IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 3, April 2022

Finger Print Based ATM System

Shaikh Mohd Faiz[1], Shaikh Nadeem[2], Motiwala Qusai[3], Dr. Shabina Sayed[4]
Students, Department of Information Technology1,2,3
Guide, Department of Information Technology4
M. H. Saboo Siddik College of Engineering, Mumbai, Maharashtra, India

Abstract: *Our Project is to develop the technique for fingerprint authentication in ATMs. This target can be mainly decomposed into image preprocessing, feature extraction and feature match. For each sub-task, some classical and up-to-date methods in literature are analyzed. Based on the analysis, an integrated solution for fingerprint recognition and authentication is developed for demonstration. Our demonstration program is coded in ASP.NET & MATLAB. For the program, some optimization at coding level and algorithm level are proposed to improve the performance of my fingerprint authentication system. These performance enhancements are shown by experiments conducted upon a variety of fingerprint images. Also, the experiments illustrate the key issues of fingerprint recognition that are consistent with what the available literatures say.*

Keywords: Finger Print.

I. Introduction

1.1 Problem Statement

In the present scenario, a traditional ATM system accepts only the PIN CODE security system, enabling the other person rather than the owner to access the account very easily. This ensures that the Traditional ATM system is not fully secured.

1.2 Objective

The objective of our project is to provide biometric security through fingerprint authentication in ATM applications. Also the experiments illustrate the key issues of fingerprint recognition that are consistent with what the available literatures say. The underlying principle is the phenomenon of biometrics “AUTHENTICATION”, in this project we propose a method for fingerprint matching based on minutiae matching.

1.3 Description of Fingerprint

The fingerprint is arguably a person’s most unique physical characteristic. While humans have had the innate ability to recognize and distinguish different fingerprints for millions of years, computers are just now catching up…

The twist of this software is that it can pick someone's fingerprint out of a crowd, extract that fingerprint for the rest of the scene and compare it with a database full of stored images.

In order for this software to work, it has to know what a basic fingerprint looks like. Fingerprint recognition software is based on the ability to first recognize fingerprints, which is a technological feat in itself, and then measure the various features of each fingerprint.

1.4 What Is A Fingerprint?

A fingerprint is the feature pattern of one finger (Figure 1.2.1). It is believed with strong evidence that each fingerprint is unique. Each person has his own fingerprints with permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time.

A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges (Figure 1.1.2). Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage one is called termination, which is the immediate ending of a ridge the other is called bifurcation, which is the point on the ridge from which two Branches derive.

DOI: 10.48175/IJARSCT-3310

Figure 1.2.1

Figure 1.2.2 Minutia (Valley is also referred as Furrow, Termination is also called Ending, and Bifurcation is also called Branch)

1.5 What is Fingerprint Authentication

The fingerprint authentication problem can be grouped into two sub-domains. One is fingerprint verification and the other is fingerprint identification (Figure 1.3). In addition, different from the manual approach for fingerprint authentication by experts, the fingerprint authentication here is referred to as FAA (Fingerprint Authentication in ATM), which is program based.

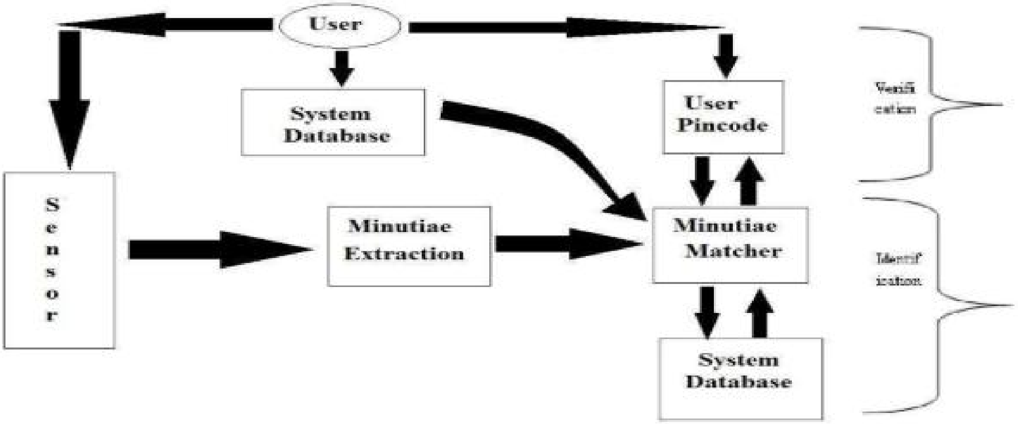


Figure 1.3: Verification Vs. Identification

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his PIN-CODE. The fingerprint verification system retrieves the fingerprint template according to the PIN-CODE and matches the template with the real time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System). However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint.

1.6 Approaches for Fingerprint Recognition

Two representation forms for fingerprints separate the two approaches for fingerprint recognition.

- **Minutia - based:** The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the currently available fingerprint recognition products. We also concentrate on this approach in our project.
- **Image-based:** The second approach, which uses image-based methods, tries to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition. And it is useful to solve some intractable problems of the first approach. But our project does not aim at this method, so further study in this direction is not expanded in our thesis.

