|  |  |  |
| --- | --- | --- |
|  | **SRI KRISHNA COLLEGE OF TECHNOLOGY**  **An Autonomous Institution | Accredited by NAAC with 'A' Grade**  **Affiliated to Anna University | Approved by AICTE**  **KOVAIPUDUR, COIMBATORE 641042** |  |

#### TITLE of the Project

**A PROJECT REPORT**

***Submitted by***

#### XXXX xxxx

**YYYY yyyyy**

**ZZZZ zzzzz**

*in partial fulfilment for the award of the degree*

Of

#### BACHELOR OF ENGINEERING

**IN**

**xxx**

**JANUARY 2023**



## CERTIFICATE

#### BONAFIDE CERTIFICATE

Certified that this project report **“Title”** is the Bonafide work of **XXXX**, **YYYY** and **ZZZZ** who carried out the project work under my supervision.

SIGNATURE SIGNATURE

XXXXX \_\_\_\_\_\_\_\_\_\_\_\_\_

**HEAD OF THE DEPARTMENT SUPERVISOR**

Professor Assistant Professor

Department of \_\_\_\_\_\_\_\_\_\_\_ Department of \_\_\_\_\_\_\_\_\_\_\_\_

Sri Krishna College of Technology Sri Krishna College of Technology Kovaipudur Kovaipudur

Coimbatore-42. Coimbatore-42.



Certified that the candidates were examined by us in the Project Work viva- voce examination held on ............................... at Sri Krishna College of Technology, Coimbatore -641 042.

**INTERNAL EXAMINER EXTERNAL EXAMINER**



## ACKNOWLEDGEMENT

#### ACKNOWLEDGEMENT

First and foremost, we thank the **Almighty** for being our light and for showering his gracious blessings throughout the course of this project.

We are grateful to our beloved Dean-Academics **Dr. Manju P &** Dean-Administration **Dr R Ramesh Kumar** for their tireless and relentless support.

We extend our sincere thanks to our Head of the Department **­­­\_\_\_\_\_\_** for his/her encouragement and inspiration.

We are greatly indebted to our Industry Mentor \_\_\_\_\_\_\_\_ & Project guide **\_\_\_\_\_\_\_** Assistant Professor, Department of \_\_\_\_\_\_\_\_\_\_\_ for their valuable guidance and suggestions in all aspects that aided us to ameliorate our skills.

We are thankful to all those who have directly and indirectly extended their help to us in completing this project work successfully.

## ABSTRACT

### ABSTRACT

## LIST OF FIGURES

#### LIST OF FIGURES



|  |  |
| --- | --- |
| S.No | Figure Name |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## LIST OF TABLES

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | LIST OF TABLES | **TABLE DESCRIPTION** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |



## LIST OF ABBREVIATIONS

#### LIST OF ABBREVIATIONS

|  |  |
| --- | --- |
| **ABBREVIATIVE** | **ABBREVIATION** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |



***TABLE OF CONTENTS***

**TABLE OF CONTENTS**

**CHAPTER NO.**

**ABSTRACT**

**LIST OF FIGURES LIST OF TABLES**

**TITLE PAGE**

**NO.**

**IV V VI**

**LIST OF ABBREVIATIONS**

**VII**

## INTRODUCTION

### CHAPTER 1 INTRODUCTION

This chapter describes the problem definition and importance of

biometric security through fingerprint authentication in ATM application. The overview of the project is also described.

#### PROBLEM DEFINITION

During the early 1960‘s, people accessed their bank accounts by going to bank tellers for all transactions: deposits, cash withdrawals, money transfers and balance inquiries. The introduction of Automated Teller Machines (ATMs) during the late 1960‘s reduced the overhead of traveling time to banks to make transactions.

An electronic telecommunications device to perform financial transactions without a human cashier‘s need is an Automated Teller Machine [1]. They are made accessible at banks, hotels, gas stations, airports, grocery stores, shopping malls, school campuses or any other public places that promote consumerism.

Debit/credit cards are mainly printed with a unique sixteen-digit number, a three-digit CVV (Card Verification Value) number and an expiration date. To help prevent fraud, card number combinations remain unique and CVV numbers are displayed on the back for additional security. The current ATM systems require users to swipe a debit/credit card to authenticate.

To verify the user‘s identity, existing ATM systems authenticate in two steps: First, swipe the magnetic stripe of the credit/debit card to access account details. Second, enter a four-digit PIN (Personal Identification Number) to unlock the account associated with the credit/debit card‘s chip.

To access an ATM, users stand in front of the machine while those waiting stand in a line a few feet away from the user. The keypads do not have a protective cover, so the clear scope over the user's shoulder allows

on-lookers to decipher the PIN number. A user‘s account is easily accessed if the credit/debit card is stolen and used with the deciphered PIN number.

The objective of this project is to provide biometric security through fingerprint authentication in ATM application. Authentication is a mechanism that makes sure a user is who he claims to be when using a system or data that is sensitive. It confirms the claim of attestation to the identity of a person or a thing. For example, a digital certificate assigned to it by Certificate Authority verifies a website‘s authenticity. Similarly, an ATM authenticates the identity of a user with a PIN number.

Therefore, it is important to protect the PIN number, as it is sensitive

data. Authentication systems must be made strong and transparent.

In summary, there are 2 main problems regarding the use of PIN system:

* + 1. Stealing/duplication of bank card and identification number that leads to ATM fraud.
    2. Users have to memorize their identification number in order to gain access to their accounts.

