American International University-Bangladesh
(AIUB)

Fingerprint-based biometric system in ATM banking (Conceptual Model)

Ariful Islam (18-37545-1)
Fardin Ahmed (18-39264-3)
Hossain Ahmed Patwary (18-39266-3)
Nawab Sakiul Alam (16-33035-3)

A Thesis submitted for the degree of Bachelor of Science (BSC) in Computer Science and Engineering (CSE) at

American International University Bangladesh in Jan,2023

Faculty of Science and Technology (FST)

Abstract

Quick and accurate user identification and verification are required as the volume of electronic transactions increases. The banking industry has already started using ATMs to process payments and provide consumers financial services. The main issue with employing these systems, however, is security. For security and identification permits in bank accounts and computer systems, personal identification numbers (PINs) and SMS verification are often employed. However, the reliability of these conventional systems is poor. On the other hand, a password or SMS verification security system won't provide as much protection as a biometric security system. Because this security method uses a person's physical or behavioral features to validate their identity. Fingerprint recognition technology may be used in tandem with ATMs for human identification to boost security. In this work, we presented a fingerprint-based biometric approach for ATM banking. The outcome is an enhanced fingerprint-based biometric verified ATM system that guarantees greater security and boosts customer trust in the banking sector.

Declaration by author

This thesis has never been completed for another degree or certificate at any university or other higher educational institution. The book presents a reference list and acknowledges content gathered from other published and unpublished works.

We acknowledge that copyright of all material contained in my thesis resides with the copyright holder(s) of that material. Where appropriate we have obtained copyright permission from the copyright holder to reproduce material in this thesis and have sought permission from co-authors forany jointly authored works included in the thesis.

…………………………………………
Ariful Islam
18-37545-1
Department of Computer Science & Engineering

…………………………………………….
Fardin Ahmed
18-39264-3
Department of Computer Science & Engineering

…………………………………………
Hossain Ahmed Patwary
18-39266-3
Department of Computer Science & Engineering

…………………………………………….
Nawab Sakiul Alam
16-33035-3
Department of Computer Science & Engineering

Approval

The thesis titled **“Fingerprint-based biometric system in ATM banking (Conceptual Model)”** has been submitted to the following respected members of the board of examiners of the department of computer science in partial fulfilment of the requirementsfor the degree of Bachelor of Science in Computer Science and Engineering on dated and has been accepted as satisfactory.

. . . .

Dr. Akinul Islam Jony (Supervisor)
Associate Professor
Department of Computer Science
American International University-Bangladesh

. . . .

Kawser Irom Rushee (External)
Assistant Professor
Department of Computer Science
American International University-Bangladesh

. . . .

Dr. Md. Abdullah- Al- Jubair
Assistant Professor & Head (Undergraduate)
Department of Computer Science
American International University-Bangladesh

. . . .

Dr. Dip Nandi
Professor and Director
Faculty of Science and Technology
American International University-Bangladesh

…………………………………………………

Mashiour Rahman
Sr. Associate Professor and Associate Dean in Charge
Faculty of Science and Technology
American International University-Bangladesh

Contributions by authors to the thesis

List the significant and substantial inputs made by different authors to this research, work and writing represented and/or reported in the thesis. These could include significant contributions to: the conception and design of the project; non-routine technical work; analysis and interpretation of researchdata; drafting significant parts of the work or critically revising it so as to contribute to the interpretation.

	Ariful Islam	**Fardin Ahmed**	**Hossain Ahmed Patwary**	**Nawab Sakiul Alam**	**Contribution (%)**
	18-37545-1	*18-39264-3*	*18-39266-3*	*16-33035-3*	
Conceptualization	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Data curation	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Formal analysis	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Investigation	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Methodology	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Implementation	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Validation	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Theoretical derivations	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Preparation of figures	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Writing – original draft	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %
Writing – review & editing	Ariful Islam	Fardin Ahmed	Hossain Ahmed Patwary	Nawab Sakiul Alam	100 %

Acknowledgments

First and foremost, we would want to convey our gratefulness to Allah for his kindness in allowing us to complete our thesis program on time.

We had like to thank the Faculty of Science & Technology (FST) for having thesis credit in the graduate program's curriculum and allowing us the opportunity to complete this. We are also grateful to AIUB's Faculty of Science and Technology and Office of Placement and Alumni for providing an opportunity for us to choose a field and complete a thesis there.

We are thankful to our supervisor **Dr. Akinul Islam Jony** sir for his kind support, direction, useful supervision, guidelines and advices.

Keywords

Biometric security system; Fingerprint-based biometric system; ATM banking; Personal identification number (PIN).

Table of Contents

List of Figures

List of Abbreviations and Symbols

Abbreviations	
ATM	Automated Teller Machine
PIN	Personal Identification Number
SE	Software Engineering
etc.	*etc.*

Chapter 1

Introduction

1.1 Fingerprint-based biometric system in ATM banking

Nowadays, autonomous systems lead a fundamental a part of everyday life in society. In this modern era, people are very concern about lead their lives peacefully. As the people living the modern society majority of civilians using ATMs regularly. According to that matter It is obvious that the number of ATM locations is rapidly rising. So, in order to improve our security, ATMs utilize biometric algorithms. Biometrics is a process that helps create very secure data that is specific to each individual based on their unique physical characteristics. Biometric data may be used to uniquely identify a person in a number of ways, including fingerprint, retina, complexion, pronunciation, gesture recognition, and writing. It is common for credentials to be lost, swapped, hacked, or seen inadvertently by a service provider. Frequently, symbols such as cursor buttons and money plus cards are lost, forgotten, duplicated, or erased. Biometric automation design is simple and may boost security and safety at the level of the fingertip. The procedure of registering a person's biometric with an identity device is simple and may not need much time or effort. Therefore, incorporating it into everyday life will have a significant influence. Our report's major objective is to employ fingerprint-based ATMs to provide a stronger security system.

1.2 Objective

The main objective of this work is to create a more secure ATM system by using fingerprints as an allowed identification. Sub-objectives are given below:

I. To follow the Software engineering research area our experimental research is standing. Type: Correlational.
II. To use activity, block & sequence diagram model in our research to implement a new security system in ATM banking. Type: Descriptive.
III. Implement these diagrams to make a strong security system plan in ATM banking transactions. Type: Explanatory.
IV. Make a strong, secure & user-friendly Automated teller machine system for the users in the future. Type: Descriptive.