II. Literature Survey

RBI 3X-Fingerprint Based ATM Machine (IJARCCE, Vol. 5, Issue 3, March 2016)

Nowadays security becomes a great issue in every part of life. Passing of information faces massive problems due to various types of attacks to the communication link. Many security algorithms are available to protect information from being hacked. The biometric authentication process adds a new dimension of security for any person sensitive to authentication. This paper presents a secured and an energy efficient ATM banking system that is a highly secured system compared with the existing one. At present most of the ATM systems use triple data Encryption Standard (3DES). Which has some drawbacks; such as, it is vulnerable to differential attacks and also slow in performance. Issues in current ATM network: ATM Card frauds, use of ATM Card duplicators card sharing by family and friends ,inability to trace the wrongful users ,ATM PINs can be shared on phone or recorded using secret cameras. In this system 3 vital things are to be matched i.e. 6 digits unique code, fingerprint and 4 digit password. In this system, a 6 digit number will be given to every user. The second thing will be the users fingerprint which will be detected by finger print recognition sensor. The third thing which is to be matched is the 4 digit pin code. The 4 digit pin code is the same concept which we are using nowadays for withdrawing money from ATM.

The design of ATM systems based on fingerprint recognition took advantage of the stability and reliability of fingerprint characteristics, The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded systems which makes the system more safe, reliable and easy to use.

(a) Fingerprint module,(b)motor,(c)motor driver,(d)ATMEGA 16 Microcontroller,(e)Lcd (f)keypad .LCD is used in a project to visualize the output of the application.LCD can also used in a project to check the output of different modules interfaced with the microcontroller. Thus lcd plays a vital role in a project to see the output and to debug the system module wise in case of system failure in order to rectify the problem.Keypad is basically used to provide the input to the microcontroller. ATMEGA 16 has 16 Kbytes of InSystem Programmable Flash, Program memory with Read-While-Write capabilities, 512 bytes EEPROM, 1 Kbyte SRAM, 32 general purpose I/O lines, 32 general purpose working registers, a JTAG interface for Boundary scan, On-chip Debugging support and programming, three flexible Timer/Counters with compare modes.A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching

The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded systems which makes the system more safe, reliable and easy to apply for better use.In these systems, bankers will collect the customer fingerprints and mobile number while opening the accounts then customer only access ATM machines. The design of ATM terminal system based on fingerprint recognition took advantages of the

DOI: 10.48175/IJARSCT-3310

stability and reliability of fingerprint characteristics, a new technology which was designed for the sake of human beings when their ATM card is stolen, based on the image enhancement algorithm of Gabor and direction filter

Fingerprint Based ATM System : Survey (IJIRSET Vol. 6, Issue 11, November 2017)

Biometric can be used to identify physical and behavioral characteristics of user fingerprints. There are many biometric devices like iris detection, face recognition, and fingerprint. In our Project, we are using fingerprint biometrics. Users' fingerprints are scanned using biometric traits and stored in a database. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. Fingerprint biometrics are easy to use, cheap and most suitable for everyone. Characteristics of fingerprints vary from person to person. Fingerprints are the unique identity of the user.

Data of a fingerprint is stored in a database using the enrollment process through the Bank. Banks provide authentication to the customer that can be accessed while performing the transaction process. If a fingerprint match is found in the database then a transaction takes place. After verification if fingerprint does not match transaction will be cancelled. Using fingerprint based ATM system user can make secure transaction.

Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of the user such as pin code and fingerprint matching. Basically we can explain the complete Fingerprint based ATM system in two phases: 1) Enrolment Phase 2) Authentication phase.

- Enrolment phase: In the robust fingerprint application, 3-4 fingers should be enrolled. This enables the system to set a high security threshold and still be able to cope with everyday real life issues like skewed finger placement, dirty, wet dry, cut or worn fingers. The Enrolment is crucial because the once recorded reference data will normally be used over the active lifetime of the user or his/her biometric hardware device. Multiple Finger enrolment: It is strongly recommended enrolling more than one finger. During daily life injuries can happen that turn a registered fingerprint currently unusable while minor cuts not affect a robust sized sensor system.
- Authentication Phase: In this phase users can make transactions by using their fingers. Users can place their finger on the Biometric scanner and the user's finger scan can be matched through a database, where all authenticated user’s fingerprints are stored .If User wants to do a transaction they simply place their finger on biometric scanner and get their money in a few seconds. If a user's fingerprint cannot be matched by the database due to some accidental cuts on their fingers then they can use their other fingers and we will also provide a 4 pin code option ,users can also use this option with their convenience.

ATM machines increase the reliability of the bank organization by providing easy access to the cash transaction. We can withdraw the cash anywhere and anytime without waiting in the queue. Hence, ATM cards are used wildly but we have to face the fraud related to the ATM transaction . To make ATM transactions more secure we are using a biometric scanning machine to identify the account holder. Finger is the unique identity of each person so using a Biometric Fingerprint scanner we can avoid ATM related fraud. The Security feature enhances stability and reliability of owner recognition .The whole system is designed by using technology of embedded systems which makes the system more secure, reliable and easy to use.

ATM Security using Fingerprint Authentication andOTP (IJERECE Vol 5, Issue 5, May 2018)

By using Biometric Authentication and GSM technology, we can overcome many of the flaws introduced by our current ATM system such as shoulder surfing, use of skimming devices, etc. In our proposed system, Bankers will collect the customer’s as well as respective nominee’s fingerprint and mobile number at the time of opening the account. The primary step is to verify the currently provided fingerprint with the fingerprint which is registered in the Bank’s database at the time of account opening. If the two fingerprints get matched, then a message will be delivered immediately to the user’s mobile number which is the random 10 digit pin number called as One Time Password (OTP). This OTP can be used only once, thus this avoids various problems associated with the present system. For every transaction, a new OTP will be sent to the account holder’s mobile number, thus there will not be a fixed PIN number for every transaction. Thus, PIN number will vary during each transaction assuring security.