#### OVERVIEW

Our main focus is to develop a far better security system by using fingerprint-based ATMs. Biometrics may be a technology that helps to form your data extremely securely, unique to all or any of the users by way of their personal physical characteristics. Biometric information is employed to spot the people perfectly by using their fingerprint, face, speech, iris, handwriting, or hand geometry then on. Tokens like mag tape cards, smart cards and physical keys, are often stolen, lost, replicated, or left behind; passwords are often shared, forgotten, hacked or accidentally observed by a third party. There are mainly two key functions offered by a biometric system. one of those techniques is identification and therefore the other is verification. Fingerprint technology is very accepted nowadays and may be a matured biometric technology and is the easiest to develop and for a complicated level of security at the fingertips. it's easy to implement and it might take minimum time and energy to get one‘s fingerprint registered with a fingerprint identification device. Thus, fingerprint recognition is taken

2

into account between the minimum intrusive of all biometric verification methods. During ancient time‘s officials used thumbprints to seal documents thousands of years back, and law agencies have been using fingerprint identification since the late 1800s.We here carry an equivalent technology on digital platforms. Although fingerprint images are initially captured, the pictures aren't kept anywhere within the system. Instead, the fingerprints are converted to templates from the first fingerprints. Not recreate it. Hence, no misusing of the system is possible [1].

Nowadays, the self-service banking system has wide popularization with the characteristic offering excellent 24 hours‘ service for patrons. Using the ATM (Automatic Teller Machine) which might provide customers with convenient banknote trading is extremely common. However, the financial crime case has risen repeatedly in recent years, Lot of criminals‘ tamper with the ATM terminal and steal the user's mastercard and password by illegal means. Once User‘s credit card is lost and therefore the password stolen, the criminal withdraws and takes advantage of the shortest time, which can bring enormous financial losses to the customer. The way to keep it up is the valid identity to the customer as it becomes the main target in Current financial circle. Traditional ATM systems authenticate generally by using the master card and password, the tactic has some defects. employing a master card and password alone cannot really verify the client's identity exactly. within the past few years, the algorithms that are used have fingerprint recognition continuously updated and sending the four-digit code by the controller which has offered the new verification means for us, the first password authentication method is combined with the biometric authentication technology verify the clients' identity better and achieve the aim that use of ATM Machines improve the security effectively [2].

#### OBJECTIVES

The ideology is to propose validation and confirmation measures on the current, ATM machine and to make a fruitful and secure exchange. The fundamental goal of this undertaking is to give a unique mark as an approved character and to plan a safer ATM framework. In this, the ATM machine fills in as when the client places his/her finger on the biometric scanner of the ATM and if the finger coordinate is discovered it will show the name of the client on the ATM machine. If by chance, that Fingerprint coordinate is not discovered, it doesn't permit any exchange. Our remarkable development in our venture is, in prior days if the client



## BIOMETRIC TECHNIQUE

### CHAPTER 2 BIOMETRIC TECHNIQUE

There are many types of biometric measurements. This includes the

behavioural and physiological measures. The author would like to focus on the physiological measures. There are fingerprints, hand geometry, eye scanning (retina and iris), and face recognition. The author will summarize each of the type before making comparison on each of them

#### FINGERPRINTS

Fingerprint identification is the most commonly recognized and most widely applied form of Biometric technology. Fingerprint ID is based upon the fact that a person's fingerprint is completely unique to the individual. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. It is the oldest biometrics method and has already been used for a long time.

#### HAND GEOMETRY

Hand geometry is based on the fact that virtually every person's hand is shaped differently and that the shape of a person's hand (after a certain age) does not significantly change. When the user places a hand on the hand reader, a three-dimensional image of the hand is captured. Then, the shape and length of the fingers and knuckles are measured. Depending on the data used to identify a person, hand reading technologies generally fall into one of three categories - application to the palm, the pattern of veins in the hand and the geometrical analysis of fingers.

#### EYE SCANNING

Eye scanning can be divided into two different fields, which is the iris scanning and retina scanning. Iris is the coloured band of tissue that surrounds the pupil of the eye. An iris recognition system uses a video camera to capture the sample while the software compares the resulting data against stored templates. The retina is the layer of blood vessels at the back of the eye. Retina scans are performed by directing a low- intensity infrared light to capture the unique retina characteristics. An area known as the face, situated at the centre of the retina, is scanned and the unique pattern of the blood vessels is captured.

#### FACE RECOGNITION

Face recognition systems identify an individual by analysing the unique shape, pattern and positioning of facial features. There are essentially two methods of processing the data: video and thermal imaging. Standard video techniques are based on the facial image captured by a video camera. Thermal imaging techniques analyse the heat-generated pattern of blood vessels underneath the skin. There are various recognition methods that emphasize identification based on the areas of the face that don't change, including upper sections of eye sockets, area surrounding cheek bones and sides of mouth

In the past, fingerprints were recorded by the application of ink to the finger which was then pressed to paper to give an impression. Fingerprints have been used as human identification long ago. People are familiar with it-and they trust it. Hand geometry is even older than digital fingerprinting; it was first used for security purposes on Wall Street more than 20 years ago. However, in Malaysia, the idea of hand scanning is not very popular compared to fingerprints.