1.3 Research Question

Research questions are given below:

1. How to upgrade ATM banking security system?
2. What types of UML models are used?
3. What will be the strategy to give a strong verification PIN code?
4. According to the biometric system what will be the impact?

In ATM banking security system, Scheduled and random physical checks of ATMs by branch staff and technicians.

Basically, there are three UML behavioral diagrams are used, such as: Activity diagram, Block diagram, Sequence diagram.

According to the strategy, to give a strong verification PIN code always try to put hard password that nobody can utilize that password.

Biometric authentication and its uses in modern-day tech and digital applications has a number of advantage like high security and assurance.

Chapter 2

Literature review

A literature review is an analysis of scholarly articles on a specific subject. It gives us a broad overview of present understanding, helping us to find related ideas, methodologies, and research gaps. We discussed about previous systems from others papers in this section. We find out the problems or gap from the existing systems. We try to identify the problems of other security system in ATM banking system.

2.1 Automated teller machine (ATM)

ATMs, also known as automated teller machines, are specialized computers that simplify the process of managing one's finances for those who have bank accounts. Customers are now able to check the status of their bank accounts in a short amount of time, as well as withdraw or deposit cash and transfer money across banks.

In the modern day, paper and metal coins have been mostly phased out as a component of our currency and have been replaced with plastic cards, which are also referred to as "plastic money." The percentage of banks in Nigeria that have ATMs climbed from 83 percent in the year 2006 to 289 percent in the year 2007. According to Hanson (1970), who wrote the book "Service Banking," [1] the Automated Teller Machine was first put to use in the year 1967 in the United Kingdom. Since that time, Japan and France have also made use of the device for a variety of applications. [Citation needed] If you want to withdraw money from an ATM, you are going to need a valid card in addition to the correct PIN number. Until that occurs, the automated teller machine won't accept it. Customers who use automated teller machines are required to provide either a plastic digital wallet embedded with a chip or an ATM card equipped with a payment terminal (that contains a unique card number and some security information). [1]

Researchers A. Rogers, D. Kristen Gilbert, Elizabeth Fraser Cabrera, and others looked at how elderly people utilize automated teller machines (ATMs). [2]. The research was broken up into two distinct parts. The first round consisted of one hundred interviews conducted by telephone. In phase two, sixteen individuals used ATMs on a consistent or near-constant basis. After that, we carried out the survey. They were interested in finding out whether or not this arrangement had the backing of the general population. However, only a small percentage of people actually answered those questions for the survey. A substantial section of the population of the world has been ignored. [2] As a result of this, the survey did not do very well. We have reason to think that there could be a solution to bridge this divide.

A combination of automated teller machine systems and basic data terminals with four output devices and two input devices are used in this process. They need to establish communication with a host processor in order to successfully complete the task. The host processor, which performs duties analogous to those of an Internet service provider (ISP), functions as a gateway that enables the owner of a bank account to access all of the various ATM networks using either a credit card or a debit card [3]. This is made possible by the fact that the host processor performs duties analogous to those of an ISP. In response to the rising number of instances of fraudulent behavior using automated teller machines, efforts are now being made to fix vulnerabilities in the PIN security system by developing secure authentication mechanisms (ATMs). In contrast to the conventional ways of entering a PIN, these approaches are evaluated based on how well they work in terms of how easily they can be remembered, how secure they are, and how quickly they can be entered. There is not a clear indication of the kinds of values that may be used for the PIN-based verification that is available at ATMs. [2]

The ATM system is essential to the financial system. But the security mechanism for ATMs isn't extremely robust or secure. Therefore, we need to find the strongest security method for the ATM system.

The introduction of automated teller machines, sometimes known as ATMs, brought about a revolutionary shift in the way that individuals handled their financial dealings. The ubiquity of the need for automated teller machines may be attributed to the accessibility and ease of these machines. However, a number of substantial roadblocks have been preventing the deployment of high-quality ATM banking services. A significant number bank customers are unhappy with the degree of privacy and protection provided by the automated teller machine service. Reginald Ihejiahi, a well-known figure in the banking industry in Nigeria, once held the position of group senior director at Fidelity Bank. According to Ihejiahi (2009), there is insufficient cooperation between financial institutions in the fight against fraud [1]. According to him, the silence of the banks on ATM fraud is slowing down their development and making it more difficult for the industry as a whole to start sharing vital information that may be helpful in a variety of different ways. The risks associated with ATM fraud are growing as a consequence of the proliferation of increasingly dangerous indiscriminate concerns. Customers who respond to unsolicited emails and text messages by providing their credit card information and who are careless with both their card and their personal identification number (PIN) are a typical source of fraud. Customers may run into issues if they misplace their ATM cards or forget their personal identification numbers [1]. The user authentication methods that are now in use, such as the application of codes, user IDs (identifiers), identity cards, and PINs, suffer from a variety of drawbacks (personal identification numbers).

A short message service verification system for ATMs was suggested by Jimoh R.G. and Babatunde A. N. The user's mobile device will get a code. After entering the code, the user may readily access the system [11]. However, this kind of technology carries a substantial risk. Although less secure, this technology is user-friendly. All the information will readily be sent to someone else if the user's phone or number goes stolen or gets misplaced. This makes the system insecure.

To better understand the security of biometric-based ATMs and to compare and contrast different authentication methods, field research and several side studies on actual ATM usage were done. Their results demonstrate that the environment has a significant impact on the safety and effectiveness of biometric-based ATMs. Examples of such elements include distractions, physical obstacles, trust connections, and memorability design of various ATM authentication procedures, including areas of social life and concentration resistance [3].

2.2 Biometric-based security system

As a kind of security, biometric authentication uses a person's unique biological characteristics to verify that they are who they claim they are. structures for biometric authentication examine behavioral or physical changes to record and verify accurate facts in a dataset. Authentication is confirmed if each sample of the biomechanical facts matches. Based on biometric information, biometrics are computer-assisted techniques for determining personality.

The use of ATM cards and the electronic payment system are both being negatively impacted by the present fraud activities, according to Prof. Selina Oko and Jane Oruh [12]. The use of an ATM security system is now quite difficult. Fraud and identity theft are also simple in this age.

