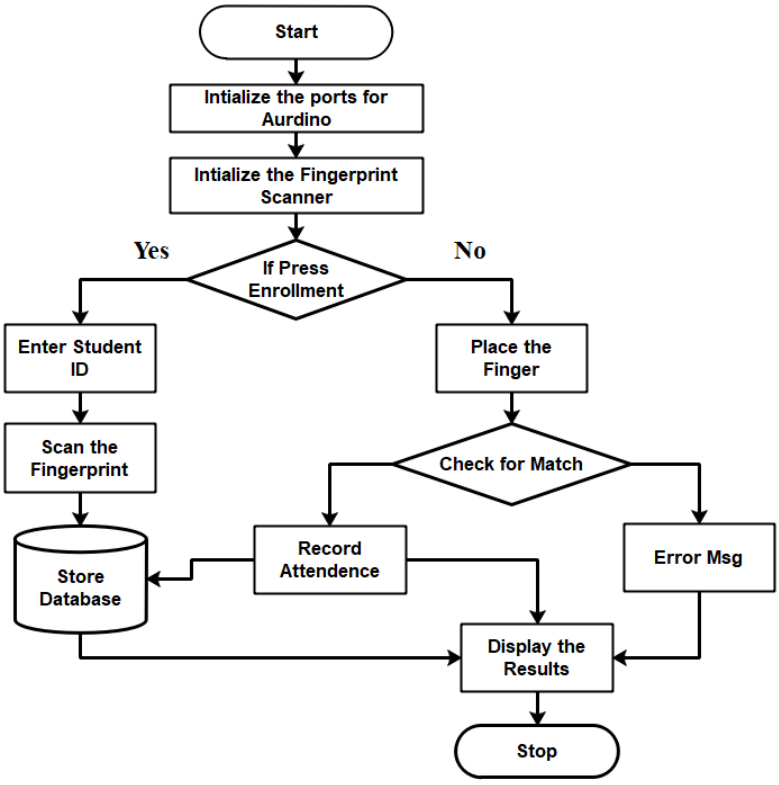

Fig..3.3. Flow Diagram for Proposed Model

A sketch is a programme created with the Arduino IDE. Sketches are stored as text files with the extension.ino on the development computer. Before version 1.0, sketches were stored with a.pde extension in the Arduino software (IDE). The

minimum Arduino C / C ++ program has only the following two functions:

- **Setup():**When a sketch is initiated after it has been switched on or restarted, this functionality is called once. This helps in setting up variables, input and output needle modes as well as rest of the libraries in the sketch [25].
- **Loop**(): Once the setting () is announced, the loop () launches itself on the main program with iterations. Then, it is needed to monitor the whiteboard until it turns off or restarts [28].

3.2. ALGORITHMSFORTHESOLVINGTHE PROBLEM

Recognize fingerprint of students is the next main task of this research. This process is the biggest sub task of the project because fingerprint recognition is a result of a series of sub processes. It is needed to detect fingerprint of humans at the beginning. After that, need to preprocess those fingerprints. Then feature extraction should be performing before going to face recognition. When feature extraction is completed, the module must be trained to recognize fingerprint and finally it can be evaluated and used to recognize students. Acquisition, Preprocessing (Template Generation), Feature extraction, and Matching are the four key design components of an automated fingerprint identification system [8].

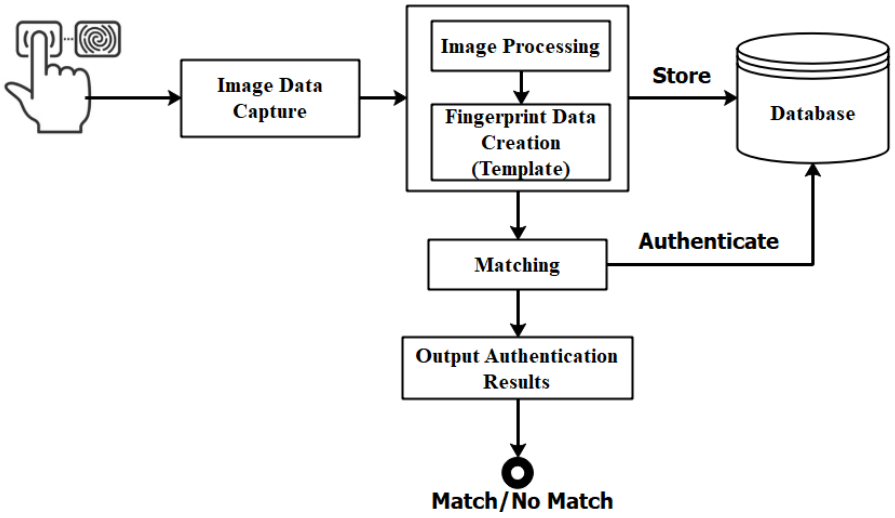

Fig.3.4 Fingerprint Biometric Recognition Model

3.2.1. Acquisition Process

The most common ways to capture a fingerprint picture are available. The phrase "live scan fingerprint" refers to a fingerprint picture that is produced straight from the finger without the need for an impression on paper. The optical frustrated total internal reflection (FTIR) idea is the most widely used method for obtaining a live-scan fingerprint images. For our research we are using an optical scanner for reading fingerprints. We are using Futronics FS88 USB compatible scanner as shown in Fig.3.3. High end CMOS sensor technology and accurate optical was found being used in .FS88 fingerprint scanner..

Fig.3.5 Furoins FS88 Optical Fingerprint Scanner

The results for fingerprint scan using Futronics FS88 & designed interface is shown in Fig. 3.4.

Fig. 3.6. Fingerprints scanned by Futronics FS88 using given Interface.

Fig. 3.4&3.5 show some live fingerprint scans. Good quality fingerprints are shown in Fig. 3.5 (a) & (b), if the person has not cleaned the finger or if the finger is wet due to sweating then it will result in dry or wet fingerprints as shown in Fig 3.6 (a) & (b), respectively. Dry fingerprints have unclear edges and wet fingerprints have smudged edges in both the cases feature extraction is difficult and this gives rise to error rate. The captured fingerprints are subjected to preprocessing [11],[12].

Fig. 3.7. Different Quality Fingerprints (a) Dry Fingerprint (b) WetFingerprint (c) Good Quality Fingerprint

First two fingerprints are poor as the ridge structure is distorted, Dry fingerprints have very weak ridges and wet fingerprints have smudged edges they lead to failure in feature extraction resulting in low accuracy [16]. In the fingerprint acquisition process, there are three parts::

- Enrolment
- Verification
- Data collection

3.2.2 Enrolment

Registration takes place once for each person. Each person should register their fingerprint pattern by placing their thumb finger on the fingerprint scanner. The scanner takes a fingerprint image and determines the unique properties of the fingerprint image. The fingerprint contains ridges and ridges with various

interruptions and breaks. Solo's various brushes and valleys are the basis for easily visible loops, arcs and swirls at the fingertips. After capturing the fingerprint brush pattern, a template is created, and the fingerprint is encrypted in numbers [21]. Necessity number series are different for each fingerprint pattern. When the process must be completed, the fingerprint scanner sends the encryption result to a memory location or database.

3.2.3. Verification Process

Another process is about the control process that a most repetitive process. This is done each time the user wishes to use the fingerprint device. When he places his finger on the surface of the fingerprint reader, the fingerprint scanner processes the fingerprint. The resulting fingerprint pattern is compared to a stored enrollment template already stored in the database or memory location where the enrollment process was performed. When the fingerprint pattern goes through the comparison process, it shows a confirmation on its screen and gives the user access [22].

3.2.4. Data Collection Process

The data collecting procedure is the last to be completed. Data on the usage of a fingerprint device or a record may be gathered over time and utilized in a manner to determine the presence of a person or the number of times they are limited [26].

3.3. DESCRIPTION OF DATA

- To be processed for minutiae detection or correlation, Automatic Fingerprint Recognition Systems require a clean fingerprint that is also free from any noise. To reduce the effects of noise, dryness, wetness of the finger, and differences in the applied pressure when scanning the fingerprint, the fingerprint must be pre-processed. The following steps are included in the pre-processing process:
- Smoothening Filter.
- Intensity Normalization.
- Estimating Orientation Field

- Segmenting Fingerprints.
- Extracting Ridge / Core point Detection.
- Thinning / ROI Extraction.