Project proposes the idea of using fingerprint and OTP in ATMs as password instead of the traditional pin number. By using fingerprint recognition, the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy. We also have an OTP feature along with the fingerprint authentication which will definitely not allow any criminal to use the password for any kind of fraud as the OTP is valid only once. Thus, it becomes useless for the next time even if any criminal gets hold of it . The main modules of a fingerprint verification system are: a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation b) Preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction c) Feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors d) Matching, in which the feature vector of the input fingerprint is compared against one or more existing templates.

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both Biometric fingerprint strategy and GSM technology. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking. The developed application has been found promising on the account of its sensitivity to the recognition of the cardholder's finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines.

Fingerprint Based Security System Format (IRJET Volume: 06 Issue: 06 | June 2019)

Biometrics is a technology that helps to make our data tremendously secure, distinguishing all the users by way of their personal physical characteristics. Biometric information can be used to accurately identify people by using their fingerprint, voice, face, iris, handwriting, or hand geometry and so on.Fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device.If an unauthorized person tries to login then the user will be alarmed with the help of a buzzer which is linked with the controller. An authorized user is given 3 chances to re-enter the id if he/she forgets.

The system uses R305 fingerprint scanner to capture fingerprints. This system can be employed at any application with enhanced security because of the uniqueness of fingerprints. It is convenient due to its low power requirement and portability. Although fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated, hence no misuse of the system is possible. In the verification, the system compares the input fingerprint to the fingerprint stored in the database of a specific user to determine if they are from the same finger (1:1 match). In identification, the system compares the input fingerprint with the prints of all registered users in the database to determine if the person is already known under a replica or false identity (1: N match).

Fingerprint images cannot be recreated from templates, hence no one can misuse the system. Speed of execution can be enhanced with the use of more sophisticated microcontrollers. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

Securing Automated Teller Machine (ATM) TransactionUsing Biometric Finger print (AJER Volume-9, Issue-9, pp-36-43, 2020)

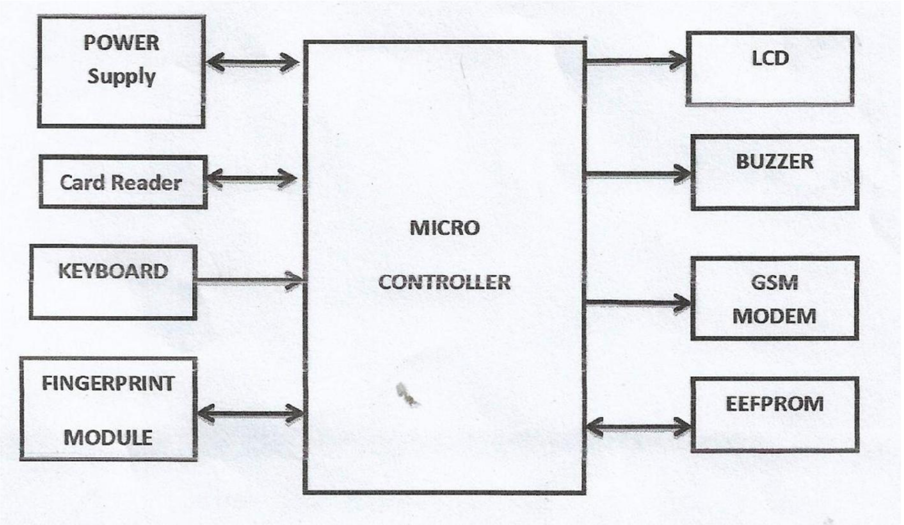
A biometric system is a recognition system that allows personal identification by determining the authenticity of a particular physiological or behavioral characteristic of the user. This identification method is preferred to traditional methods that involve passwords and PINs for several reasons. Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral Characteristics to recognize or authenticate its identity. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost

The proposed system works with biometric fingerprint only, the customer uses fingerprint at ATM and if matched correctly, then all banks of the customer have an account with appears, the customer will select the bank to transaction with, then select the account type with that bank , then chose to withdraw, check account balance and so on. Customer will now choose or select the bank he wants to withdraw money from and specify if the account is Current or Savings, this is a means of securing ATM transactions using biometric fingerprint.

Conventional methods of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged.s. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology using fingerprint identifiers may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud and lead to user convenience by broadly providing the following three functionalities (a) positive identification (b) large scale identification and (c) screening.

2.1 The Existing System

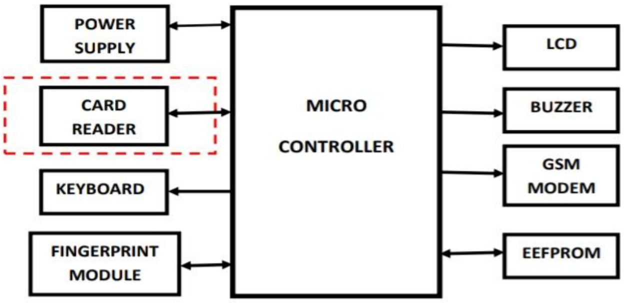
The existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The ATM system compares the PINentered against the stored authorization PIN for every ATM users. If there is a match, the system authenticates die user and grants access to all the services available via the ATM. If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM.



2.2 The Proposed System

The proposed system is an improvement of the existing system, and it does not require card and PIN tooperate. The proposed system work with biometric fingerprint only, the customer uses fingerprint at ATM and ifmatched correctly, then all banks of the customer have account with appears, the customer will select the bankto transaction with, then select the account type with that bank , then chose to withdraw, check account balanceand so on. Customer will now choose or select the bank he wants to withdraw money from and specify if theaccount is Current or Savings, this is a means of securing ATM transaction using biometric fingerprint.This proposed system has a lot of advantages over the existing Card and PIN method as stated follows:

DOI: 10.48175/IJARSCT-3310



2.3 Feasible Study

The essence of this project is taken from various books and journals based on various integrity and security check systems. Various PDF were downloaded via Internet and references. Subject related to the interface study has been done by understanding the .Net, Matlab and SQL server environment and studying the language use to code the logic from the reference guides and taken help from the project guide.