An MBS-based (multimodal biometric system) security solution was proposed by Madhukar Kale and Professor P.G. Gawande [4]. Procedures using the iris, fingerprints, and palm prints are used. For the very first time, information on a person's fingerprints, palm prints, and irises is now being gathered. Each one has been subjected to its own separate preprocessing, and a singular feature representation has been produced by extracting and combining the characteristics of all of them. This representation is kept in its current state on the server. The next step is called "matching," and it consists of comparing the test image to the feature vector that has been saved while utilizing the Euclidean distance that is the shortest. [5] GSM modem technology was the foundation for the security system that was suggested by M. Gayathri, P. Selvakumari, R. Brindha, and others. As a result, GSM is used in the strategy that was recommended. A transceiver may take the form of a standalone modem that connects by digital, Bluetooth, or wireless technology; alternatively, it might be a mobile phone that is equipped with GSM modem capabilities. Universal Mobile Telecommunication is what is meant to be abbreviated as "GSM" (Global System for Mobile Communication). The ability to transmit mobile telecommunication services is genuinely made possible by mobile communication technology. Biometric systems are now widely used around the globe. A fingerprint sensor is present on almost all smartphones and smart gadgets, and some of them also feature iris sensors. Individual identities are recorded using biometric sensors. There are several kinds of sensors, including iris, speech, and fingerprint readers.

Biometric sensors are used to record a person identify. The authentication procedure is often used to control access to physical and digital resources including offices, rooms, computers, ATM systems, and other resources. Many different kinds of sensors can take photos of fingerprints. There are three different kinds of image sensors for fingerprints: optical, strong, and transducer [6]. Despite its benefits, the FTIR-based optical sensor might be overwhelmed by a dry or wet finger, leading to inaccurate readings [6]. The Zigbee technique is the foundation of the Wireless Biometric Security System [7]. Ravi Shankar Kumar, Mohit Kumar, Raju Kumar, and Mukesh Kumar Thakur identified certain universal issues with security systems. A user's fingerprint is taken using a fingerprint sensor module, compared to database information specific to the user's fingerprint, and displayed on the computer screen utilizing this technological method. Apart from that, it has a tiny risk of hacking but is otherwise cheaper, quicker, and more portable. They can easily find all of the info if someone attempts to breach their database.

Nevertheless, the existing security system is unable to provide us the highest level of protection. The conventional method of identification, which depends on having an ID card or specific information like a social security number or password, is not totally reliable.
The system based on GSM has certain drawbacks. Like There has been electronic interference. Due to its pulse-based transmission method, GSM is known to interfere with devices like hearing aids. Then there are additional issues like repeaters, bandwidth latency, and a low data transmission rate. These are the security system's limitations [5]. A unimodal system is transformed into a multimodal system using Euclidean distance and the principal lined mechanism. However, the database-stored picture is deteriorating day by day. [4].

2.3 Fingerprint-based biometric system in ATM

Among the many qualities employed are voice, face, fingerprints, veins, eyes, retina, gesture recognition, and calligraphy [8]. The vast majority of fingerprint scanners rely on minute details.

Samir Nanavati asserts that pattern methodology has the ability to replace minutiae recognition, which accounts for 80% of fingerprint scanner scan methodologies. This technique generates templates by extracting characteristics from a set of ridges rather than discrete points. The dependence on small, fragile points is reduced by the use of several ridges [8]. The disadvantage of pattern matching is that the produced blueprint has a much higher byte capacity and is more sensitive to finger positioning during authentication. The accuracy and dependability of fingerprint technologies have been established. Identification, classification, and analysis of fingerprints have a long history. This has set fingerprints apart from other biometric systems, along with their distinctive qualities. The enrollment phase and the authentication phase are the two main phases of the suggested system. [14] The implanted fingerprint identification system uses a microprocessor that functions with great accuracy but at a slower pace for applications that employ the minutiae-based biometric matching approach. [14]

The biometric security system that was designed by Awatade Vidya, Atar Nasrin, Bansude Vijaysingh, and Hegadkar Rani [15] was based on GSM, which served as the system's basis. As part of this research project, a high-security locker system is being planned and built. The system will include GSM, fingerprint, and password technologies. They have devised a safe method of accessing the lockers, which makes use of GSM, password, and fingerprint technologies. This method ensures that only authorized users are able to get entry to the lockers. This system comprises a door security mechanism that, in addition to opening the entry in real time, may also be used to initiate, authorize, and verify the person who is seeking to enter the building. This functionality is in addition to the fact that the system opens the entrance in real time. It will not be difficult to get into the system if a user forgets their password and then acquires the password from an illegitimate source. The price of technical developments has decreased while their capabilities have improved, which has led to a big increase in the number of alternatives that are now available. This has led to a substantial increase in the number of options that are now accessible. On hardware that is no more than a quarter of an inch thick and no more than an inch square in size, photographs may be shot and processed. In addition, while many people view the availability of fingerprint solutions on the market as a negative because it ensures market competition, others see it as a positive because it results in a variety of trustworthy solutions for desktop, laptop, physical access, and point-of-sale circumstances. This is despite the fact that many people view the availability of fingerprint solutions on the market as a negative because it ensures market competition. There is a distinction to be made between personal information and biometric data. It is not possible to utilize biometric templates to copy confidential information in the other way, nor is it possible to steal them and then use them to get access to confidential information. It is possible that this technology will help to make ATMs even more secure. In the process for the second level of authentication, two different authentication methods are used. Numerous financial institutions make use of it in order to complete transactions via the internet. The goal of the method for the second level of authentication is to check that the person who is logging in is doing so to the correct one. At the second level of security, the first two of the three user authentication processes that are often utilized are put into practice. [9].

1. A password or a pin.
2. Digital certificates or smart cards.
3. A biometric or biological characteristic, such as fingerprints.

In addition to acquiring the Passcode, a counterfeiter or fraudster would want knowledge of the one-time login information with the secondary level of verification. When using an ATM, customers normally have three opportunities to successfully enter into the banking system. The automated teller machine will often refuse to accept the customer's credit or debit card and then throw it away if the user forgets to log in to a financial institution. A hacker is unable to use the ATM to steal money from the owner's wallet since the charge plate stops them from figuring out the right passcode and accessing the ATM. The performance factor is characterized by the swiftness and precision with which a transaction is carried out. The user's line of sight to the display should never be obstructed in any way. The customer's personal identification number (PIN), extension, and implanted fingerprint all contribute to the account's overall level of security. When using an ATM, customers typically have three opportunities to successfully log into the bank's system.