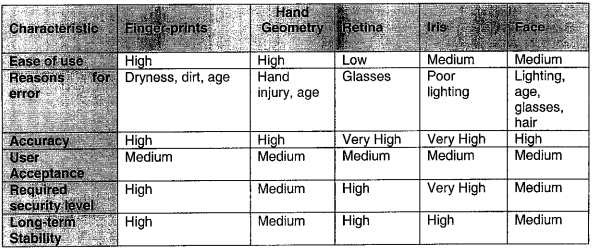
Retina biometrics is considered to be the best biometric performers. However, despite its accuracy, this technique is often thought to be inconvenient and intrusive. The retinal scan, according to some studies, is more expensive and less "user-friendly" than fingerprinting. The fact that it requires the user to place their eye near a scanning device, which then reads blood vessel patterns unique to each person, is often a cause of discomfort. The retinal scanner requires an individual to stand still while it scans the unique patterns of the retina with a low-intensity light source.

By contrast, iris scanning uses a camera and requires no intimate contact with the reader; reading the retinal information. Eye and retinal scanner are ineffectual with the blind and those who have cataracts.

However, it is difficult to gain general acceptance by the end user. Some are suspicious and don't want any of their physical features saved on some database. They are frightened of iris and retinal recognition because they believe a laser will scan and thus damage their eyes. Cost is another thing that makes banks reluctant to deploy eye biometrics on a broad scale.

Facial recognition, which compares a user's facial characteristics with the stored results of an algorithm calculation (similar to a data hash), offers the ultimate security. Some systems match two static images, and others claim to be able to unobtrusively detect the identity of an individual within a group. But facial recognition has had only very limited success in enterprise applications, such as access to nuclear facilities, because of its cost and complexity. The attraction of this biometric system is that it is able to operate 'hands=free', limiting the amount of man-machine interaction. However, this system is highly unreliable and expensive. For example, it will not distinguish twins or triplets, not recognize the user after a haircut, and not recognize a person who changes from wearing and not wearing glasses.

Although many parts of the human body can provide data for electronic identification, users remain most comfortable offering their fingertips. Fingertip scanners are the most commonly used form of biometrics - and the least expensive and easiest to deploy —but not all scanners are the same. Some match the ridges in a thumbprint, others are straight pattern-matching devices, and still others take unique approaches such as ultrasonic. Here are more comparisons between the biometric measurement that the author taken from **IT Professional** (January/February 2001)



#### Fig 2.1. Comparison of Biometrics

From the analysis and comparisons between the biometric measurement, it gives the conclusion that accuracy, convenience (of user acceptance) and cost is among the main criteria in choosing which biometric measurement should be implemented in a particular system. The author thinks that fingerprint biometric is most suitable for ATMs because it has high accuracy, and can generally be accepted by users because it is convenient and many people are familiar with it. Moreover, the cost for the devices is affordable.

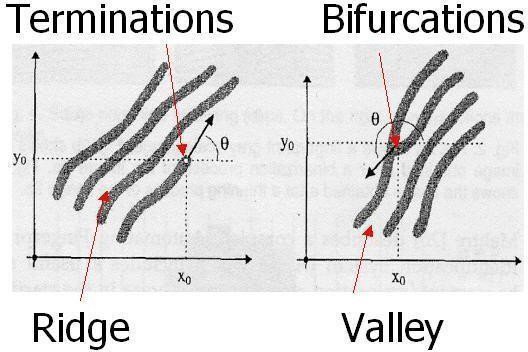
#### WHAT IS A FINGERPRINT?

A fingerprint is the feature pattern of one finger (Figure 2.2.1). It is believed with strong evidence that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have been used for identification and forensic investigation for a long time.



#### Fig 2.2.1 Finger Pattern

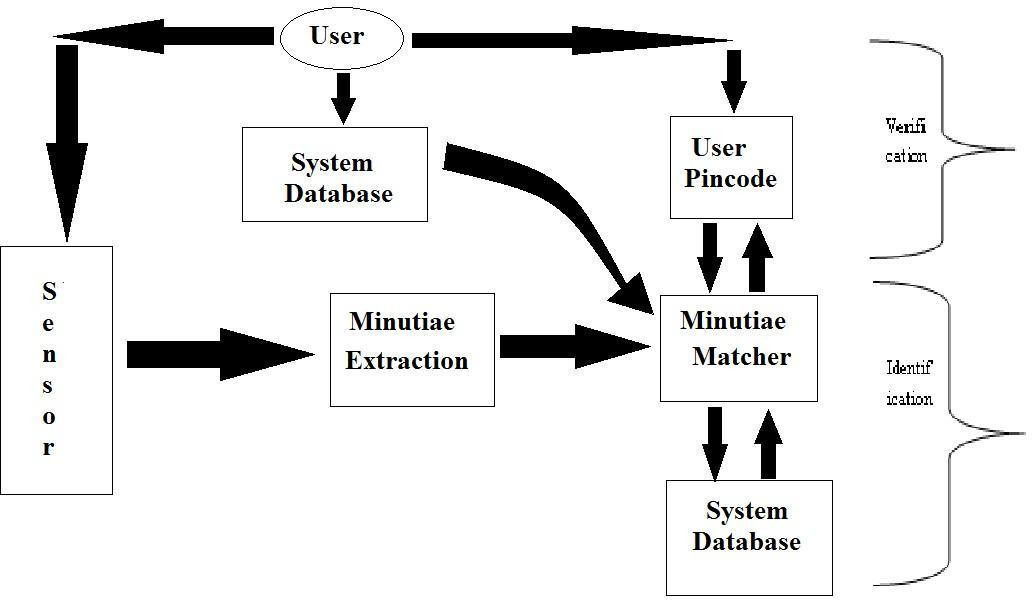
A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges (Figure 2.2.2). Among the variety of minutia types reported in literature, 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.



#### Fig 2.2.2 Minutia (Valley is also referred as Furrow, Termination is also called Ending, and Bifurcation is also called Branch)

* 1. **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 2.3.1). 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.