III. System Analysis and Design

- The current banking system is very popular with the feature of offering customers high quality service 24hours a day, but with a low quality security for the transaction
- The traditional method of personal identification number (PIN) at the ATM has stood the test of time, mainly due to its speed and storage, but with greater risk to customers and the bank
- ATM security has often been compromised, hence the need to ensure the operation of ATM transactions using the biometric fingerprint.
- This research proposes to secure transactions at ATMs using a biometric fingerprint. The proposed system is an improvement of the existing system through the use of a biometric fingerprint and a BVN to secure transactions at ATMs.
- The proposed new system will also be profitable as it is based on the existing system

3.2 Flow chart

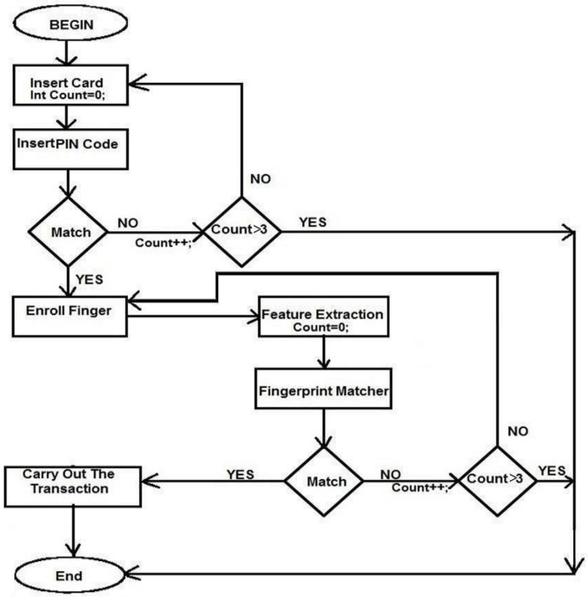
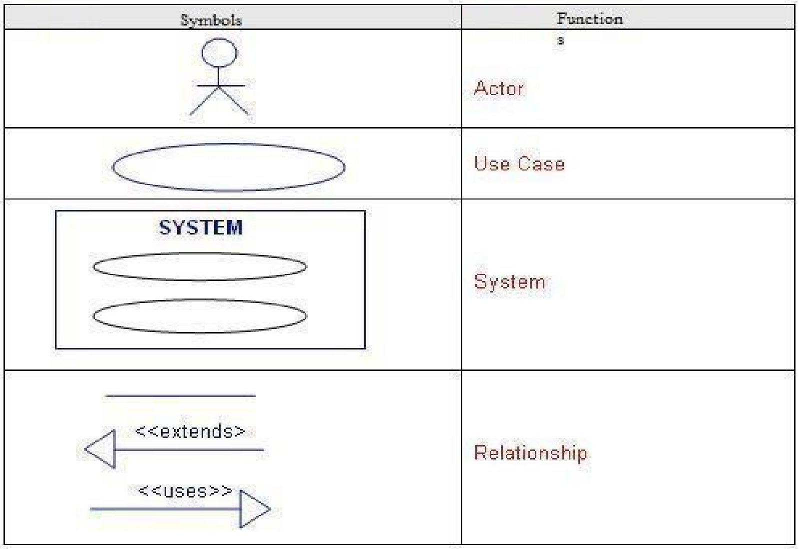


Figure 3.2 Flow chart diagram

3.3 Use Case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system and depicting the specifications of a use case. A use case diagram can portray the different types of users of a system and the various ways that they interact with the system. This type of diagram is typically used in conjunction with the textual use case and will often be accompanied by other types of diagrams as well.



Symbols	Functions
	Actor
	Use Case
SYSTEM	System
<<extends> <<uses>>	Relationship

Figure 3.3: Use Case Symbols & Functions

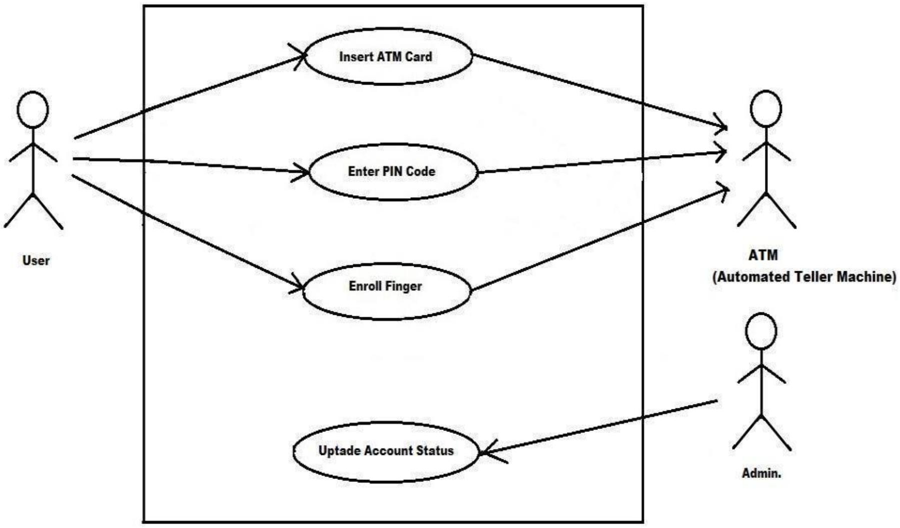


Figure 3.4: Use case diagram

3.4 E-R Diagram

Entity–relationship model (ER model) is a data model for describing a database in an abstract way. In the case of a relational database, which stores data in tables, some of the data in these tables point to data in other tables - for instance, your entry in the database could point to several entries for each of the phone numbers that are yours. The ER model would say that you are an entity, and each phone number is an entity, and the relationship between you and the phone numbers is 'has a phone number'. Diagrams created to design these entities and relationships are called entity–relationship diagrams or ER diagrams.