The list given above is exhaustive but depending on the applicationand captured datasubset of this may be used.

Fig.3.8. ASampledatasetwith100 fingerprintimages

3.3.1. Smoothening & Intensity Normalization

Smoothening Filter and Intensity normalization are very common image processing techniques. This work uses a Gaussian filter of size 3*3 to remove effect of noise if required.

Gaussian filters represent linear smoothing filters in which the weights are selected using Gaussian functions. These filters are mostly used to smooth the image and remove Gaussian noises. It is represented as follows:

$$h(m,n)=\left[\frac{1}{\sqrt{2\pi\sigma}}e\frac{m^2}{2\sigma^2}\right]\times\left[\frac{1}{2\pi\sigma}\frac{n^2}{e2\sigma^2}\right]$$

To help in the interpretation of a picture, a high boost filter is employed to retain a few of the low-frequency features... Before deleting the low pass picture in high boost filtering, the input picture is increased by an amplification factor, as shown below:.

$$\text{High boost}=A\times f(m,n)-\text{low pass}$$

$$\text{High boost}=(A-1)\times f(m,n)+f(m,n)-\text{low pass}$$

$$\text{High boost}=(A-1)\times f(m,n)+\text{high pass}$$

This model gives a better result by removing noise as shown below.

Fig.3.9..Resultant of images with Gaussian High boost filter

Depending on lighting conditions, pressure applied while scanningand cleanliness of the scanner surface the image intensity changes.Before extracting feature vector from the fingerprint image, wenormalize the region of interest in each sector separately to aconstant mean and variance. We divide the input image in nonoverlapping sectors of size $W*W$ pixels. Normalizationis doneto remove the effects of sensor noise and finger pressuredifferences. Let $G(x,y)$ denote the gray value at pixel (x, y), μ_i and σ_i the estimated mean and variance of sector S_i

respectively, and $N_i(x,y)$ the normalized gray-level value at pixel (x,y). For all the pixels in sector S_i the normalized image is definedas:

$$N_i(x,y) = \mu_0 + \sqrt{\frac{\sigma_0 * (G(x,y) - \mu_i)^2}{\sigma_i}} \quad \text{if } G(x,y) > \mu_i$$

$$N_i(x,y) = \mu_0 - \sqrt{\frac{\sigma_0 * (G(x,y) - \mu_i)^2}{\sigma_i}} \quad \text{otherwise}$$

This method gives output as shown in Fig 3.7, we have selected $\mu_0 = 100$, $\sigma_0 = 100$ and applied the method discussed above for the fullimage.

Fig.3.10. Result of Intensity Normalization

Every pair shows original and normalized fingerprint, resultant fingerprint have uniform brightness irrespective of original image.

3.4. Orientation Field Extraction

Let I_m be the initial image restricted to the significant mask obtained in the segmentation and withthe ridge-valley structure emphasized as previously described.The orientationextraction procedure is composed of three steps: orientation estimation, spatialperiod computation, orientation refinement [24].

Filtering-based orientation estimation algorithms can only fix small noisy (wet or dry fingerprints) or missing patches (scars) in the picture since they only work at the local level. As a result, the described technique uses an oriented anisotropic Gaussian filter to improve the ridge pattern before computing the final orientation. The resilient noise to pixel-alignment approach is used to determine the orientation of the Gaussian filter. A 9x9 mask containing eight oriented differentiations of pixel values is used to calculate the orientation. This mask's structure was introduced in and was built specifically to acquire the prevailing direction of fingerprint ridge valley structure. Because estimated values were confined to a set number of eight discrete values, this change only employs this mask to compute eight pixel value differentiations. The mean values of five pixels in eight directions are obtained in the first stage [23].

$$\mu_i(x,y) = \frac{\sum_{j=1}^{5} p_j^i}{5}$$

where: $\mu_i(x,y)$ represents the means of pixel values in eight directions,

p_j^i - represents the pixel values in one of i directions from the normalized image,

i - represents the discrete direction value $(0,....,7)$, respectively from 0^o to 157.5^o, with 22.5^o step

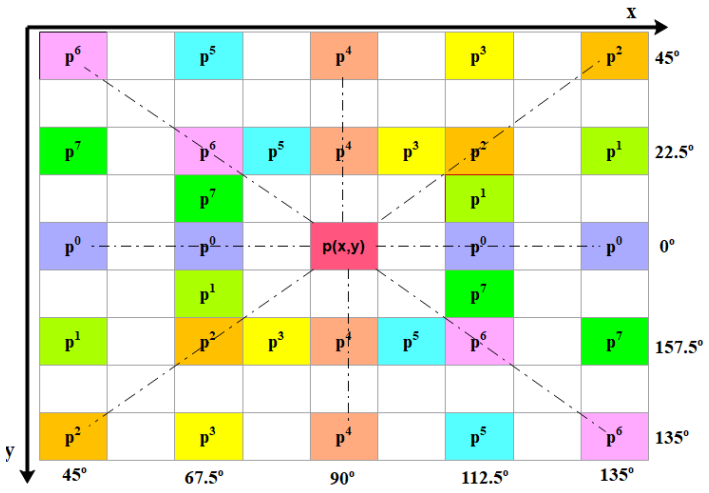

Fig.3.11. The 9×9 mask to compute the differentiation of pixel values.

Differentiation (fluctuation) of neighboring pixels values has been computed, in each direction as:

$$\mathrm{Diff}_i(x,y)=\sum_{j=1}^{5}\left|S_i(x,y)-p_j^i\right|, i=0,1,...,7$$

The reference orientation of the centre pixel is anticipated to be the orientation with the least variation of grey values. Each pixel in 13x13 window has its own average value, which is computed individually in each direction:

$$\mathrm{Avg}_i(x,y)=\sum_{u=x-w/2}^{x+w/2}\sum_{v=y-w/2}^{y+w/2}\mathrm{Diff}_i(u,v),\quad i=0,1,...,7 \text{ Wherein, } w=13$$

The orientation of the smallest value, from all eight oriented averaged differentiation values, is expected to be the closest to the dominant orientation of that pixel:

$$\alpha(x,y)=i_{min}(x,y)22.5^o \text{ where } i_{min}(x,y)=\arg(\min\{\mathrm{Avg}_i(x,y),\ i=0,1,....,7\})$$

In the end, the anisotropic Gaussian filtering is applied to perform the ridge pattern enhancement :

$$E_n(x,y)=\frac{\sum_{u=-w}^{w}\sum_{u=-w}^{w}N(u+x,v+y)G_a(u,v)}{\sum_{u=-w}^{w}\sum_{u=-w}^{w}G_a(u,v)}$$

Wherein, $w=4$ and anisotropic Gaussian kernel is shown by:

$$G_a(u,v)=\exp\left(\frac{(u\alpha C)^2+(v\alpha C)^2}{2\sigma_i^2}+\frac{(-u\alpha C)^2+(v\alpha C)^2}{2\sigma_j^2}\right)$$

where $\sigma_i=10,\sigma_j=90$ and their ratio determines the Gaussian kernel flatteningdeformation.