#### Fig 2.3.1 Verification vs. Identification

* 1. **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 current 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.



## LITERATURE SURVEY

### CHAPTER 3 LITERATURE SURVEY

The word ―biometrics‖ derived from the Greek words ―bios‖ and

―metric‖ which suggests life and measurement respectively [3]. To implement this idea, we‘ve studied different investigated works and located the following data. Most finger-scan technologies based on minutiae. The downside of pattern matching is that it‘s more sensitive to trueness of the finger during verification and the created template is several times larger. For fingerprint recognition, a system must capture a fingerprint then follow a certain algorithm for fingerprint matching. This paper discusses a minutiae detection algorithm to show key parameters of fingerprint image for identification. The maturity of Biometric techniques and typically the dramatic improvement of the captured devices have led to the proposal of fingerprinting in multiple applications but within the last years, minutiae are the main quiet algorithm used [4]. Biometric data separated and distinct from personal information.

They‘re going to not be stolen and accustomed access personal information to solving the bugs of traditional identification methods the author of designs a replacement ATM terminal customer recognition system is used for the core of microprocessor and an upgraded enhancement algorithm of fingerprint image intensify the security of bank accounts also as ATM machines [5]. Miaoetal proposed the Gabor filters (GFs) play an important role within the extraction of Gabor features and thus the enhancement of various sorts of images. Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the foremost important [6]. If images of fingerprint are shoddy images, they end in missing features, leading to the degrading performance of the fingerprint system. Hence, it is vital for a fingerprint recognition system to gauge the quality and validity of the captured fingerprint images [7].

To have a good process of operation for fingerprint matching, in counting on the spectral details features two feature reduction algorithms given the Column Principal Component Analysis and the Line Discrete Fourier Transform feature reductions. Biometric templates can‘t be reverse-engineered to recreate personal information which they cannot be stolen and accustomed to access personal information [8]. Fingerprint records usually reach impressions on the last joint of the fingers and thumb, to the extent that fingerprint cards typically record parts of the lower finger areas of the fingers [9]. Among those new technologies for handling payment processing, biometric payment technology has recently attracted more and more attention as a viable solution to decrease identity theft [10]. It‘s visiting be historical, current or theoretical.

samples of electronic money are bank deposits, electronic funds transfer, direct deposit, payment processors, and digital currencies. Electronic money is often understood as how of storing and transmitting conventional money through electronic systems or as digital currency, which varies in value and is tradable as a currency in its title. Electronic money transfer at an ATM is additionally a certificate of indebtedness device that‘s stored on an electronic or remote device within the protection of the server. On the other hand, electronic security is any tool, method or process accustomed to protect system information assets. Information could even be a valuable strategic asset that‘s managed and guarded accordingly. This insurance could even be a risk management or risk mitigation tool, and appropriate safety measures mitigate the danger of underlying transactions commensurate with its value [10].

#### ATM FRAUD - TECHNICAL ATTACK ON PIN KEY

For decades, people had used a personal identification number (PIN) to protect against fraud and effectively eliminate most common attempts to gain unauthorized access. However, with the rapid changes in technology, we can't keep relying on identification numbers as a security means to our privacy. ATM fraud is one of the crimes that results from an inappropriate way of handling PIN. A corrupt bank employee can discover your debit card pin number after just 15 attempts, according to a study by computer scientists in Cambridge.[1]

In most cases withdrawals go without a hitch but ATM fraud has started to be a growing nuisance. This type of fraud, including use of

stolen cards at ATMs, has grown from €8.2 million in 1997 to €21.2

million in 2001, representing about 5% of all card fraud.

Two years ago, it was a London problem but it has now spread all over the country. Sandra Quinn of the Association of Payment Clearing Services (APACS) says that more recent figures are due soon and they are expected to show a sharp jump in ATM fraud.[2]

In the United Kingdom, the ATM scam uses different tactics to steal money from ATM users. The scam, called the Lebanese Loop works like this: A plastic or metal sleeve is constructed that fits into the card slot of an ATM machine. When the next unsuspecting customer arrives to withdraw money, the card is caught in the sleeve and doesn't completely enter the machine. You will get the screen asking you to enter your PN number, but no matter how many times you enter the number nothing else happens. This gives a thief, standing behind you, plenty of opportunity to see you punch in your pm. After you give up the thief uses a small tool to pull out the sleeve with your card and promptly withdraws the maximum cash from your account. [3]

ATM fraud has become more sophisticated with cracking programs to steal ATM holders' money very easily. The newest device for stealing information is a thin, transparent-plastic overlay on an ATM keypad that captures a user's identification code as it is entered. To the card holder, it might look like some sort of cover to protect the keys. In fact, microchips in the device record every keystroke. Another transparent device inside the card slot captures card data. While the cardholder completes the transaction, a computer attached to the overlay records all the data necessary to clone the card. [4]

Another method used is to distract us by spilling a drink over us or doing something like dropping a E 10 and asking who owns it. While distracted, they will nab your cash or card or both, having already surfed your shoulder to get your PIN number. Sometimes those using the distraction method will take your card and quickly skim it through a machine in order to make a copy. The card is then returned to the machine, with the user being none the wiser. [2]

The newest device for stealing information is a thin, transparent- plastic overlay on an ATM keypad that captures a user's identification code as it is entered. To the card holder, it might look like some sort of cover to protect the keys. In fact, microchips in the device record every

keystroke. Another transparent device inside the card slot captures card data. While the cardholder completes the transaction, a computer attached to the overlay records all the data necessary to clone the card. [5]