V.Padmapriya, S.Prakasam, and other researchers have discussed the use of a combination of fingerprint sensor tokens and GSM connection in ATM security systems. This system suggests an architecture that integrates the traditional PIN-based authentication with the GSM technology as well as fingerprint technology. Nevertheless, the design bears the signature of either a candidate or an independent third party. There is a disagreement between the primary user and the designated user in the system architecture that has been proposed. [10]

For automated teller machine (ATM) banking systems, this paper suggests an integrated fingerprint multimodal biometric technique. This method uses fingerprint biometric technology to identify people in conjunction with the ATM to increase security. For biometric information systems, hardware problems are a major worry. If suppliers of biometric services can use certain occurrences to ascertain which features of their services need to be developed. It may be a outstanding depiction of our nation. Over 75% of the respondents to this survey agree with Nisha Bhanushali et al. (2004) who claimed that the location of an ATM significantly affects the potential for crime and fraud to occur there [13]. They suggested developing an ATM system with a biometric system based on fingerprints.

The ATM system can be improved with biometrics, and users may stop frauds and thefts. Everything has benefits and drawbacks and this method is no different. Despite these drawbacks, biometrics will be quite beneficial. The fingerprint analysis, algorithms, software models, and API that will be discussed in this work will improve the ATM system and increase its security, which is the consumers' primary concern [13].

The E-Banking System is developing a biometric technique to increase ATM privacy (fingerprint). By using a combination of security measures, such as a Passcode and a biometric identification system, this study [16] offers a high-level solution for altering current ATM systems. When the primary cardholder is unable to complete transactions, they also advised the nominee to employ a fingerprint identification system. However, users may have encountered certain frequent issues with this suggested method, such as hacking and lack of protection for nominate.

Chapter 3

Methods

The feature pattern on one finger creates a fingerprint. Strong evidence supports the idea that every fingerprint is distinct. Everybody has their own fingerprints, which are permanently distinct. Therefore, fingerprints have been utilised for forensic analysis and identification for a very long time. Numerous ridges and furrows make up a fingerprint. In each little local window, these ridges and furrows exhibit strong commonalities like parallelism and average breadth. Minutia, which are certain aberrant points on the ridges, are what differentiate fingerprints instead of the ridges and furrows, as demonstrated by extensive study on fingerprint recognition. One is called termination, which is a ridge's immediate end. The point on the ridge where two Branches originate is known as the bifurcation.

Figure: Fingerprint 1

Figure: Fingerprint 2

Two sub-domains exist inside the fingerprint authentication issue. Both fingerprint identification and fingerprint verification fall within this category. Additionally, FAA (Fingerprint Authentication in ATM), which is a program-based method rather than an expert-manual approach, is used here for fingerprint authentication.

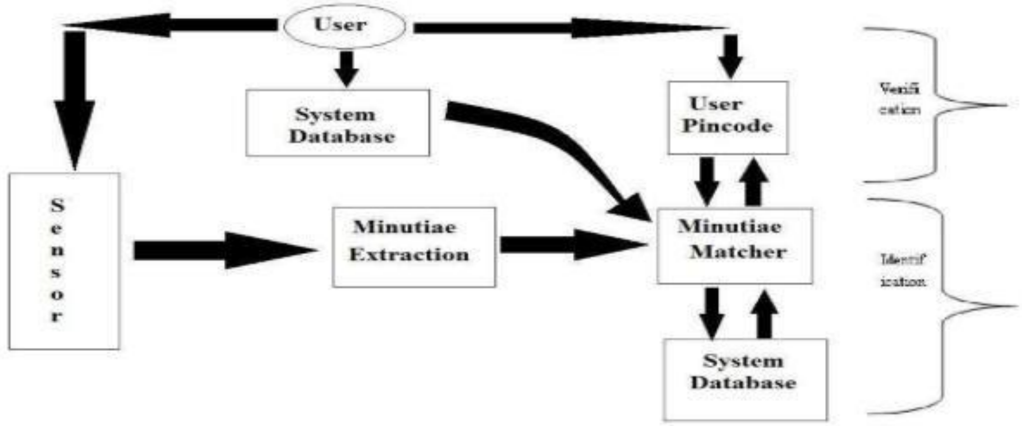

Figure: Verification Vs Identification

The process of fingerprint verification involves confirming a person's identity using his or her fingerprint. Along with his identity information, such as his PIN-CODE, the user gives his fingerprint. In accordance with the PIN-CODE, the fingerprint verification system gets the fingerprint template and compares it to the user's real-time fingerprint acquisition. Usually, it is the fundamental AFAS design principle (Automatic Fingerprint Authentication System). By using a person's fingerprints, one can identify another person. The fingerprint identification system attempts to match the person's fingerprint with those in the entire fingerprint database without knowing who they are. For cases involving criminal investigations, it is extremely helpful. It is also the AFIS's guiding design principle (Automatic Fingerprint Identification System). However, every issue with fingerprint recognition, whether it is a verification or identification processes ultimately rely on a precise fingerprint representation.

In our system, there are two main phases. Enrollment phase and Authentication phase.

Enrollment Phase:
The registration step is another name for the enrollment phase. During this stage, a person uses the fingerprint scanner to register his fingerprint and store it in the database.

Authentication Phase:
In the authentication step, a person's identity is verified by comparing the test image he supplies with the stored image, proving that he is who he says he is. The subunits' precise operation is as follows:

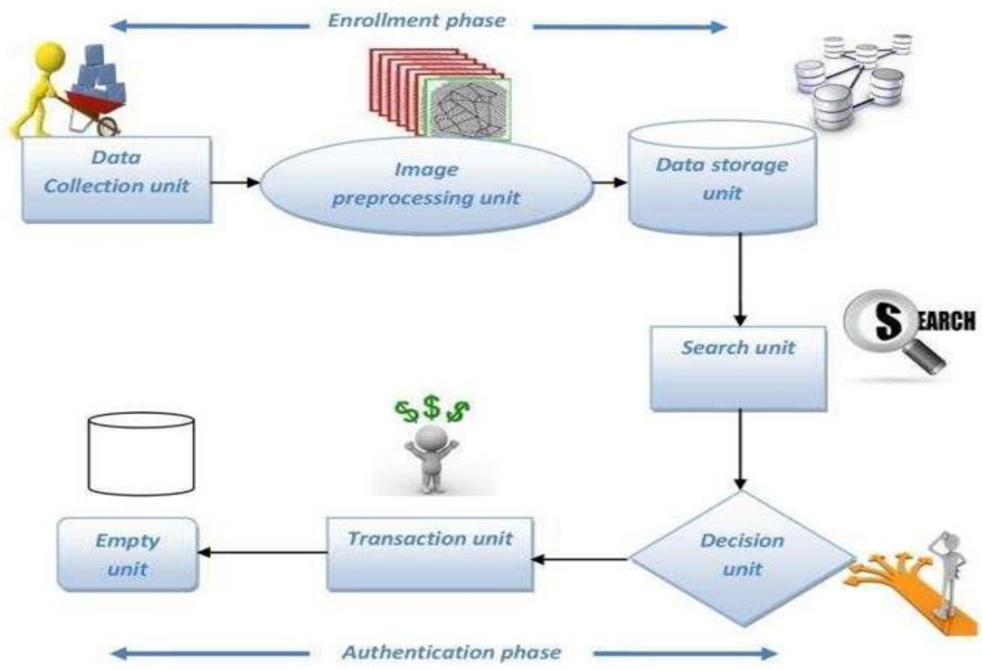

Figure: Fingerprint based ATM System

Data Collection Unit: An optical sensor or optical scanner is the most fundamental and crucial necessity for this stage. In this device, the user fingerprints are gathered. This component significantly enhances the database unit by adding the user's fingerprint. returns a byte every newly added ID.

Image pre-processing unit: The Scanner receives the image as input and pre-processes, it while it is processing the picture. The test image is an analogue image that is converted into a digital image, and if the preprocessed image's quality is good enough, the image is then turned into a template.

Data storage unit: Each pre-processed image has a specific template size and is stored as data (approximately 512 bytes per template). Additionally, the template is kept in the database for later usage. This device enables the user to configure the module in 1:1 mode for saving a specific person's fingerprint while also storing fingerprint data in the module.

Search Unit: When a finger is placed on the fingerprint sensor, the search feature is activated is called. The existing memory is then checked and returns a matching ID if found.

Decision unit: The database-stored images and the input image are compared by the system. After various steps, the database picture is stored to make transactions easier. The test image's required resolution is 500 dpi based on comparisons between the stored template and test image (dot per inch). The user of the input is an authorised user once the image comparison is successful.

Transaction unit: The transaction is completed if the decision-making entity gives the user permission. Empty function: This function is used to purge the fingerprint database of any remaining data. To strengthen security, a pin number and biometric information are combined. The transaction would be safe and secure because biometric data cannot be stolen or faked. The pin number might potentially be faked, though. The proposed system's transaction time is 10 seconds or so. Since the clients want and anticipate quick transactions, this is accomplished with greater care.

We are integrating fingerprint authentication in this system based on the ATM system. The system has embedded non-volatile memory and SEA/RSA acceleration engines (Flash). The system sets aside a specific amount of Flash memory for fingerprint libraries, or fingerprint templates. Flash stores fingerprint templates in a logical order. Taken into account, the serial number of the template used in the library is 0, 1, 2, 3... N. Let's consider the fingerprint capacity N. An individual can access the library by template number, thus the photographs are stored in the database as templates before being compared to input images. If the image does not match, additional authentication is performed before the transaction may be completed. The system has inbuilt non-volatile memory and SEA/RSA acceleration engines (Flash). The microprocessor with code that manages a computer's interaction with its connected serial devices is known as a UART (Universal Asynchronous Receiver/Transmitter). It enables modems and other serial devices to "speak" to the computer equipped with the RS-232C Data Terminal Equipment (DTE) interface and exchange data with them.

Chapter 4

Conceptual Model

According to the requirements of everyday life, ATMs are extremely useful and appropriate. Therefore, we have to proceed with extreme caution whenever we use such products. There are a few topics on which we need to have absolute clarity with regard to those topics. For example, a biometric-based security system and a biometric-based algorithm used in ATM machines, all of which are examples of the many different sorts of diagrams, such as activity diagrams, block diagrams, and sequence diagrams.

ATM fraud concerns are become more concerning as a consequence of the widespread nature of the underlying issues. Consumers making mistakes with their card and passcode numbers are a common source of fraudulent activity [1]. If the PIN number system uses a verification-style security system or a biometric-based security system, then it will be possible to prevent fraudulent activity at ATMs. The findings of the poll based on one hundred respondents were inadequate [2]. The results of a survey that has a significant amount of people responding to it will be reliable.

The use of short message service authentication in automated teller machines is fraught with danger [11]. This technology is user-friendly, but it has a lower level of security. If some form of biometric system were to be added to this proposed system, then it would allow for improved levels of security. This might be one of the possible responses to your question. A cash machine that is placed close to or even within a bank has a better level of security than one that is located a significant distance away or outdoors. The automated teller machine should be placed in an area that is less crowded but is nonetheless densely inhabited. A covert camera is necessary both inside and outside of the automated teller machine (ATM), and it must be positioned in such a way that it cannot record the PIN digits of the user but can only view his face. The Wireless Biometric Security System is one that uses Zigbee Technology as its foundation. There are reliability issues with the Zigbee technology's database security system [7].

They have to work on fortifying and better protecting their database system. It is possible to maintain confidential information and execute financially sound transactions when using solutions that are based on biometrics. At the moment, it is quite challenging to make use of a security system for an ATM [12]. If a comprehensive security system, such as facial recognition, iris scanning, or fingerprinting is adopted by the banking sector, it will be more effective for everyone. If this occurs, it will be more effective for everyone. [5] There is a proposition for a new security system that utilizes GSM modem technology in conjunction with a multimodal biometric system (MBS). For a GSM-based system, we recommend using safe algorithm A3/A8 implementations, secure ciphering algorithms, and end-to-end security in order to overcome these vulnerabilities. In order to solve the problems that arise with multimodal biometric systems, an image processing system that is based on a high resolution will be implemented.

It has been suggested that a biometric security system that utilizes fingerprints and is based on GSM should be used in the banking industry [15]. It has a few issues that need to be addressed. We got to the conclusion that the system would be safe if the user was unable to access any sources that were not pre-approved in order to find a solution to the issues that were brought to our attention. The only fingerprint that may be used is the user's own, and as long as the proper fingerprint is supplied, verification is not necessary. The only fingerprint that can be used is the user's own. The biometric security system that is based on fingerprints and is used for automated teller machine banking will be an effective security system if the procedures that are stated in this approach are followed out. The design of the system that is being recommended has a feature that creates tension between the principal user and the nominated user [10]. You will discover that the nominee user component of this system is not necessary for the system to work properly if you remove it.