Fig. 3.12.a) Original low fingerprint image,b) Fingerprint image after normalization

The ridge's direction is orthogonal to the average phase angle of pixel value changes, as shown by gradients, because gradients are pixel scale orientations. The modification in this method has the following significant aspects:

Orientation Field Extraction Method
1. Compute the gradients $\partial_x(x,y)$ and $\partial_y(x,y)$ at each pixel of the fingerprint image $E_n(x,y)$. Depending on the computational requirement, thegradient operator may vary from the simple Sobel operator to the morecomplex Marr-Hildreth operator. 2. If gradient values i.e. $\partial_x(x,y)=\partial_y(x,y)$ are same, when added randomly $\pm 1$to a gradient. If one of gradients values equals 0 (for example $\partial_x(x,y)=0$) then, it is also randomly ± 1. 3. Estimate the local orientation in $W\times W$ blocks, centered at pixel (x,y) using the following equations: $$V_x(x,y)=\sum_{u=x-\omega/2}^{x+\omega/2}\sum_{v=y-\omega/2}^{y+\omega/2}2\partial_x(u,v)\partial_y(u,v)$$ $$V_y(x,y)=\sum_{u=x-\omega/2}^{x+\omega/2}\sum_{v=y-\omega/2}^{y+\omega/2}(\partial_x^2(u,v)-\partial_y^2(u,v))$$ $$\theta(x,y)=\frac{1}{2}\tan^{-1}\left(\frac{V_x(x,y)}{V_y(x,y)}\right)$$

3.5. Orientation Refinement

Let R be a rectangular region in the image I_m, and $\mathbf{R}:\mathbf{R}\to\square$ be an orientation field, defined in R, possibly given by the initial estimation $\mathbf{O}_m$; we denote with $\mathbf{R}(x)$ the orientation $\mathbf{R}(x,y)$ at point. $\mathbf{x}=(x,y)^T\in R$. The refinement process is defined by two operators. Let $R\in\square$,we select N_C points $\mathbf{C}_R=\{\mathbf{r}_i\}_{i=1,2,..,N_C}\subset\square^2$ from the circumference

of radius R centered at $\mathbf{0}$. We define the adjuster G_a ofthe field $\mathbf{R}(x)$ as the following orientation field:

$$G_a(x) = \frac{1}{N_C}\sum_{k=1}^{N_C} \mathrm{sgn}\left[a(\mathbf{x},\mathbf{r}_k)\right] a(\mathbf{x},\mathbf{r}_k)^2 \mathbf{R}(\mathbf{x}+\mathbf{r}_k)$$

where $$a(\mathbf{x},\mathbf{r}_k) = \mathbf{R}\left\{\frac{\mathbf{R}(\mathbf{x}+\mathbf{r}_k)}{|\mathbf{R}(\mathbf{x}+\mathbf{r}_k)|}\frac{(\mathbf{r}_k \cdot 1 - i\mathbf{r}_k \cdot j)}{\|\mathbf{r}_k\|}\right\}$$

i and j are the usual vectors of the canonical base for $\square^2$. i is the imaginary unit, $\mathbf{R}$ gives the realpart of a complex number, $\square$ denotes the inner product, $\|\square\|$ is the Euclidean norm in $\square^2$ and $|\square|$ isthe absolute value in $\square$. We call adjusted field the orientation field $\mathbf{AF}$ obtained as:

$$\mathbf{A}\mathbf{R}_0(x)^2 = (1-s)\mathbf{R}(x)^2 + sG_a(x)^2$$

$$\mathbf{A}\mathbf{R}_0(x) = \frac{\mathbf{A}\mathbf{R}_0(x)}{|\mathbf{A}\mathbf{R}_0(x)|}\max(|\mathbf{R}_0(x)|, |G_a(x)|)$$

where $s \in (0,1)$ is a small parameter.The smoother G_s is the other operator and it is defined as follows:

$$G_s(\mathbf{x}) = \frac{1}{N_C}\sum_{k=1}^{N_C} \mathrm{sgn}\left[f_d(\mathbf{x},\mathbf{r}_k)\right] a(\mathbf{x},\mathbf{r}_k)^2 \mathbf{R}(\mathbf{x}+\mathbf{r}_k)$$

where $a(\mathbf{x},\mathbf{r}_k)$ is defined as above and

$$f_d(\mathbf{x},\mathbf{r}_k) = \mathbf{R}\left\{\mathbf{R}(\mathbf{x}+\mathbf{r}_k)\overline{\mathbf{R}(\mathbf{x})}\right\}$$

where $\overline{\mathbf{R}(\mathbf{x})}$ is the complex conjugate of $\mathbf{R}(x)$. We call smoothed field the orientation field $\mathbf{SR}$ obtained as:

$$\mathbf{s}\ \mathbf{SR}_0(x)^2 = (1-s)\mathbf{R}(x)^2 + sG_S(x)^2,$$

$$\mathbf{SR}_0(x) = \frac{\mathbf{SR}_0(x)}{|\mathbf{SR}_0(x)|}\max(|\mathbf{R}(x)|, |G_S(x)|)$$

The key operator of our procedure for orientation refinement is the smoother, that succeeds in reconstructing and giving global coherence to a noisy orientation field.

The drawback of its application is the shifting effect it has on loops; since we iteratively apply the smoothing operator, we need a reliable mask where loops are in the background. The adjuster has the converse effect on loops, giving them back their initial position and enhancing their rounded shape [17],[18].

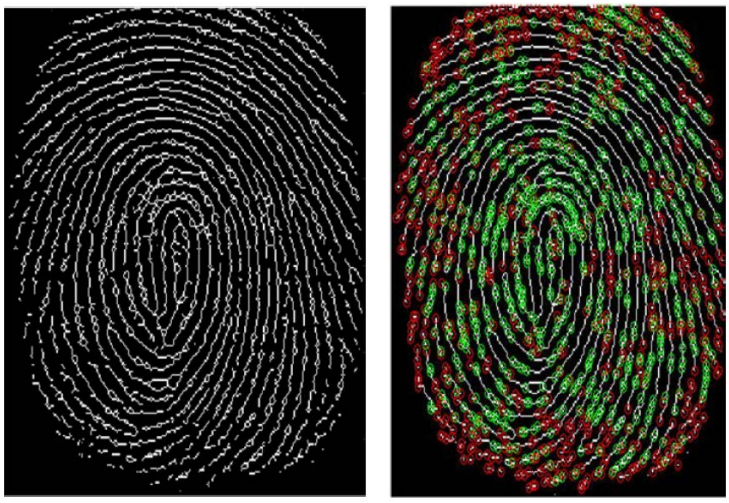

Fig.3.13. True Minutiae Sets

In this project Student fingerprint and collected and stored in the database as shown in the fig.3.13

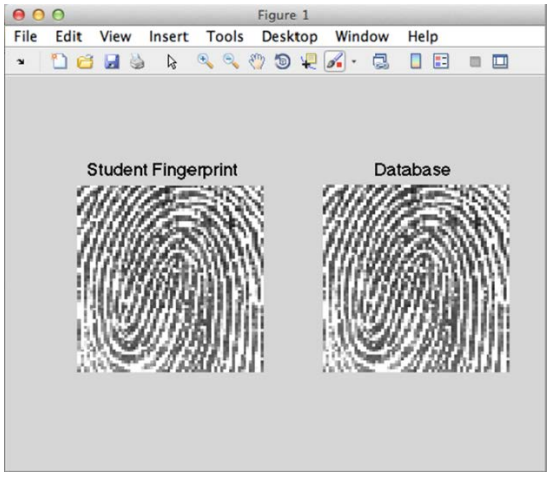

Fig.3.14. Storing in Database

3.6 Algorithm used.

Note: The entry made by the user through the keypad accounts for the following buttons being pressed: A, B, C, D. For the password, the user has access to all 10 digits as well as two special characters like * and #.

Algorithm for Bio-Metric Attendance System

Step 1: Check for the Fingerprint and NodeMCU modules.
if Module check is passed:
goto Step 2.
else
goto Step 1.
Step 2: Authenticated login with Keypad.
if Password matched:
goto Step 3.
else
goto Step 2.
Step 3: Display Home Screen. Read user input.
if Entered key is A:
goto Step 4.
else if Entered key is B:
goto Step 4.
else if Entered key is C:
goto Step 6.
else
goto Step 7.
Step 4: Read input from user for the student ID.
if Entered key is A:
goto Step 5.

else if Entered key is B:

goto Step 6.

else if Entered key is D:

goto Step 3.

Step 5: Scan Fingerprint from the user and record it.

Step 6: Check the corresponding ID, delete it if it exists.

Step 7: Scan and check if the finger is stored in the device data store.

Step 8:

if D key is pressed:

goto Step 3.

if Finger found:

goto Step 8.

else:

Display that finger is not found.