The secrecy of the key, although necessary, is not sufficient. This is illustrated by a famous fraud, which took place at the Chemical Bank in New York in 1985. An ATM technician, who had been fired, would stand in line and watch a customer keying in his PIN. He would then pick up the discarded receipt, which contained the account number, write this number to the magnetic strip of a blank card, and use this with the observed PN to raid the poor customer's account. He managed to steal over $80,000 before the bank saturated downtown New York with security men and caught him in the act. Needless to say, the emergence since then of worldwide ATM networks makes such attacks much easier to do, and extremely difficult to stop. [6]

With all the drawbacks, passwords and personal identification numbers (PINs) soon may become relics of our computer past as biometric identification technology takes over the critical task of identifying and authenticating computer users, and permitting access to secure sites, files and Intranets.[7]

#### FUTURE DIRECTION — THE IDEA OF BIOMETRIC ATM

According to Roberto Torres, Frost & Sullivan automatic identification industry research analyst, "The underlying driver in the commercial arena is the business community's search for tools which can prevent fraud. Problems stemming from false identification of individuals have seriously hurt the financial industry, government agencies and business establishments for decades."

Biometrics is an old Greek word for a very new concept. "Bio," meaning life, and "Metric," the measure of, so Biometrics is in essence, the measure of life. Biometrics is an emerging technology for automatically identifying individuals using their distinct physical or behavioural characteristics. Types of Biometrics can be any unique human characteristics, such as fingerprint, voice, face, iris, retina, palm, signature, wrist vein, and hand geometry. Biometrics provides a better solution for the increased security requirements of our information

society than current identification methods (passwords, numbers and magnetic strip cards with a PN number) for various reasons: the person to be identified must be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password (or write it on a yellow sticky note), PIN or carry a token. Using biometric systems to identify the user of a computer, ATM, cellular phones and even credit card purchases will reduce fraud and unauthorized access. This could save the economy billions of dollars. [6] Mark Radke of Diebold, one of the biggest ATM manufacturers in the United States, says the emergence of biometrics has been slow in part because of the technology and partly due to slow overall acceptance by the public. But that's changing, he says, to the point where credit unions, which have been more aggressive than banks about using biometrics, see the new technology as a customer draw. [5]

"Banks realize biometrics are not something to be ignored," says Jennifer Schmidt, a Meridien Research analyst and author of a study on biometrics in financial services institutions. Biometrics provide a unique advantage over other forms of security, such as user name and password, in that an individual's biometrics print is one-of-a-kind. Whether it's the pattern of blood vessels in the eye or the long-familiar thumbprint, no one else in the world has the same measurable characteristic. [8]

Bank United became the first US bank to trial a biometric-enabled Diebold ATM at three of its branches using iris technology from Sensar in the spring of 1999. The bank's customers gave positive feedback to the trial, with 98 per cent of those surveyed saying that they would like to see more machines installed locally. However, Bank United has yet to install any further machines. UK building society Nationwide became the first organisation worldwide to trial iris recognition technology supplied by NCR back in 1998. The results of the pilot were very positive for the customer, with 94 percent saying they were comfortable with the technology and 91 percent saying they would choose iris identification in future above either PINs or signatures. [2]

Citibank is looking into the feasibility and cost of using biometrics technology as a more efficient and secure method of identifying its customers. Meanwhile, Huntington Bancshares is studying the impact of identity theft and fraud with a close eye on biometrics as a possible approach to reducing the chronic problem. Tom Connaughton, managing director of risk management at Citibank North America, in New York,

said his company wants to be a leader in extending biometrics technology to customers, providing them with several types of identification options, such as fingerprint and facial-recognition technologies, so they can choose which one they're most comfortable with. Having customers use biometrics to gain access to accounts is the only way for the bank to know for sure whom they're dealing with, Connaughton said. [9]

Bill Rogers, publisher of Biometric Digest, says things should change now that some major corporations are getting behind biometrics. "Microsoft has committed to putting biometrics in a future release of Windows. Compaq Computer has built a PC with a fingerprint scanner built into the keyboard. Visa, MasterCard and Discover are doing pilot projects where your fingerprint is put into the bar code, the merchant drops the card into the reader, you put your finger on a scanner and they know the card is yours. Once the credit card companies and Microsoft or the hardware manufacturers make them part of the standard system, it'll move faster." [5]

There is a good chance that biometric authentication and verification will become more commonplace in the near future. Enterprise implementations and specialized applications such as ATMs are more likely to use biometric as an alternative. The potential of this growing technology could not be ignored since it may become one of the most anticipated technologies to ensure that human's security and privacy are well protected.