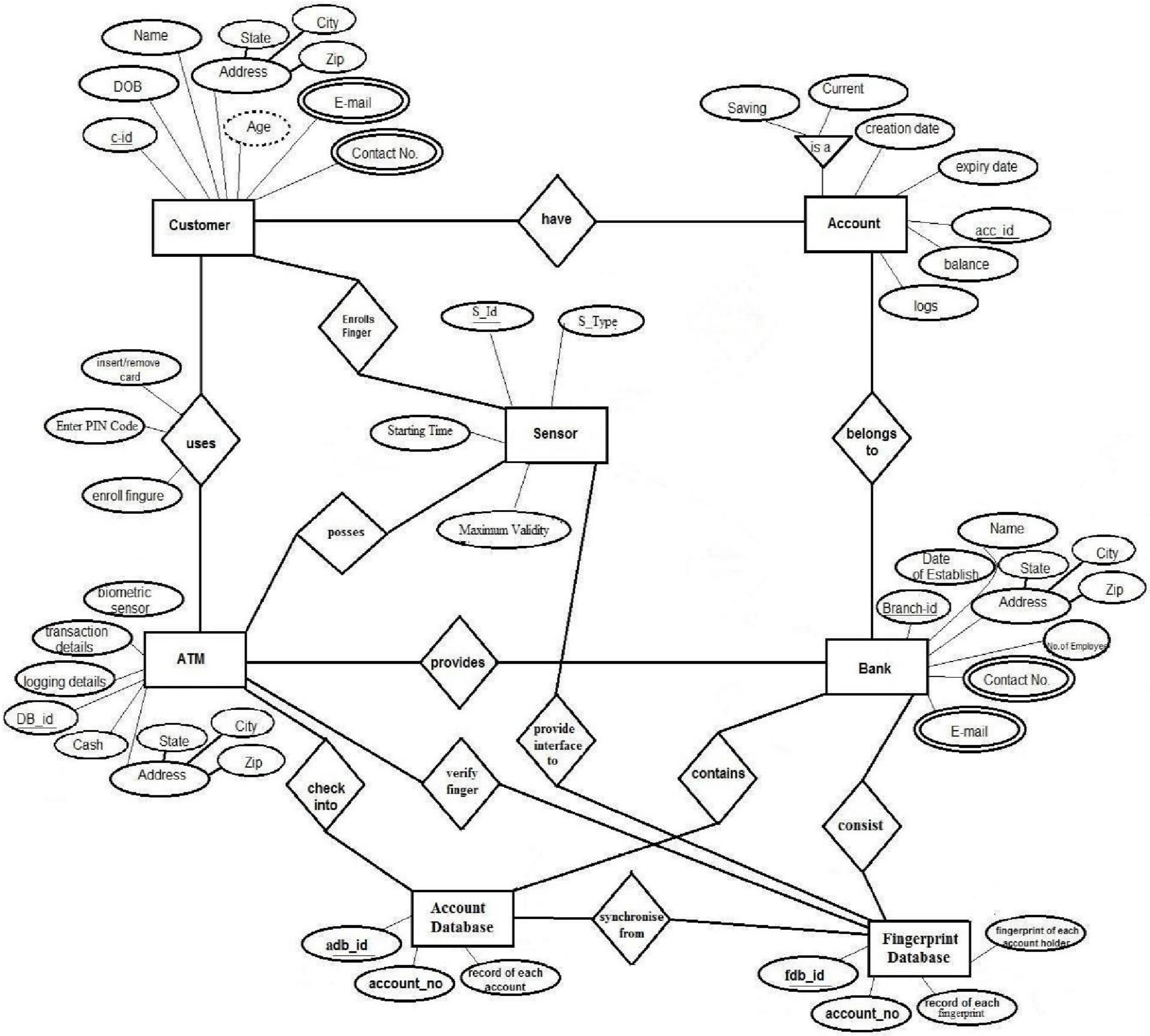


Figure 3.5: Entity Relationship Diagram

3.5 Sequence Diagram

A sequence diagram in a Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development.

DOI: 10.48175/IJARSCT-3310

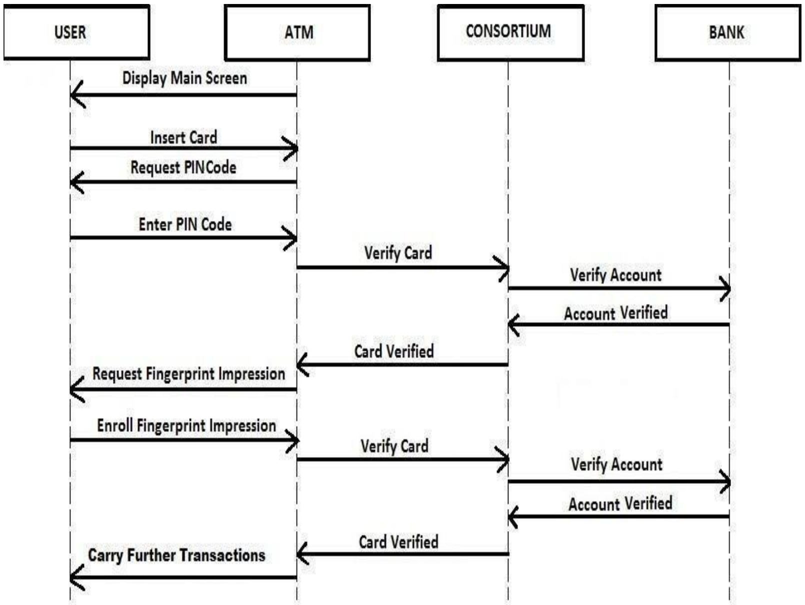


Figure 3.6: Sequence diagram

3.6. Activity diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step by-step workflows of components in a system. An activity diagram shows the overall flow of control.