The findings of this research suggest a comprehensive plan for the modernization of existing ATM systems [16]. In order to provide the highest level of safety, the solution integrates biometric fingerprint technology and password protection features. Because of what we've learned about hacking, we know that it's essential to find a way to circumvent the issue that arises when a sensor detects anything and issues a warning, which causes the ATM to go offline if anything is connected to the card reader or input. This is something that we came across throughout our research. In addition, a nomination option is not required initially since doing so puts the security of users at risk. This means that it is not needed. It is feasible to access an account with nothing more than the fingerprint of the account holder.

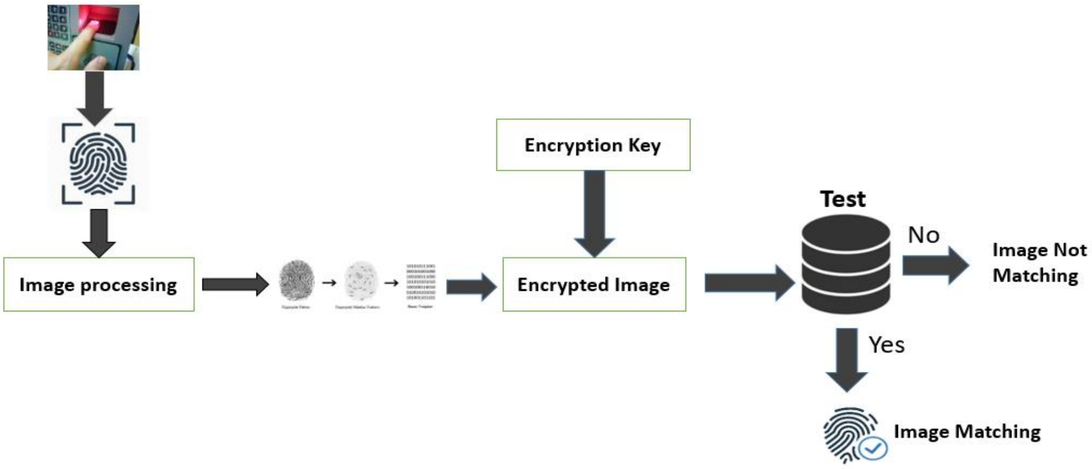

Figure: Proposed ATM Design

One kind of biometrics technology is fingerprint scanning. When accessing the ATM for a transaction, we use our fingers. This system is what we are utilizing since it is simple to install. We don't need to get rid of the present ATM. The operation of an ATM fingerprint involves gaining access to server-based data. Before accessing the procedure, we must get bank authentication. Using a biometric device, bank employees scan customer fingerprints.

The whole process of a biometric system extracting a fingerprint's characteristic and storing it in a database is known as enrolment. Customers who want to use an ATM with biometric scanning must first put their finger at When using a biometric scanner, the person's features are scanned and then extracted and compared to stored features; if the features match, the transaction may proceed; otherwise, it cannot.

4.1 Design & Procedures

4.1.1 An activity diagram of an ATM banking system

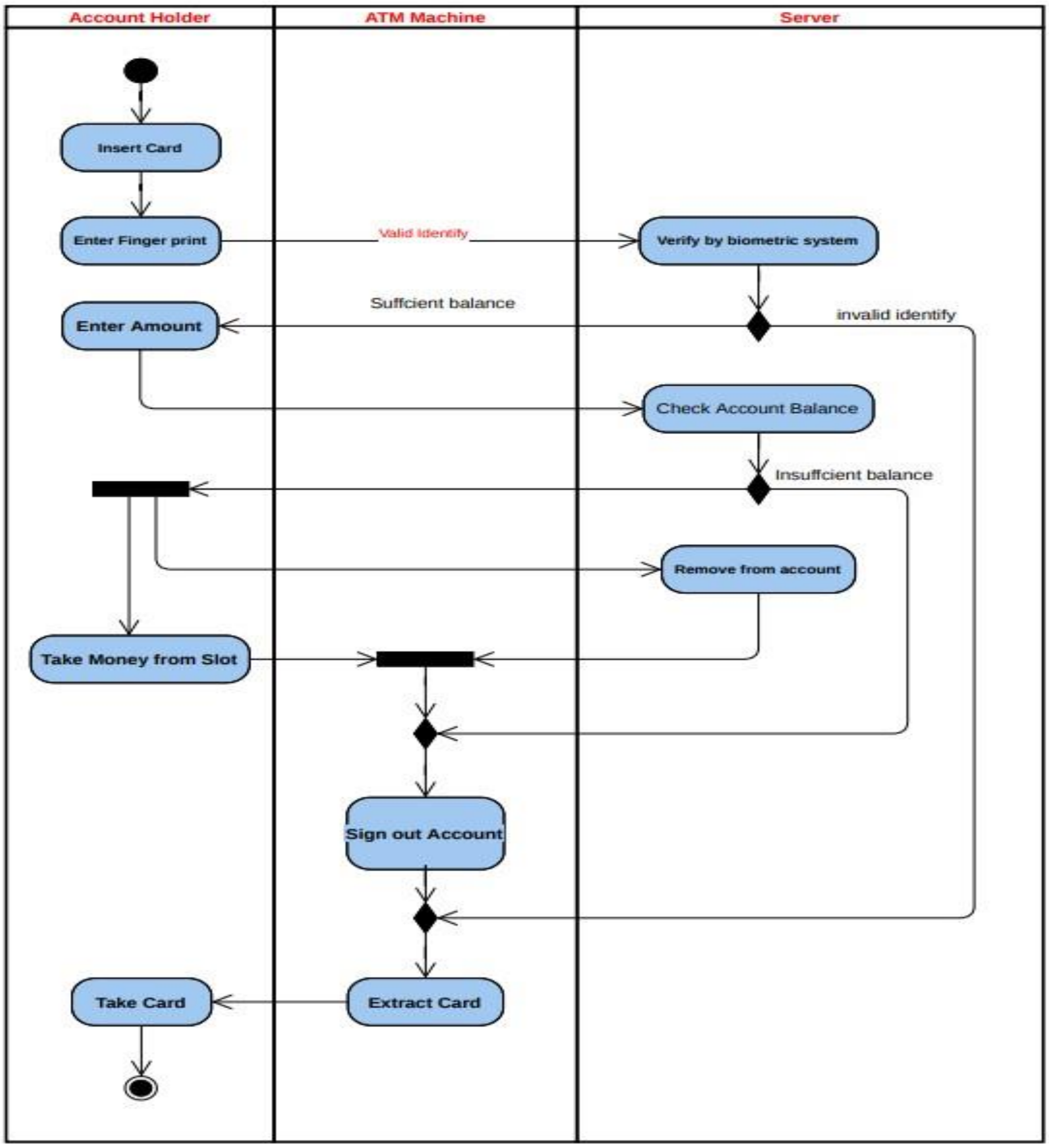

Figure: An activity diagram of an ATM system

Figure 1 Activity diagrams were used in the process of developing the automated teller machine (ATM) banking system. An activity diagram, which is a graphical representation of the flow of events and the movement of controllers inside a system, is comparable to a flowchart or a data flow diagram. A use case diagram could include depictions of the processes involved. The