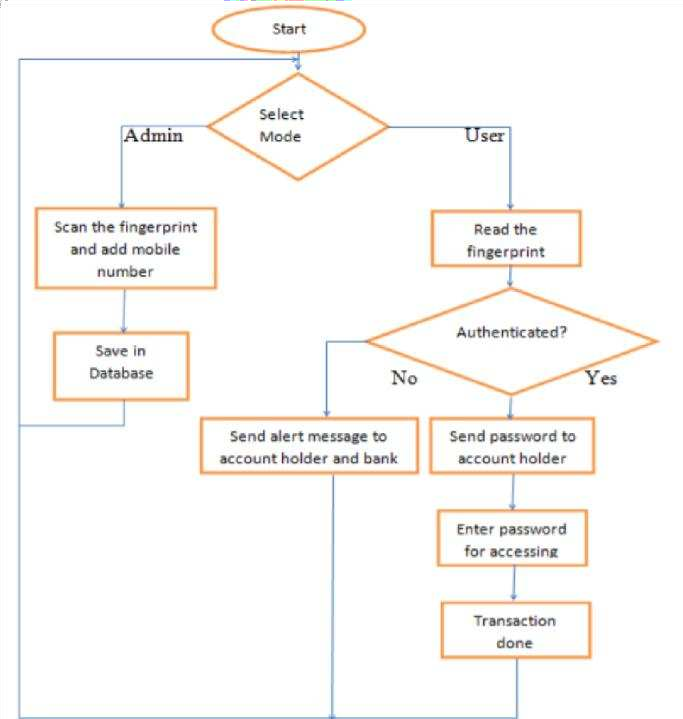


# PROPOSED SYSTEM

### CHAPTER 4 PROPOSED SYSTEM

The proposed system to increase safety and security by introducing a fingerprint system. The advantage of finger-scan technology is accuracy. By using the fingerprint system many disadvantages are rapidly reduced. They do not have the need to carry an ATM card in your wallet and no chance of loss card, CARD can be stolen, password can be shared or, hacking all customers are satisfied by our system because of quick and better service.

Moreover, initially Fingerprint is converted into string values that are stored in the EC2 database. Every user's fingerprint is stored as a string which means every string is unique. All the strings are stored in a vast cloud memory, when a user withdraws his money, he places his finger print, then that unique string is being searched in the cloud and the authentication process takes place.



#### Fig.4.1. Flowchart for ATM fingerprint

#### ADVANTAGES

* + - Fingerprint based ATM System is more secure than ATM card.
    - User can make transaction using his fingerprint any place and at any

time, he need not have to carry an ATM card.

* + - User can transfer money to various accounts by mentioning account

number in case of emergency.

* + - The system can be used in various Banks.
    - Low educated people can access it easily.
    - When our ATM card is misplaced then no one uses or access it. It

automatically blocks.

* + - No one can hack the pin code. The hackers can easily guess the 4-

digit pin code



***METHODOLOGY DETAILS***

### CHAPTER 5

**METHODOLOGY DETAILS**

Unique mark confirmation is to check the realness of one individual by his finger impression and PIN code and Fingerprint distinguishing proof is by coordinating the data of the client, for example, pin code and unique mark coordinating. Essentially, we can clarify total Fingerprint based ATM framework in two stages:

* Enrolment Phase
* Authentication phase

#### Enrolment phase:

In the robust fingerprint application, up to 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 biometric reference data is collected for enrollment and stored in a database or in portable data carrier such that 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 to enrol more than one finger. During daily life injuries can happen that turn a registered fingerprint currently unusable while minor cuts do not affect a robust sized sensor system.

#### Authentication Phase:

In this phase users can make transactions by using their fingers. User can place a 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 a biometric scanner and get their money in a few seconds. If a user's fingerprint cannot match by 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 conveniences. Feature extraction: The feature extraction process from a fingerprint image is generally categorized into three levels. Feature can be used to categorize into major pattern types such as loop or whorl.

#### EQUIPMENT AND METHODOLOGY Fingerprint sensor:

For thedevelopment of the ATM,R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high- performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software‘s compositions, stable performances, simple structures, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions

**Raspberry Pi 3RPig:**

low cost, small credit-card sized computer. RPi3 is faster than Arduino

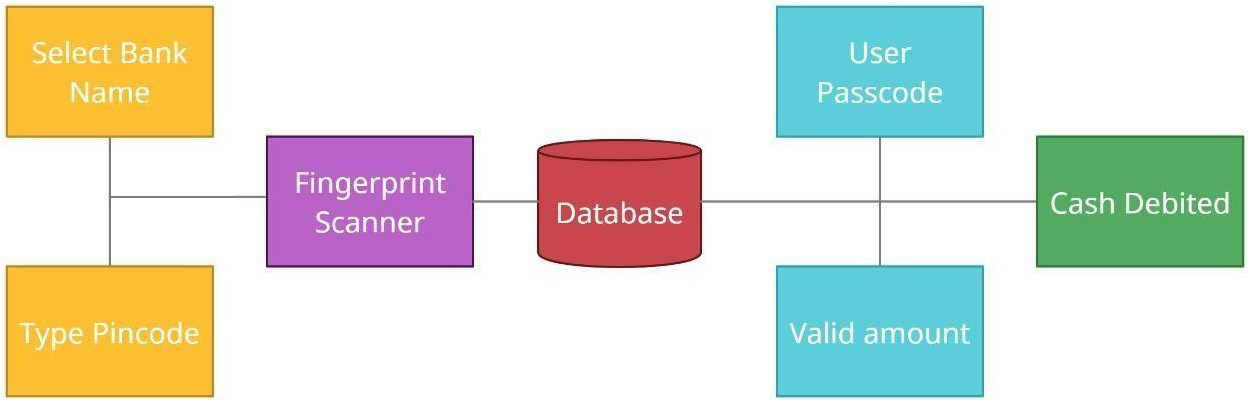
**Cloud server and Fingerprint processing:**

Host server is AWS EC2. Date, time, message status, ID, sensor value and also Fingerprint is converted into string value and stored in the EC2 database. Every user's fingerprint is stored as a string. Which means every string is unique? All the strings are stored in a vast cloud memory, when a user withdraws his money, he places his finger print, then that unique string is being searched in the cloud and the authentication process takes place.

**Software Role:**

21

The authentication process is done by a few simple steps for all users. First the basic details which comprises State, district and branch are being selected to make it fast and easy for the software to search the desired string (to verify the fingerprint). Then the verification takes place within a few seconds and the money can be withdrawn.