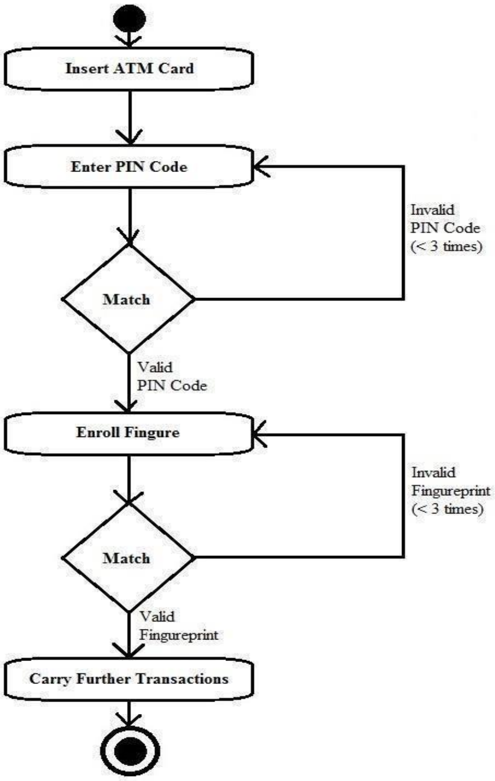


Figure 3.7: Activity Diagram

DOI: 10.48175/IJARSCT-3310

3.7 Data Flow Diagram

3.7.1 Data Flow Diagram Level 0

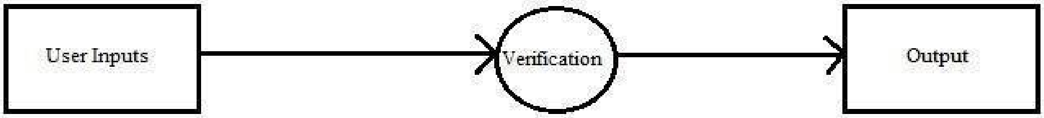


Figure 3.8 DFD Level 0

3.7.2 Data Flow Diagram Level 1

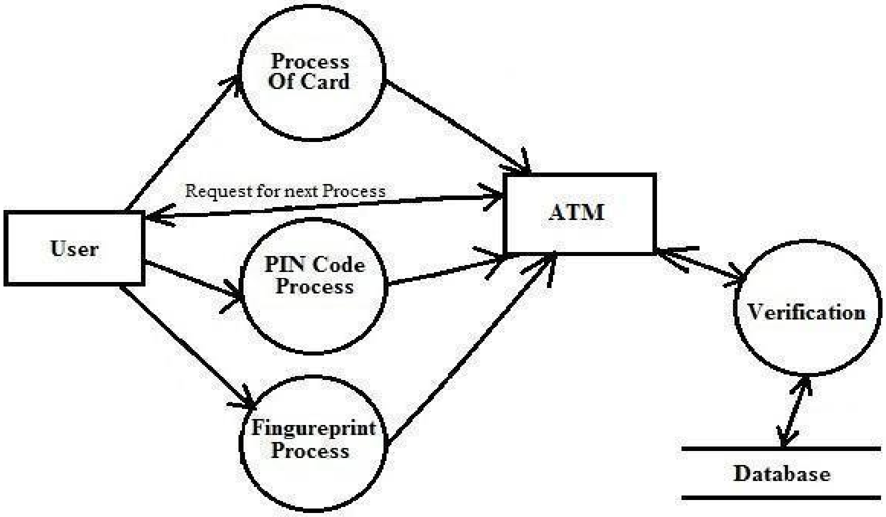


Figure 3.9 DFD Level 1

3.7.3 Data Flow Diagram Level 2

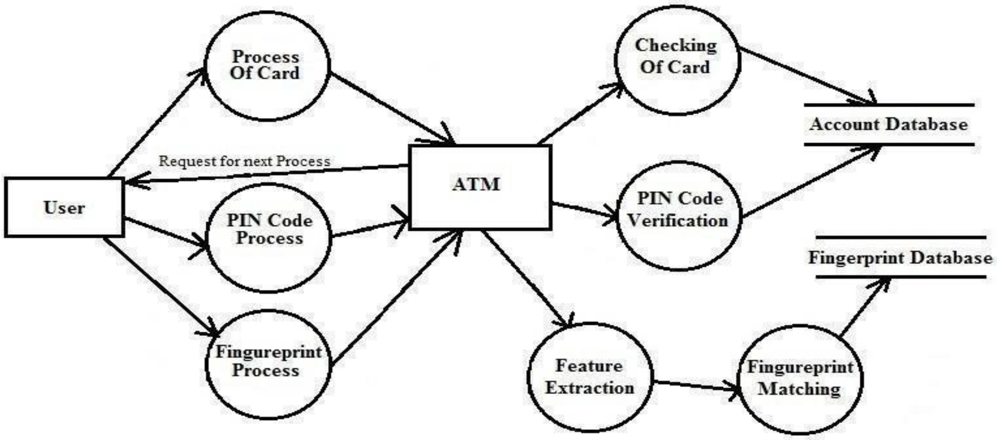


Figure 3.10 DFD Level 2

DOI: 10.48175/IJARSCT-3310

3.8 Methodology

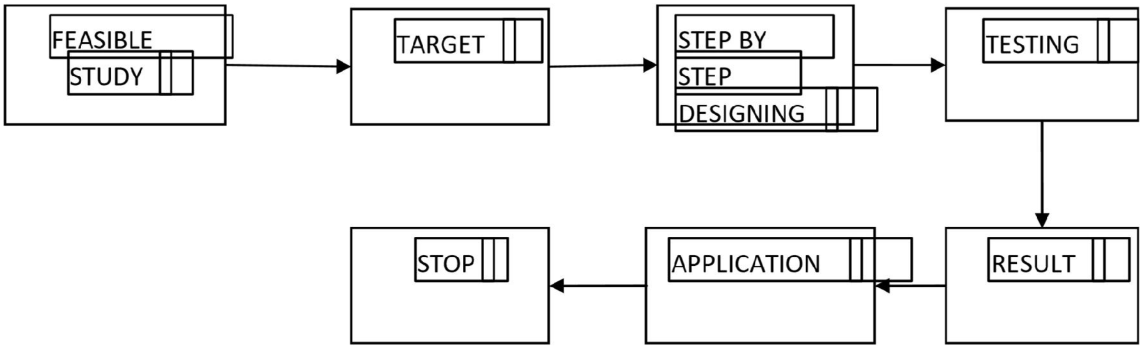


Figure 3.11: Block diagram of Methodology

3.9 Steps Involved In Fingerprint Image Processing

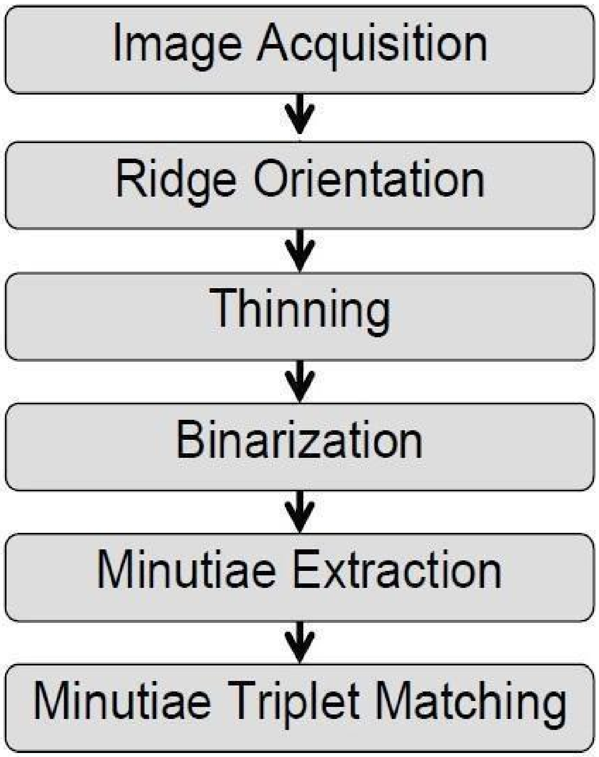


Figure 3.12: Steps of Fingerprint Recognition

3.9.1 Image Acquisition

Image acquisitionis the creation of digital images, typically from a physical scene. The term is often assumed to imply or include the processing, compression, storage, printing, and display of such images. The most usual method is by digital photography with a digital camera, digital pictures with image scanners but other methods are also employed. Here, we are using the digital image for the image processing which will we taken by the image scanners and image sensors.