activities that are represented could take place in a sequential order or in parallel. The first image is an illustration of how the ATM System communicates with people who use ATMs. It adheres to a format or set of works that focuses on the events that take place when an automated teller machine is utilized. In this particular case, one of the security measures shown by the ATM system is a check of the cardholder's available balance. This activity diagram demonstrates how the system responds to each user request by effectively connecting with the user in the proper manner. Another action that the user interacts with when using the ATM system is impacted by a different circumstance. The exchanges that take place when a user attempts to access and withdraw money from an ATM using their ATM card are shown in this flowchart. By paying close attention to the occurrences shown in the graph, we should be able to generate an educated opinion of the behavior of the system. Consequently, the resulting activity diagram is more valuable for creating the ATM system. It is essential to know the ATM security system's design and construction schematics. This explains why it is difficult to design a system that is totally functional without it.

In order for the system to be aware of the many inputs and conditions that it must handle, we must develop this activity diagram. We will also mention the crucial steps and link them to the other UML diagrams. By only completing the Activity Diagrams at each level, we are able to construct any security system we choose.

4.1.2 A simple block diagram of a biometric security system

A security system operation is shown in diagram in figure 2. A block diagram may be created using a wide variety of symbols. Several of them including:

1. The oval denotes the start or finish of something.
2. Arrows are a kind of line that connects the representative forms and depicts connections between them.
3. Process/Compute: A rectangle depicts a process, a computation, or an assignment.
4. Choice: A diamond denotes a choice.

Each block below provides a specific device name, such as sensor, LCD screen, and database, which are the hardware we need to construct a biometric system. We employ fingerprints, palm prints, iris scans, face scans, etc. in biometric systems. Here, we'll go through the operation of a fingerprint security system.

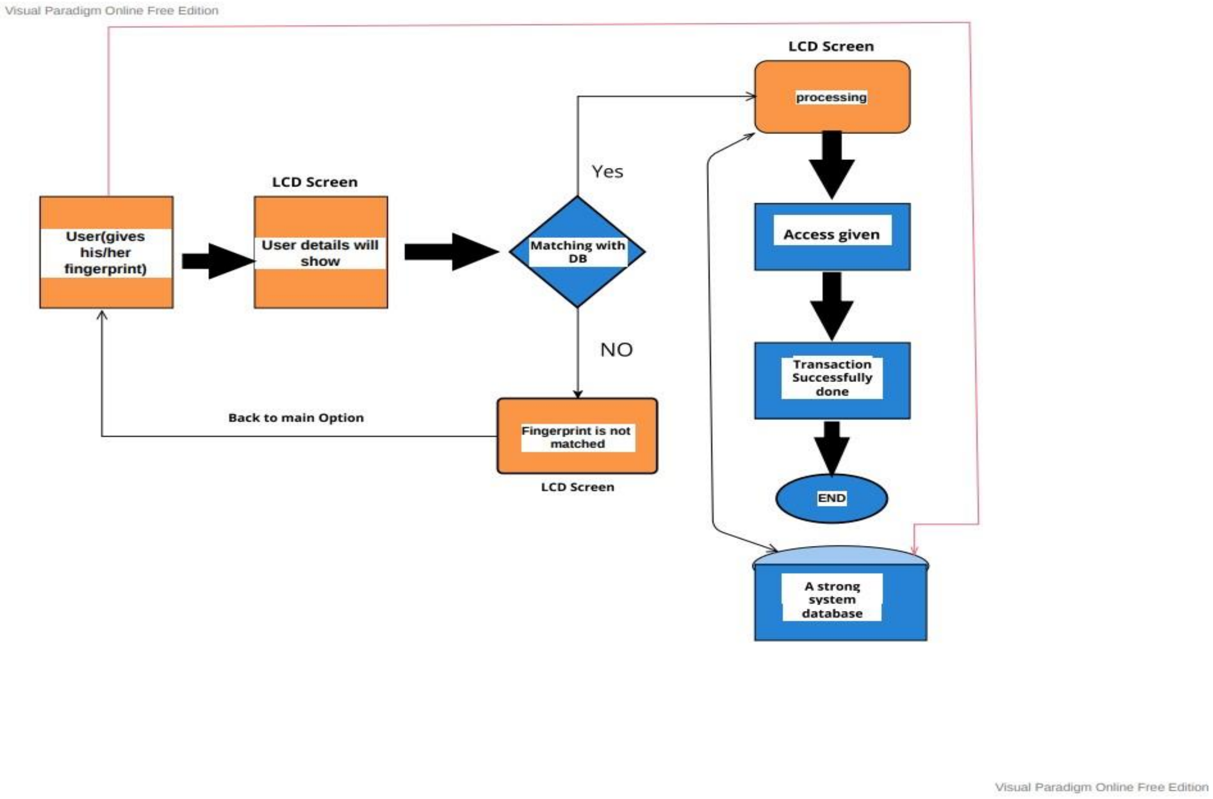
Visual Paradigm Online Free Edition
LCD Screen
processing
Yes
LCD Screen
User(gives his/her fingerprint)
User details will show
Matching with DB
Access given
NO
Transaction Successfully done
Back to main Option
Fingerprint is not matched
LCD Screen
END
A strong system database
Visual Paradigm Online Free Edition

Figure: Block diagram of biometric based security system

First of all, a fingerprint is required when we need access to a system, thus we need a sensor for that. The LCD panel will display the results once the user places his or her finger on the sensor, along with a note indicating whether the user is legitimate or not. After receiving a command from the sensor and completing a search, a reliable database system will let the user know whether or not they are a genuine user. As a result, the sensor will periodically send a command to the LCD screen and database.

The decision box will receive a command from the LCD screen to verify the yes or no condition that we previously wrote and compare it to the database. The LCD panel will display the word "Processing" if the answer is affirmative, indicating that the user is legitimate. The user will then have access and be able to retrieve or withdraw his funds. The procedure will come to a close when you see the notification "Transaction successfully done" after getting the money. The next user will then be presented with the machine's first choice, which is to request a new user's fingerprint.