#### Fig.5.1. Diagram for Fingerprint based ATM

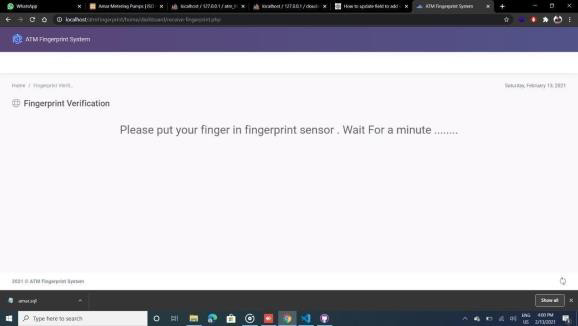


***IMPLEMENTATION AND RESULT***

**CHAPTER 6 IMPLEMENTATION AND RESULT**

* 1. **FINGERPRINT SYSTEM WELCOME MODULE**

In this research, we are mainly concentrated on the end user and a poor literacy people. In this way we created a simple login page. Using this login page, we have two options: they are going to use the option card and fingerprint (Fig.6.1).



#### Fig.6.1 Fingerprint system welcome module

#### FINGER PLACING MODULE

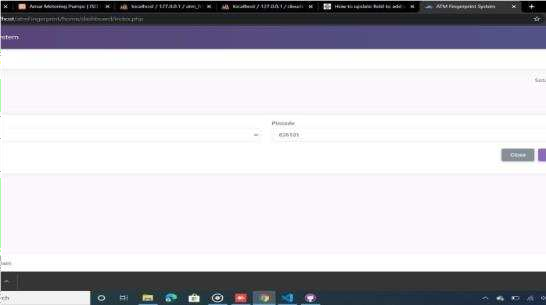
The customer wants to use the card option he or she should select the particular option. Otherwise, he/she wants to select another option for the fingerprint



#### Fig.6.2. Finger placing module

#### PIN NUMBER FEED MODULE

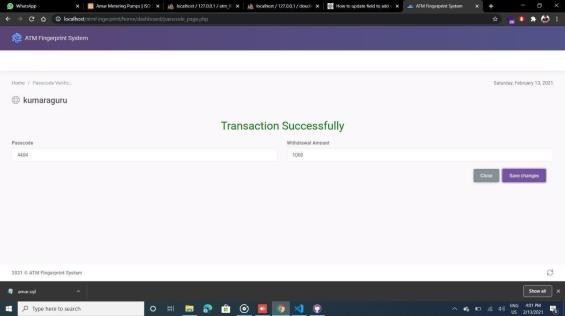
After selecting the fingerprint, the user has to place his or her finger in the scanner to verify identity (Fig.6.2). In this step the user‘s fingerprint will be identified with the help of a fingerprint scanner.



#### Fig.6.3. Pin number feed module

#### TRANSACTION SELECTION MODULE

After the second step, the next step is the most important step. In this step the customer has to enter the pin number correctly (Fig.6.3). In this step all the customer has a security pin number given by the bank. If the customer enters the security pin number correctly and clicks on submit, the customer can do the further activities. If the customer enters the wrong pin number, it will allow entering it three times. If the pin number exceed more than three times, the ATM card



#### Fig.6.4. Transaction selection module

* 1. **SURVEY OF FINGERPRINT WITH OTHER BIOMETRICS**

The following module is as usual banking system account selection and transaction selection module. In this step, his or her transaction will be on their decision. We have three options. First one is to check their balance, next is to withdraw cash from their account, and the last is to transfer cash from one account to another account and the transaction is completed successfully. (Fig.6.4).

The advantages of enhancing ATM security using fingerprints are Low educated people can access it easily. When our ATM card is misplaced then no one uses or accesses it, it automatically blocks, no one can hack the pin code. The hackers can easily guess the 4digit pin code. Crimes which are happening in ATMs become a serious issue that affects not only customers but also bank operators. Number of the population is still skeptical about using ATMs because of the issues associated with it, Fingerprint technology is the most widely accepted and mature biometric method and is always the easiest to deploy and for a higher level of security at your fingertips.

#### ALGORITHM

**Step 1:** User wants to enter the corresponding bank name and pin code of that bank.

**Step 2:** Scan the fingerprint value and pass along with the bank name and pin code.

**Step 3:** Check whether the user is valid or not by using ajax with MySQL database.

**Step 4:** If the user is valid then it moves to the transaction page else it moves back to the index page.

**Step 5:** If the user enters the valid password and valid amount the amount will be debited or else it shows the error message.

**Step 6:** Check whether user given data is valid or not by using ajax with MySQL database.

**Step 7:** If all the data is correct, the user can debit the amount.

#### SAMPLE CODE

#### PASSWORD CHECK

function passcodeCheck() { var obj = {

"atm\_bank\_select\_name": $('#atm\_bank\_select\_name').val(), "atm\_bank\_input\_pincode\_number":

$('#atm\_bank\_input\_pincode\_number').val(),

"fingerPrintValue": $('#atm\_bank\_input\_fingerprint').val(), "atm\_bank\_input\_passcode\_number":

$('#atm\_bank\_input\_passcode\_number').val(), "atm\_bank\_input\_withdrawal\_amount":

$('#atm\_bank\_input\_withdrawal\_amount').val()

}

if ($('#atm\_bank\_input\_withdrawal\_amount').val() % 100 == 0 && $('#atm\_bank\_input\_withdrawal\_amount').val() <= 20000) {

var saveData = $.ajax({ type: 'POST',

url: "../../app/model/users/amount\_withdrawal.php", data: obj,

success: function(resultData) {

var result = JSON.parse(resultData);

if (result.statusPasscode && result.statusAmount) {

$(".valid\_amount").hide();