3.9.2 Ridge Orientation

Ridge orientation is the process of obtaining the angle of the ridges throughout the image. Ridge orientations are calculated on a block-basis for a WxW block, where, W is generally equal to 16 i.e. 16x16 block.

3.9.3 Thinning

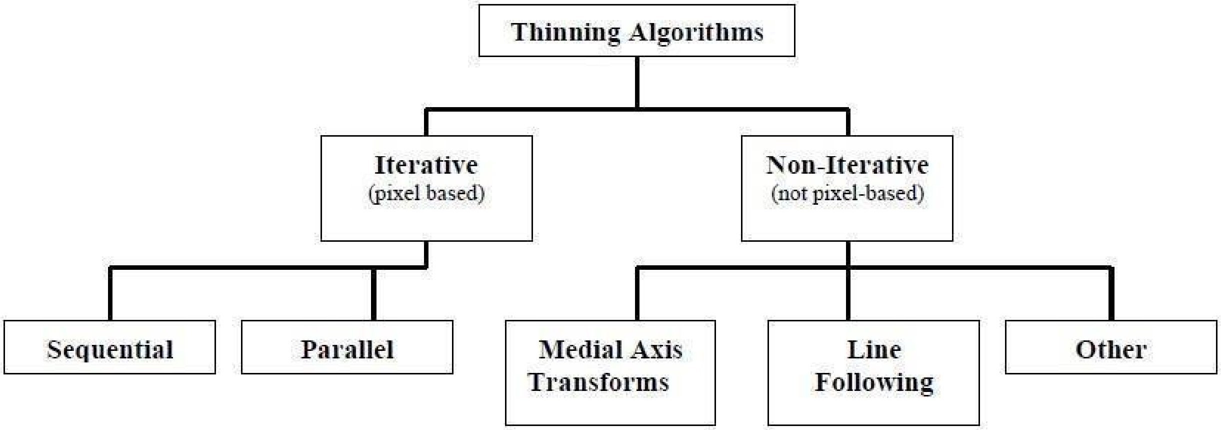


Figure 3.12: Classification Of The Thinning Algorithms

The table above shows a classification of thinning algorithms. The second class of sequential thinning algorithms is parallel. In parallel thinning algorithms the decision for individual pixel deletion is based the results of the previous iteration. Like sequential algorithms, parallel thinning usually considers a 3*3neighborhood around the current pixel. A set of rules for deletion is applied based on pixels in the neighbourhood. Fully parallel algorithms have trouble maintaining connectedness, so they are often broken into sub-iterations where only a subset of the pixels is considered for deletion.