Return to Step 7.

Step 9: Display the ID found on the screen.

Send the matched ID and the timestamp to the server for processing.

Return to Step 7.

This algorithm succinctly produces the effect of the system developed. It allows the model to perform all the required operations. This simple implementation can be improved by adding more functionality. With our limited keypad size, user entry can only be restricted to a certain combination. The password entry can be improved a IOT [28].

3.7. Conclusions

Fingerprinting is a time tested technology with excellent levels of accuracy. Strong fingerprint systems can process thousands of users without permitting a false match and can verify approximately 100% of users with just one or two finger placements. Fingerprint technology may be used in a variety of logical and physical access situations because to its small size and low power needs, as well as its tolerance to environmental changes like background light and temperature. In this chapter, the architecture of the proposed solution has been presented, having hardware module and software module. In the acquisition aspect, Pre-processing steps like Template Generation, Feature extraction, and Matching are used as key design components of the automated fingerprint identification system. Here, we have analyzed the functioning of FS88 fingerprint scanner. Also, in the fingerprint acquisition process, Enrolment, Verification and Data collection steps are discussed. Here, the Orientation Field Extraction aspects are also dealt with. The orientation refinement is attempted by applying the Algorithm for the Bio-Metric Attendance System.

4. IMPLEMENTATION

4.1. IMPLEMETATION OF INTERFACES

4.1.1.Creating a MySQL Database

To store attendance details, it is necessary to have a database. First create a local database on Arduino and after completing database locally, it was implemented on a cloud environment. Database part starts by installing MySQL server and Python bindings for MySQL on Arduino. While the process of installation, it prompts and asked a password for MySQL root. After completing the installation, the shell is displayed, and it was used to do all the configurations with the MySQL server. First, it is needed to login to MYSQL server root and create a database on the server [34].

```
mysql> Create Database Stud_Atten

mysql> USE Stud_Atten
```

Fig.4.1.Login of MySQL

After creating a database, three tables created to store student Fingerprint's registrationdetails, store course details and store student's attendance details. Student registration details table consists with student first name, last name, e mail address and course. Data is inserting to this table at the time of Fingerprints are registering for students. In other words when data writing to the Fingerprints. Attendance table consists with student name,tag id, date, and time. Course details table consists of course, codes and course names.At the time of working with a database, it is required to have a connection with the database. To connect to the database, it is needed to import the library to connect with the database at the beginning of the script. Following code segment will import MySQL python libraries.

```
import mysql.connector
```

Fig.4.2. MySQL Connector

Then it is necessary to start connection by specifying a host name, user, password, anddatabase. When local database used, the following code segment creates the connection to the MySQL database.

```
mydb=mysql.connector.connect(
        host=”localhost”,
        user=”admin”,
        passwd=”admin@123”,
        database=”Stud_Atten”
    )
```

Fig.4.3.Connecting to the Database.

After implementing database locally and checked, the database was hosted on a web server in order to get more expanded capabilities. For hosting the database, a free hosting service web site used that is called “db4free.net”. This web site provides facility to host MySQL databases for free. A MySQL database created there with three tables called class detail, student data and attendance data. The database contain following tables

a) STUDENTS_LIST: This table provides all of the information on the students enrolled in that specific course. It includes their name, roll number, section, and department, as well as their unique Finger Id.

```
mysql> select * from STUDENTS_LIST;
+------------------+-------+---------+------------+-----------+
| STUDENT          | ROLL  | SECTION | DEPARTMENT | FINGER_ID |
+------------------+-------+---------+------------+-----------+
| RAJAT_CHAUDHARY  | 12543 | B11     | CSE        |         1 |
| PRIYARANJAN      | 12519 | B11     | CSE        |         2 |
| DURGESH_DEEP     | 12250 | B12     | CSE        |         3 |
| DEEPAK_KUMAR     | 12228 | B9      | CSE        |         4 |
+------------------+-------+---------+------------+-----------+
```

b) DATE_AND_DAY: It contains two columns that maintain track of all the days that a certain class was held, as well as the day number. Each time a new class is taken, it gets updated.

```
mysql> select * from DATE_AND_DAY;
+------------+------+
| DATES      | DAY  |
+------------+------+
| 2012-12-01 | 1    |
| 2012-12-02 | 2    |
| 1245-12-09 | 3    |
| 2014-07-02 | 4    |
+------------+------+
```

c) ROLL NO TABLES: There are n tables, with n denoting the number of students enrolled in the course. The dates of the class and their attendance on that given day are listed in these tables.

```
mysql> select * from Y12519;
+------------+-----+-----------------+
| DATES      | DAY | PRESENTorABSENT |
+------------+-----+-----------------+
| 2012-12-01 | D1  |               1 |
| 2012-12-02 | D2  |               1 |
| 1245-12-09 | D3  |               0 |
| 2014-07-02 | D4  |               0 |
+------------+-----+-----------------+
```

d.) DAY TABLES: There are n tables, with n being the number of days that courses were held. These tables list the students' names, roll numbers, and attendance.

```
mysql> select * from D1;
+---------+-----------------+
| ROLL_NO | PRESENTorABSENT |
+---------+-----------------+
| 12543   |               0 |
| 12519   |               1 |
| 12250   |               0 |
| 12228   |               0 |
+---------+-----------------+
```

4.1.2. Fingerprint Attendance System Code for Arduino

In the following sections, the Arduino code for a fingerprint attendance system is illustrated. Despite the fact that the code is well-documented with comments, we'll go over a few key points here. For integrating fingerprint module with Arduino board, we utilised fingerprint library.

In the initial phase, this project includes a header file that defines the input and output pins, as well as the macro and defined variables. Following that, in the setup function, this project directs designated pins and starts the LCD and fingerprint module.

```
 void setup()
 {
    delay(1000);
    lcd.begin(16,2);
    Serial.begin(9600);
    pinMode(enroll, INPUT_PULLUP);
    pinMode(up, INPUT_PULLUP);
    pinMode(down, INPUT_PULLUP);
    pinMode(del, INPUT_PULLUP);
    pinMode(match, INPUT_PULLUP);
    pinMode(buzzer, OUTPUT);
    pinMode(indFinger, OUTPUT);
    digitalWrite(buzzer, LOW);
    if(digitalRead(enroll) == 0)
    {
      digitalWrite(buzzer, HIGH);
      delay(500);
      digitalWrite(buzzer, LOW);
      lcd.clear();
      lcd.print(“Please wait”);
      lcd.setCursor(0,1);
      lcd.print(“Downloding Data”);
```

Given void *checkKeys()* function is used for checking Enroll or TAKE_ATTENkey is pressed or not and what to do if pressed. If the ENROL key

pressed the *Enroll()* function is called and TAKE_ATTEN key press then *take_atten()* function is called. The selected function is performed using the fingerprint image and converted into the template, prior to being saved by the selected ID into the fingerprint module memory.

```
 uint8_t getFingerprintEnroll()
 {
   int p = -1;
   lcd.clear();
   lcd.print(“finger ID:”);
   lcd.print(id);
   lcd.setCursor(0,1);
   lcd.print(“Place Finger”);
   delay(2000);
   while (p != FINGERPRINT_OK)
   {
     p = finger.getImage();
```

Given function is used for storing attendance time and date in the allotted slot of EEPROM.

```
 void attendance(int id)
 {
   int user=0,eepLoc=0;
   if(id == 1)
   {
     eepLoc=0;
     user=user1++;
   }
   else if(id == 2)
```

```
{
  eepLoc=210;
  user=user2++;
}
else if(id == 3)
```