$(".show\_passcode\_failure").hide();

$(".show\_amount\_failure").hide();

$(".show\_success").show(); setTimeout(function() {

window.location.replace("index.php");

}, 3000);

} else if (!result.statusPasscode) {

$(".valid\_amount").hide();

$(".show\_success").hide();

$(".show\_amount\_failure").hide();

$(".show\_passcode\_failure").show(); setTimeout(function() {

window.location.replace("index.php");

}, 3000);

} else if (!result.statusAmount) {

$(".valid\_amount").hide();

$(".show\_passcode\_failure").hide();

$(".show\_success").hide();

$(".show\_amount\_failure").show(); setTimeout(function() {

window.location.replace("index.php");

}, 3000);

}

}

});

} else {

$(".valid\_amount").show();

}

}

#### FINGERPRINT CHECK

function fingerprintCheck(fingerprintValue) { var obj = {

"fingerPrintValue": fingerprintValue, "atm\_bank\_select\_name": $('#atm\_bank\_select\_name').val(), "atm\_bank\_input\_pincode\_number":

$('#atm\_bank\_input\_pincode\_number').val()

}

var saveData = $.ajax({ type: 'POST',

url: "../../app/model/users/receive\_fingerprint\_auth.php", data: obj,

success: function(resultData) {

var result = JSON.parse(resultData); if (result.status) {

$('#atm\_bank\_input\_user\_name').val(result.username); document.getElementById("myForm").submit();

} else {

window.location.replace("index.php");

}

}

});

}

$(document).ready(function() {

$(".show\_success").hide();

$(".show\_failure").hide();

$("#paragraph\_hide").show(); setTimeout(function() {

var fingerprintValue = 2; if (fingerprintValue) {

clearTimeout(myVar);

$("#atm\_bank\_input\_fingerprint").val(fingerprintValue); fingerprintCheck(fingerprintValue);

} else {

console.log("failed");

}

// if(obj.fingerprint\_value == 1){

// clearTimeout(myVar);

// $("#paragraph\_hide").hide();

// $(".show\_success").show();

// }else if(obj.fingerprint\_value == 2){

// clearTimeout(myVar);

// $("#paragraph\_hide").hide();

// $(".show\_failure").show();

// }else{

// clearTimeout(myVar);

// $("#paragraph\_hide").hide();

// $(".show\_failure").show();

// window.location.replace("index.php");

// }

}, 1000);

myVar = setTimeout(function() { window.location.replace("index.php");

}, 12000);}

## CONCLUSION AND FUTURE SCOPE

#### CHAPTER 7

**CONCLUSION AND FUTURE SCOPE**

The implementation of ATM security by using fingerprint also contains the Original verifying methods, which were inputting customer fingerprints, which is sent by the controller and verified properly. The security feature was enhanced largely for the stability and the reliability of owner recognition. The whole system was built on fingerprint technology, which makes the system safer, reliable and easy to use. This will be the most promising technology in electronic money transactions.

#### 7.1 FUTURE SCOPE

In future, we can add face recognition features in this current system using image processing in which we can use open CV software using python language, which gives higher accuracy in face recognition and some other algorithms.

Also, we can add some sensors like a tilt sensor which is used to alert about the robbery of cash from the ATM. As in the current system, we are entering the less no. of the fingerprint of persons but in future, we can increase this count.

#### REFERENCES

1. Pranali Ravikant Hatwar and Ravikant B Hatwar, ―BioSignal based Biometric Practices‖, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.
2. Edmund Spinella, ―Biometric Scanning Technologies: Finger, Facial

and

Retinal Scanning‖, Available at:

[https://www.sans.org/readingroom/whitepapers/authenticati](http://www.sans.org/readingroom/whitepapers/authenticati) on/ biometric-scanningtechnologies-finger-facial-retinal-sca nning-1177.

1. Gu J, Zhou J, Zhang D.A combination model for orientation field of

fingerprints. Pattern Recognition, 2004, 37:543-553.

1. N. Selvaraj and G. Sekar, ―A Method to enhance the safety Level of ATM banking industry using AES Algorithm‖, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010.
2. T.C. Glaessner T. Kellermann and V. McNevin, ―Electronic Security: Risk Mitigation in Financial Transactions: Public Policy Issues", Working Paper, World Bank Publications, pp. 3-5, 2002.
3. B. Richard and M. Alemayehu ―Developing E-banking Capabilities

during a Ghanaian Bank: Preliminary Lessons‖ Journal of Internet Banking and Commerce, Vol. 11 and 12, No. 2, pp. 1-6, 2006.

1. J. Yang N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon,

S. Xie and Y. Yang ―A Fingerprint Recognition Scheme supported Assembling Invariant Moments for Cloud Computing Communications‖, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.

1. J. Leon G. Sanchez G. Aguilar, L. Toscano, H. Perez and J.M. Ramirez, ―Fingerprint Verification Applying Invariant Moments‖, Proceedings of IEEE International Midwest Symposium on Circuits and Systems, pp. 751-757, 2009.
2. LO Gorman ―Overview of Fingerprint Verification Technologies‖,

Information Security Technical Report, Vol. 3, No. 1, p. 21-32, 1998.

1. G.B. Iwalokun O.C. Akinyokun, B.K. Alese and O. Olabode "Fingerprint Image Enhancement: Segmentation to Thinning", International Journal of Advanced computing and Applications, Vol. 3, No. 1, pp. 15-24., 2012.

x