Non-iterative thinning methods are not based on examining individual pixels. Some popular non-pixel based methods include medial axis transforms, distance transforms, and determination of centrelines by line following. In line following methods, midpoints of black spaces in the image are determined and then joined to form a skeleton. This is fast to compute but tends to produce noisy skeletons. It has been conjectured that human beings naturally perform thinning in a manner similar to this.

Another method of centreline determination is by following contours of objects. By simultaneously following contours on either side of the object a continual centreline can be computed. The skeleton of the image is formed from these connected centrelines. Medial axis transforms often use gray-level images where pixel intensity represents distance to the boundary of the object. The pixel intensities are calculated using distance transforms. In Figure below the maximum pixel intensity would increase toward the dark lines at the centres of the circles. Note that there are other methods of computing medial axis transforms. The following is the result of the Thinning algorithm when applied to a binary image:-

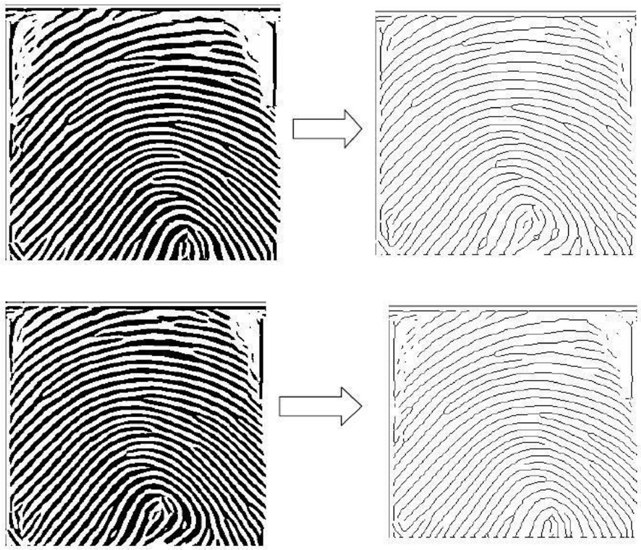


Figure 3.14: Result of thinning algorithm

3.9.4 Binarization

Fingerprint binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs (Figure 5.4).

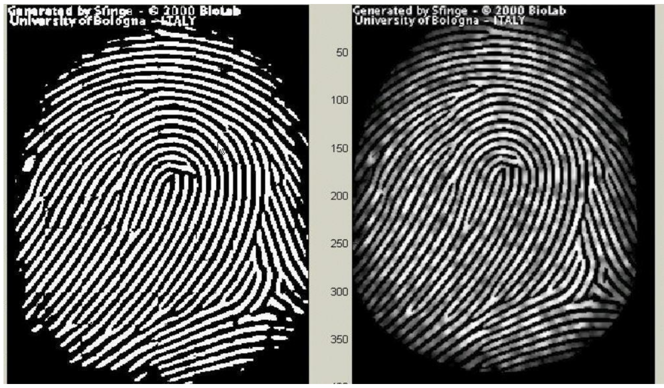

Generated by Sfinge - © 2000 BioLab
University of Bologna - ITALY
Generated by Sfinge - © 2000 BioLab
University of Bologna - ITALY
50
100
150
200
250
300
350

Figure 3.15: The fingerprint image after adaptive binarization binarized image (left), enhanced gray image (right)

IV. Result

The result is being measured by comparing the security components of the ATM system or by matching the PIN-Code and the fingerprint pattern matching which decide the end result of the system.

4.1 Future Work

- Improving of the existing system through the use of a biometric fingerprint to secure transactions at ATMs. This system will also be profitable as it is based on the existing system and thus reduce cost for research work.
- Creating a database of customer biometrics and testing to reduce the time of transaction compared to traditional system.
- Adding a card reader for people who are still using traditional methods.

V. Conclusion

The execution of ATM protection by availing fingerprint also has the traditional verifying methods that were inputting the client's fingerprints, that is sent by the administrator and checked correctly. The protection feature was improved highly for the firmness and solidity of the client's identity. The complete system was constructed on a fingerprint system that makes the mechanism safe, dependable and effortless to avail. This shall be the most favourable technology in electronic or digital money transactions.

References

[1]. Bharti Patil , Bhagwan S. Chandrekar , Mahesh P. Chavan , Bhavesh S. Chaudhri; RBI 3X-Fingerprint Based ATM Machine, IJARCCE Vol. 5, Issue 3, March 2016.

[2]. Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha; Fingerprint Based ATM System: Survey, IJIRSET Vol. 6, Issue 11, November 2017.

[3]. Aruna R, Sudha V, Shruthi G, Usha Rani R, Sushma V; ATM Security using Fingerprint Authentication and OTP, IJERECE Vol 5, Issue 5, May 2018.

[4]. Steffy Mathew, Mohammed Arshak C, Muhammed Ajmal KP, Mohammed Fazil KK, Honey Susan Eldo; Fingerprint Based Security System for ATM, IRJET Volume: 06 Issue: 06 | June 2019.

[5]. URANG Awajionyi S. and Ojekudo Nathaniel A; Securing Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint, AJER Volume-9, Issue-9, pp-36-43.