4.1.3. Creating GUI Interface

4.1.3.1. Login Page (Admin)

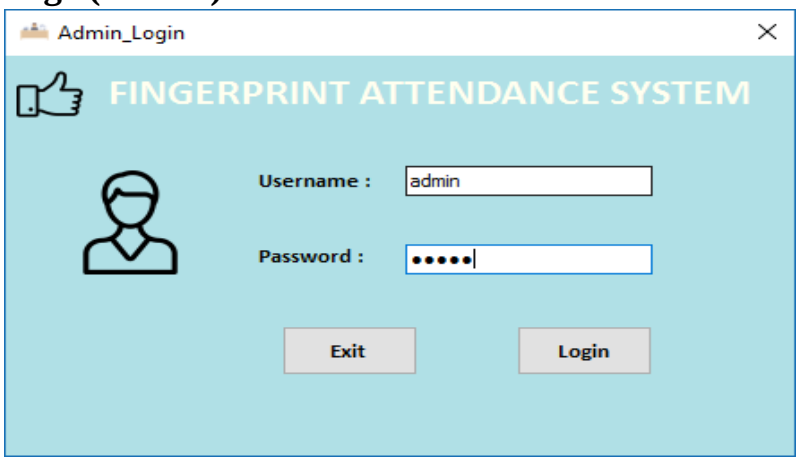

Fig.4.4 Login Page (Admin)

The login page for admin can be created using the sample code below.

```
<?php
@require_once ‘config/config.php’;
?>
<html>
<head>
<?php @require_once ‘config/78ommons.php’; ?>
</head>
<body>
```

<!—wrap starts here →

<!—header →

<?php //@require_once ‘menu/header.php’; ?>

<h1 id=”logo-text”>Kashipara Group</h1>

Software Solution

<!—navigation →

<?php //@require_once ‘menu/menu.php’; ?>

<!—content-wrap starts here →

<?php echo $_SESSION[‘Msg’]; ?>

<form id=”formSubmit” method=”post”action=”process/processLogin.php”>

<input type=”hidden” name=”type” value=”login” />

<table class=”tbl” width=”700px”>

<tr>

<td>User Name</td>

<td><input type=”text” id=”UserName” class=”validate[required]”

name=”UserName” /></td>

</tr>

<tr>

<td>Password</td>

<td><input type=”password” id=”Password” class=”validate[required]”
name=”Password” /></td>
</tr>
<tr>
<td></td>
<td><input type=”submit” value=”Login” name=”submit” /></td>
</tr>
</table>
</form>

<?php @require_once ‘menu/sidemenu.php’; ?>
<!—content-wrap ends here →

<!—footer starts here→
<?php @require_once ‘menu/footer.php’; ?>
<!—wrap ends here →

</body>
</html>

4.1.3.2. Home Page

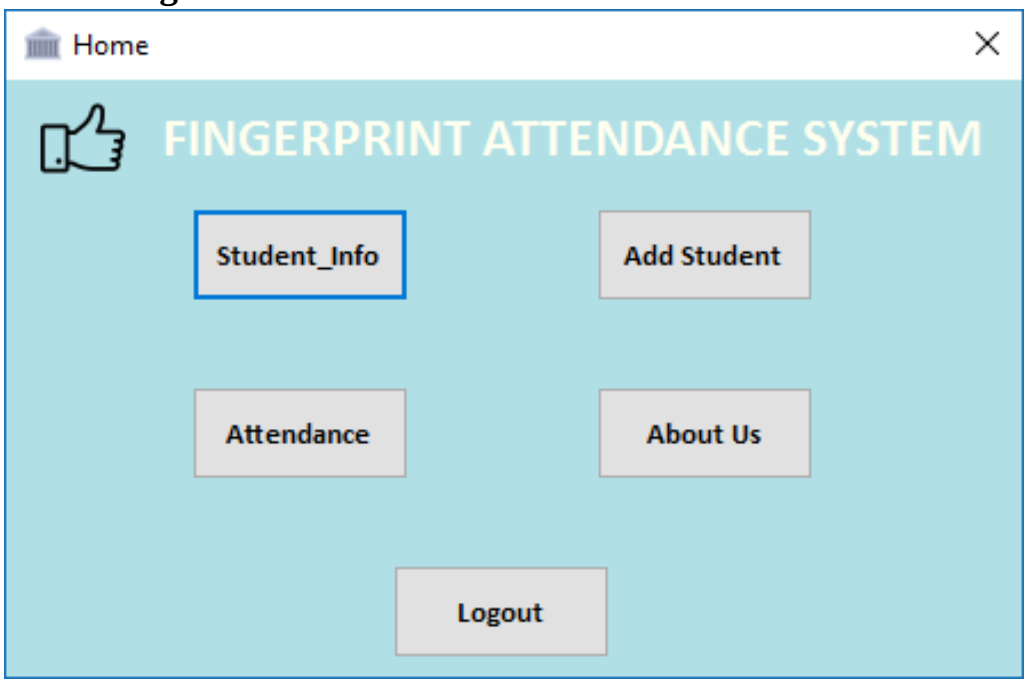

Fig.4.5. Home Page

4.1.3.3. Student Information

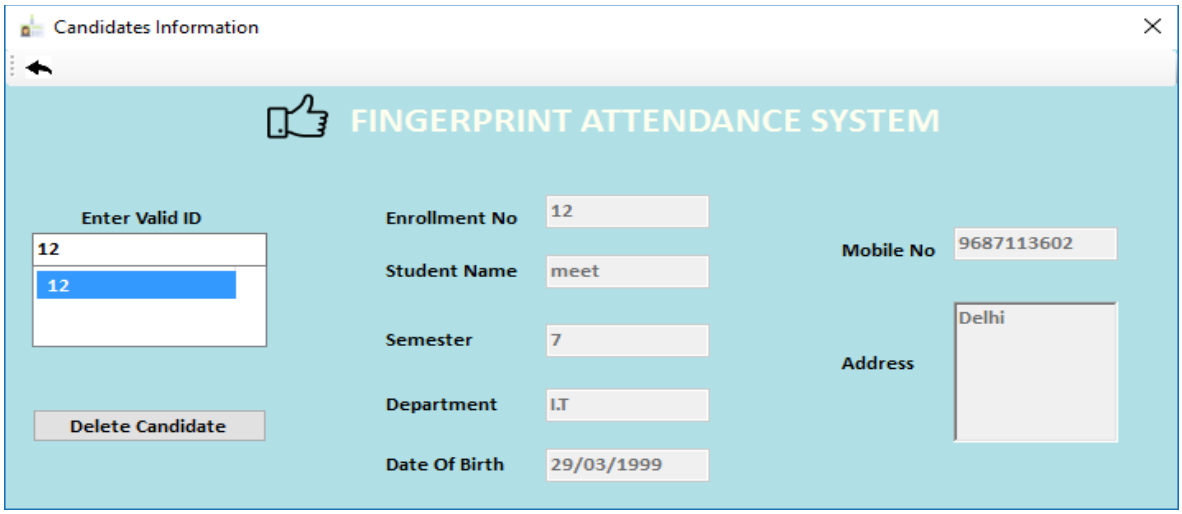

Fig.4.6. Student Information page

4.1.3.4. Add Student

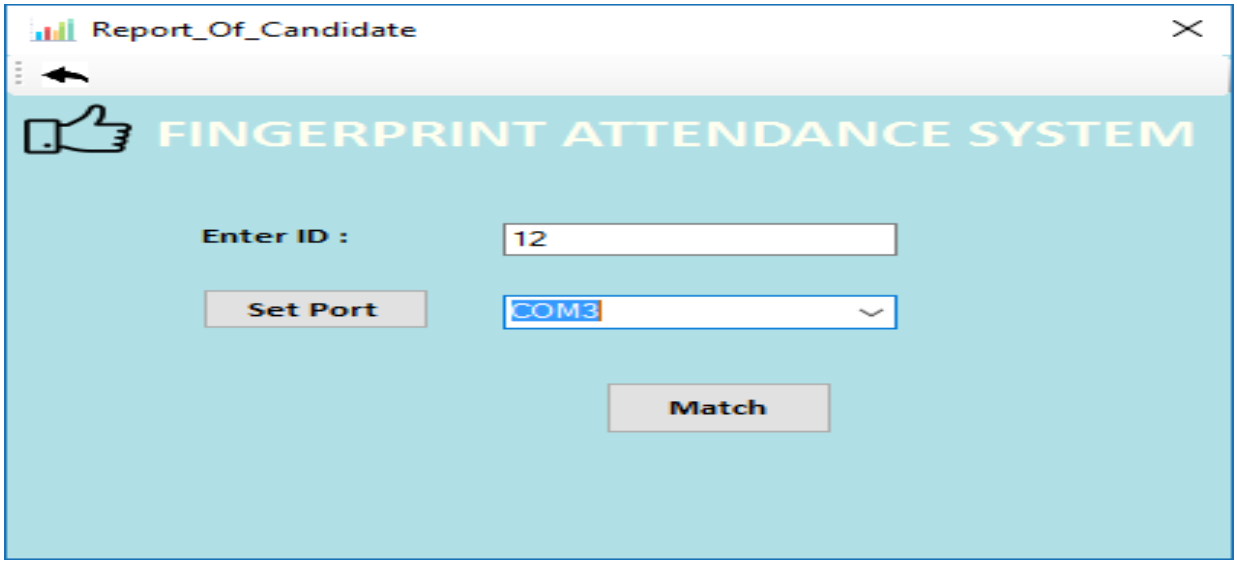

Fig.4.7. Add Student Page

4.1.3.5. View Attendanc

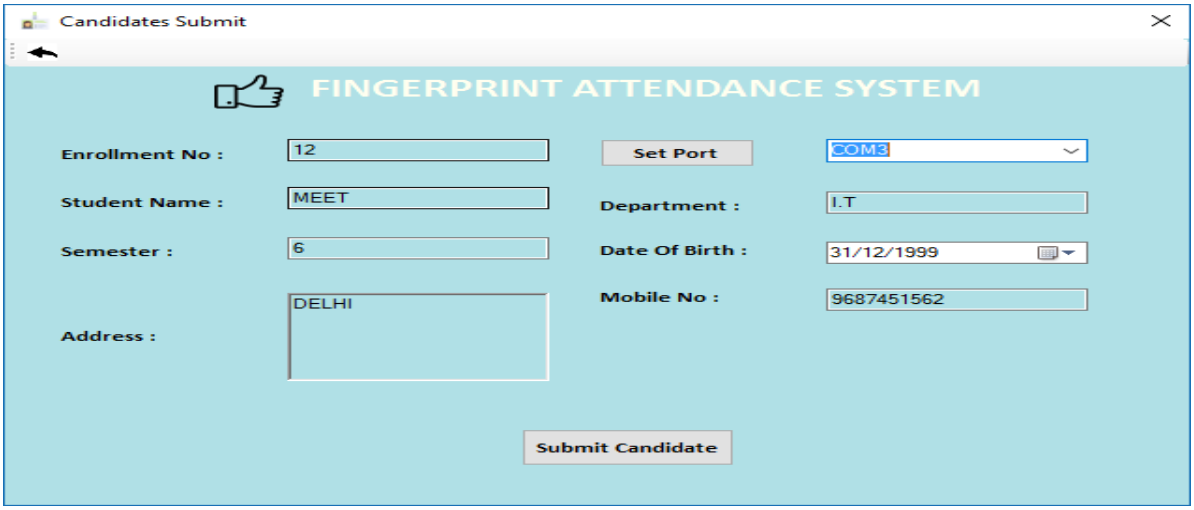

Fig.4.8. View Attendance

4.1.3.6. Fingerprint Enrollment Window

Fig.4.9. Fingerprint Enrollment Window

4.2. Performance

This application was created to fast recognize fingerprints and display the visual result. In the command window, all processes show the amount of time they took to complete. The performance of two primary components of this application was evaluated by using different database sizes for database creation (Part 1) and the identification procedure (Part 2). Figure 4.10 shows the time it takes to create a new database in relation to the size of the databases fingerprint pictures. Table 4.1 also shows the amount of datasets on disc as well as their elapsed time.

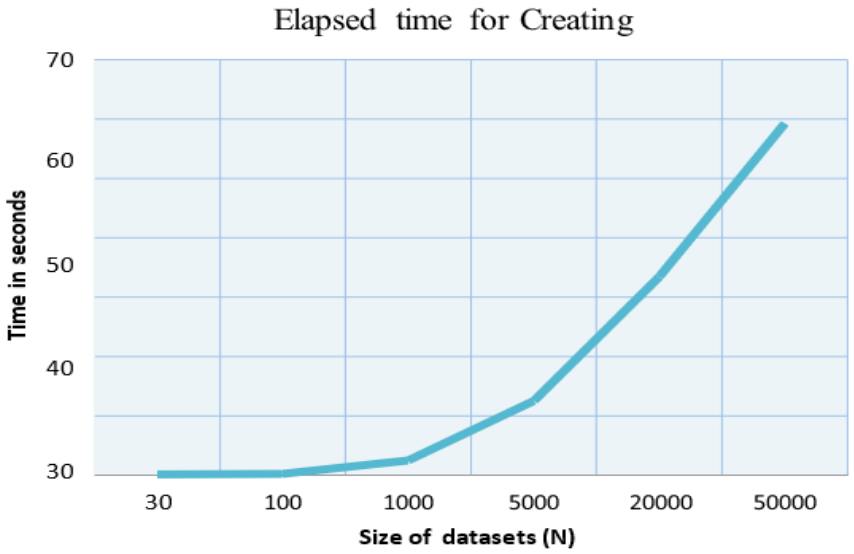

Fig.4.10. elapsed time to create a new database from different size of datasets.

Number of Images in Datasets	Size on Disk	Elapsed time (Sec.)
30	1,144,962 bytes	0.1725
100	3,936,105 bytes	0.2503
1000	39,936,105 bytes	2.5008
5000	199,680,538 bytes	12.5049
10000	399,360,176 bytes	25.5501
20000	798,720,352 bytes	33.2906
50000	1,996,800,000 bytes	59.0427

Table 4.1. Size of the datasets on disk and elapsed time to make a new database.

In the second phase, this application is supported by varied database sizes, which includes transforming vector input photos, using a hybrid model, and calculating Euclidean distance with four sides. In figure 4.11, the time it takes to identify each fingerprint using the technique is depicted. With a higher database size, the time it takes to compare fingerprints has grown. This signifies that the size of the database has influenced the elapsed time for identification. It is expected that by picking the largest database, the time it takes to identify someone will be reduced.

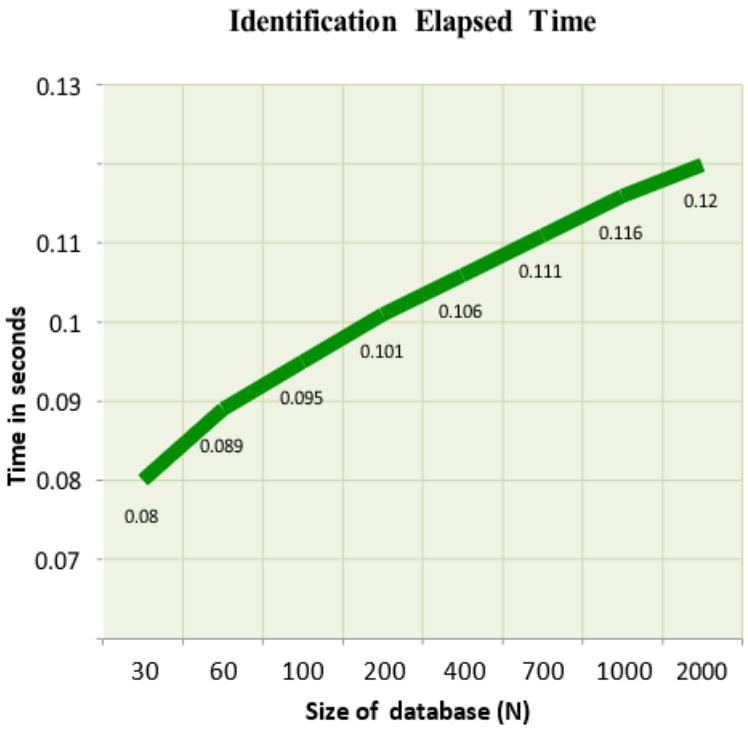

Fig.4.11 – Eelapsed time for identification fingerprint in varied database sizes. Identification done in 0.08 seconds and match yielded fingerprint vs. database with 30 images. Amplification done by taking database size to 0.12 seconds.

4.3. Conclusion

This project mainly comprises tasks related to the development of student attendance management system with the help of fingerprint verification system. This project represents a framework using which attendance management can be made automated

and on-line.This project have designed and implemented database for attendance system using MYSQL. This project has shown the fingerprint recognition process, based on minutia extraction of fingerprint image. The template generated in fingerprint recognition system is successfully stored and retrieved from database. The developed system is more efficient and time saving than the old traditional attendance taking method.

5.TESTING

The purpose of the testing phase is to identify defects or errors by placing individual components of the application under scrutiny. And in the test stages, functions, objects, or modules represent different stages of testing. When the system testing process begins, such components are conjoined in order to structure the entire system. At this stage, the testing function is mainly aimed at determining whether the system is able to meet its functional requirements, and also that it does not behave unexpectedly. In this general system test procedure, the test data is the inputs that are designed into the system, while the test system input is the test cases, and the outputs are predicted from this input only when the system. to your specifications? Silk is mainly made to study behavior in a coherent system. Test cases are selected to examine the behavior of the system under all possible combinations of existing conditions. Consequently, the expected behavior of the system for different combinations is specified.

Therefore, only test cases whose inputs and outputs are expected on the lines are selected. Invalid records and records that should be properly reported, as well as records that do not occur frequently, can be considered as special cases.

5.1.TESTING METHODOLOGY

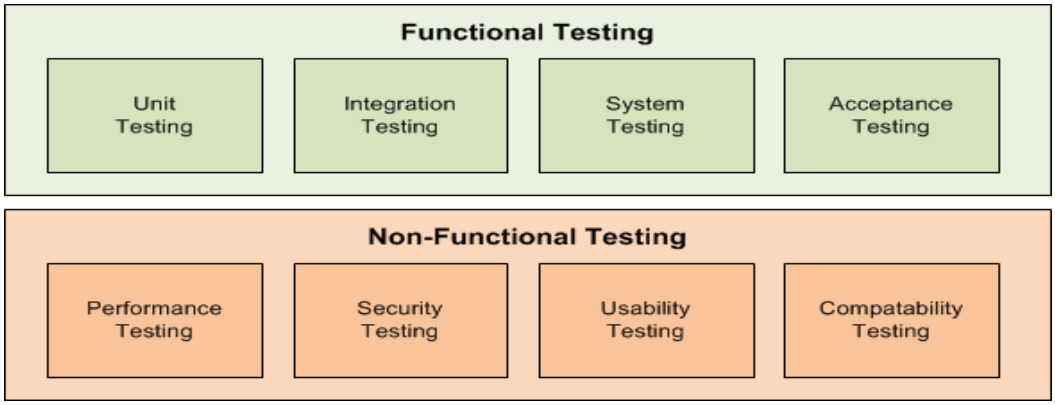

Fig.5.1.Testing Methodology

5.2. Conducting the Test Procedure

5.2.1. Unit Testing

The application is based on the unity and implementation of the verification of the unity of the software (mode). In the case of a phase-out system, the planes of the unitary unit can be prepared by means of a control system, the control unit can be used to control the mains of the fault condition due to the presence of limitations in the software modules. In addition to the warranties and guarantees of use of the module and the module, the interface between the module and the module, the interface between the module and the probe are considered important. For example, this is the case with the module and the module is not valid, and it is not known to be independent and adamant but not to the error. This is how it is realized in the past [19]. It is vital that the components and components of the fund are in good condition and that the components are individually individualized. However, it is necessary to verify that the fund is verifiable if the initial situation is positive. The first step is to provide a procedure for programming and programming. In the final phase of the test, the result is that it can be used as a result of a functional operation and which results in a modification of the mode of operation.

5.2.1.1. Testing Strategy

The following strategy is used to test the units:

- **Functions to be tested** - The functions to be tested include the work of an individual component to execute the entire program properly.
- **Test items** - Test items include all the individual items or functions that together make up the entire system.
- **Purpose of testing** – Its purpose is to verify the functionality of the device as the main source of the project.
- **Acceptance / Failure Criteria** - This criterion is based on the development of primary source file.

Test Case#1

Name of Test	To test the detection of Fingerprint Module
Item to be Tested	R305 Fingerprint Module
Sample Input	Testing
Expected Output	Module Detected
Actual Output	As Expected
Remarks	Pass

Test Case#2

Name of Test	To test the Wi-Fi Connection
Item to be Tested	NodeMCU
Sample Input	Testing Node
Expected Output	Internet Connected
Actual Output	As Expected
Remarks	Pass

5.2.2. Integration Testing

There are chances that data will be lost through the interfaces, and if this happens, then one module may have an adverse effect on the sub-functions of another, and also when these modules will be combined, they may not produce the desired main functions. Global data structures can also present problems. Integration testing was a symmetric technique for building the structure of the program and, at the same time, testing for errors associated with the interface. First, all modules are added up in the testing process and then the entire program will be fully tested [19].

5.2.2.1. Testing Strategy

The following strategy is used to perform an integration test:

- **Functions to be tested -** The functions to be tested here are mainly the composed of two or more components added together.

- **Test items -** Test items include the device to which it is connected and therefore properly connected.
- **Aim of the test:** The aim here is to examine the functional modularity of all modules, which will be addressed in the respective tests mentioned below.
- **Success / Failure Criteria**- Success / failure criteria for this type of test is based only on proper cleaning of the corresponding files associated with these test cases.

Test Case#3

Name of Test	To test the detection of Fingerprint Module
Item to be Tested	Faculty Authentication
Sample Input	********
Expected Output	Enroll Now
Actual Output	As Expected
Remarks	Pass

5.2.3 Functional Testing

Useful testing is a kind of discovery where the experiments will be founded on the details of the product part that is under test. Capacities will be accordingly tried by giving them the best possible information and looking at the yield, and the interior program structure is seldom taken into consideration (Unlike white box testing).

5.2.3.1 Testing Strategy

The following strategy is implemented in a realistic way as described below:

- **Functions to be tested** -The functionalities of the probable are included in the validation of the functionalities.
- **Test items** –includes elements of the application.

- **Aim of the test**- the basic method of test validation and verification is validated by the centralized functionalities of the map in accordance with the requirements for the use of all cases.
- **Success / Failure Criteria**- The pass/fail criteria are the actual outputs of the combined modules matching the intended outputs. In the tables below, the tabulation of the functional test has been done.

Test Case#4

Name of Test	To test fingerprint matching with finger already enrolled
Item to be Tested	Match
Sample Input	Finger on R305
Expected Output	Student Found. Attendance Marked.
Actual Output	As Expected
Remarks	Pass

5.2.4. System Testing

Following coordination testing, the product was fully assembled as a package; a few interface flaws were discovered and corrected, and following the last round of programming tests, approval tests will begin. When the product's components are available in a fashion that the client can recognize, the approval test will be successful. The framework was tested against the framework's requirements. Framework testing was really a series of examinations whose primary purpose was to thoroughly exercise the PC-based framework. Despite the fact that each test will have a different purpose, they all seek to ensure that all of the framework's components have been properly integrated and are performing their assigned functions.

5.2.4.1. Testing Strategy

The failures occurring in the test case showed that there was a defect in the code, which was rectified by suitably altering the code to remedy the issue and rerunning the test cases to ensure that the issue had been handled. When an event or an item is inserted in the sensor network before the nodes are deployed, failure test cases occur. This implies that there was an error creating an event message indicating non-implementation of the sensor nodes. During the development process, each device was fully checked during unit testing and verified to be functional. In integration testing, all modules are linked, and the entire software has been properly tested.

Test Case#5

Name of Test	To test authentication during boot-up
Item to be Tested	Initial Authentication
Sample Input	********
Expected Output	Login Success
Actual Output	As Expected
Remarks	Pass

Test Case#6

Name of Test	Deletion check
Item to be Tested	Delete finger data
Sample Input	Finger on R305
Expected Output	Finger Deleted
Actual Output	As Expected
Remarks	Pass

Test Case#7

Name of Test	Enrollment at correct Index (Primary Key)
Item to be Tested	Index on Enrollment
Sample Input	New Finger on R305 at Index: 69
Expected Output	Finger Enrolled at Index 69
Actual Output	As Expected
Remarks	Pass

Test Case#8

Name of Test	Matching false finger
Item to be Tested	False finger
Sample Input	False finger on R305
Expected Output	Finger Not Detected
Actual Output	As Expected
Remarks	Pass

5.5.Conclusion

In this chapter the testing methodology containing functional testing and non-functional testing was described. different testing strategies like unit testing, integrated testing, functional testing, and system testing have been applied and described with different test cases. In unit testing, the software design was tested. The detection of fingerprint module was tested by applyingR305 finger print module while wi-fi connection was tested by using NodeMCU. In integration testing, faculty

authentication is used to test detection of fingerprint module. In functional testing, fingerprint matching with already enrolled finger was tested with Match. In system testing, authentication during boot up is done by testing initial authentication, besides deletion check by applying delete finger data. All these test cases are verified and found to have generated better outcomes.

CONCLUSION

This project thesis has shown a reliable and smarter attendance system by applying fingerprint recognition-based biometric system and IOT that removed impersonation and made the records secure. The current prototype is capable of fully accepting a fingerprint, storing it locally, transmitting matched data, receiving status as well as deletion of the IDs. Every module has a capacity of holding 128 individual fingerprints. Therefore, any class with less than this threshold number of students will be easily capable of performing the task without error. To counter the need for more than 128 IDs, the module can be modified to incorporate extra storage using an SD-card. The precision of the fingerprint module has a high degree of accuracy, which helps in keeping the efficiency as well as the security of greater standards.

Limitations

Limitations of the current model are based on the fact that the current storage facility provided is on-device. Instead of having limited on-device storage, the model can be enhanced to perform storage on the cloud or on a separate SD card. Other limitations include limited battery power and slower server response times.

Future Enhancements

Numerous enhancements can be made to the module. While some have been previously discussed like inclusion of an SD-card reader. Other enhancements can be attempted in the following areas:

- Android/IOS mobile integration, using contemporary Arduino libraries coupled with existing module infrastructure.
- Creating better fingerprint matching algorithms to increase accuracy.

- Better, faster, and more secure transmission methods.
- Global storage and connection-oriented module.

REFRENCES

1. Current Biometric Adoption and Trends [Electronic Resource] URL https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf.

2.Communications of the ACM [Electronic Resource] URL: https://dl.acm.org/doi/fullHtml/10.1145/328236.328110

3. Fingerprint biometric based access control and classroom attendance [Electronic Resource] URL: https://ieeexplore.ieee.org/abstract/document/7443699?casa_token=RwMW6-_2rIYAAAAA:K6jg41p7Y1XgcAml8ocZTnEGuDIxYNeF5ziHLwb7FqqJI874Y7LsxKckmxLExogPEoMoniKsY7A5gw

4. Universal Studios Hollywood, “Biometrics,” [Electronic Resource] URL https://www.universalstudioshollywood.com/faqs/how-are-biometrics-used-at-universal-studios-hollywood/.

5. Student attendance monitoring at the university using NFC,” [Electronic Resource] URL https://ieeexplore.ieee.org/abstract/document/6266137?casa_token=FZMat4-X9KwAAAAA:xMgxDGs_Beho8sqse0XIXEbB2Sh6diQ__UMHHETSwymef4V7nSbmkk56jmAFCpMuMxs1zOsg_qcciA

6.“Development of an online biometric-enabled class attendance register system,” [Electronic Resource] URL: https://ieeexplore.ieee.org/abstract/document/7530647

7.“A new image thresholding method based on Gaussian mixture model,” [Electronic Resource] URL Publisher Site | Google Scholar | Zentralblatt MATH | MathSciNet

8.Biometric Systems and Their Applications, Visual Impairment and Blindness[Electronic Resource] URL https://www.intechopen.com/books/visual-impairment-and-blindness-what-we-know-and-what-we-have-to-know/biometric-systems-and-their-applications.

9. NFC Forum, “NFC [Electronic Resource]
URL] http://www.nfcforum.org/news/june06_architecture_and_specs/nfc_architecture_schematic
10. A History of Fingerprinting [Electronic Resource] URL http://www.south-wales.police.uk/fe/master.asp?n1=8&n2=253&n3=1028. Accessed 30 January 2010
11. Serkan T (2009) Women uses tape to trick biometric airport fingerprint scan. Crunch Gear [Electronic Resource] URL
http://www.crunchgear.com/2009/01/02/woman-uses-tape-to-trick-biometric-airport fingerprint-Sc an.
12. History of Fingerprinting. FINGERPRINTING [Electronic Resource] URL
http://www.fingerprinting.com/history-of-fingerprinting.php. Accessed 30 January 2010.
13.[ElectronicResource]URL:https://www.how2electronics.com/fingerprint-sensor-based-biometric-attendance-system/
14. Electronic Resource] URL: https://www.skyfilabs.com/project-ideas/biometric-attendance-system-with-iot
15. [Electronic Recorce] https://circuitdigest.com/microcontroller-projects/fingerprint-attendance-system-using-arduino-uno
16. Fingerprint Based Student Attendance System Using GSM [Electronic Resource] URL http://www.ijsr.net/archive/v2i10/MDkxMDEzMTE=.pdf
17. Development of Attendance System using Biometric Fingerprint Identification. [Electronic Resource]
URL:http://eprints.uthm.edu.my/3297/1/12_Norshidah_Katiran__19Feb2010_.pdf.
18. Attendance Management System using Fingerprint Scanner. [Electronic Resource]
URL:http://library.utem.edu.my/index2.php?option=com_docman&task=doc_view&gid=5283&Itemid=113

19. The Four Levels of Software Testing [Electronic Resource] URL: http://www.seguetech.com/blog/2013/07/31/four-levels-software-testing
20. What are The Advantages and Disadvantages of the Evolutionary Prototyping Technique [Electronic Resource] URL http://www.answers.com/Q/What_are_the_advantages_and_disadvantages_of_the_evolutionary_prototyping_technique.
21. Fingkey Hamster II fingerprint sensor [Electronic Resource] URL http://www.nitgen.com/New_site/eng/product/ pc_hamster2.asp
22. FVC2004 Fingerprint Verification Competition [Electronic Resource] URL http://bias.csr.unibo.it/fvc2004 download.asp
23. [Electronic Resource] URL https://how2electronics.com/fingerprint-biometric-attendance-system-arduino/
24. [Electronic Resource] URL https://circuitdigest.com/microcontroller-projects/fingerprint-attendance-system-using-arduino-uno
25. Biosec. 2015. OK-300 Data Sheet. (Online) [Electronic Resource] URL http://biosec.com.cn/r/cms/www/biosec/OK300.pdf
26. [Electronic Resource] URL https://www.bayometric.com/fingerprint-readertechnology-comparison/
27. [Electronic Resource] URL https://components101.com/modules/ds3231-rtcmodule-pinout-circuit-datasheet
28. [Electronic Resource] URL https://store.arduino.cc/usa/arduino-uno-rev3
29. Functional req//DevOps. [Electronic Resource] URL: https://www.guru99.com/functional-requirement-specification-example.html (the date of access: 01.01.2020).
30. UML-Diagrams. [Electronic Resource] URL: https://www.uml-diagrams.org/use-case-diagrams.html/ (the date of access: 09.04.2020).

31. online. visual-paradigm. [Electronic Resource] URL https://online.visual-paradigm.com/diagrams/tutorials/use-case-diagram-tutorial/ (the date of access: 15.01.2020).
32. Visual paradigm. [Electronic Resource] URL: https://www.visualparadigm.com/guide/uml-unified-modeling-language/what-is-componentdiagram/
33. techterms. [Electronic Resource] URL: https://techterms.com/definition/database/
34. My Sql Database [Electronic Resource] URL : https://www.mysqltutorial.org/