Finally, if the user's fingerprint is not recognized, the LCD screen will display the message "Fingerprint is not matched" before returning to the sensor and starting again at the beginning.

4.1.3 A sequence diagram of a fingerprint-based ATM

A fingerprint-based ATM system process is shown in this figure. This graphic supports our overall research strategy. Four separate objects, User, ATM, Consortium and Bank were used to create this flowchart. By interacting with one another, these items control the system.

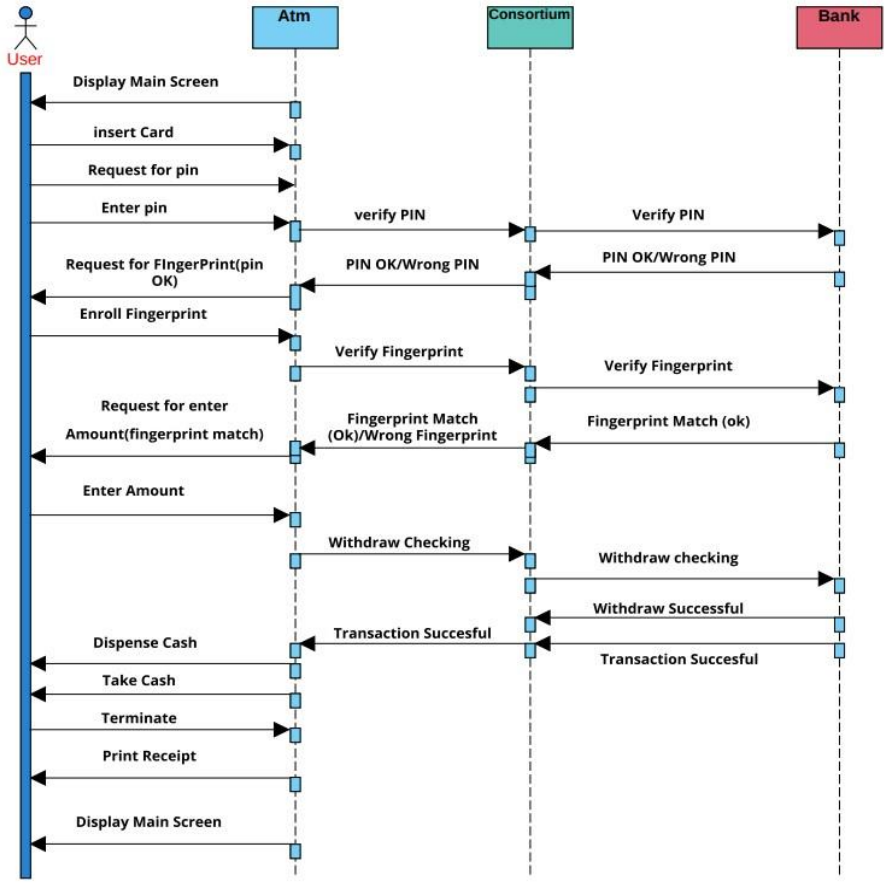

Figure: Sequence diagram of a fingerprint security system in ATM banking

To validate these claims, consortium works. The ATM will display the home screen to the user whenever he requests a cash withdrawal. The consumer has to insert their card into the machine. The consumer will next be prompted by the ATM to enter his PIN. After entering a PIN, the ATM transmits the PIN number to Consortium for validation; after being verified, Consortium sends the PIN number to the bank. The bank will issue a "Wrong pin" message if it deems that the PIN number is wrong, communication to the consortium, which will then send an ATM and ask the customer to try again with the pin. However, the consortium will get a notification stating "PIN approved" if the bank determines the PIN number is accurate.

The ATM will then request the user's fingerprint after receiving it from the consortium. The ATM records the user's fingerprint, transmits it to the consortium for confirmation, and the bank then receives the consortium's confirmation. The bank will alert the consortium and the consortium will alert the ATM when the fingerprint does not match the user.

The ATM will then urge the consumer to input his fingerprint once again. This allows us to avoid massive fraud. Even after learning the PIN number and taking the card, no one will be able to steal money since each individual's biometric verification and identity results are unique. When the user's fingerprint matches that of the ATM, the user will be prompted to input a value. The bank will then inform the consortium of the successful fingerprint match.
The user enters the amount, the ATM transmits it to consortium to validate it, consortium sends it to the bank, and consortium receives it from the bank.

The consortium will get a notice from the bank indicating "Withdraw successful" and "Transaction successful" when the withdrawal has been completed. Additionally, it will transmit that data to the ATM, giving the user the chance to withdraw money. The ATM will provide the customer the option to halt the transaction once the money has been received. The main page is then shown to the next new user once the user chooses "Print receipt."

Chapter 5

Results or findings

The risk of ATM fraud is growing as it becomes more common and endangers more people. User negligence with their one of the most frequent types of fraud is the use of card and PIN information [1]. The security problem will be resolved if the ATM system implements our recommended paradigm. One advantage of fingerprint technology is its accuracy. Due to the vast amount of information included in fingerprints, it is extremely impossible to find two fingerprints that are exactly same. Then, fraudsters are unable to manage the accounts of others. Our fingerprint method also has the advantage of using very minimal memory to retain the biometric template. By confirming a tangible, real-world attribute as both something the user possesses and something the user is, fingerprint-based biometric technologies in ATM banking provide providers greater confidence that a person is genuine.

Figure: Risky & less secure SMS verification system in ATM

The use of short message service authentication in automated teller machines is fraught with danger [11]. This type of rapid communication is simple to use while having a lower level of safety. The numbers used in the SMS verification process are fairly easy for cybercriminals to steal. The fingerprint security approach that we mentioned might prove effective in this case. A security system that makes use of fingerprints will do away with this threat completely. Because to the use of biometric authentication, no one is able to access the account of another individual. Because fingerprints cannot be passed from one employee to another, it is impossible to exchange passwords or "clock in" on behalf of another worker. Because of this, more precise monitoring is possible, as well as increased security against the theft of essential components. In addition, there is no requirement for any form of verification or code number since there is none required. In the past, a number of studies have proposed the use of SMS as a financial security method for ATMs. However, it is not risk-free. The existing security system will be replaced with the technology that we propose, which will also provide an improved security mechanism for the automated teller machine banking system. At the moment, it is quite challenging to make use of a security system for an ATM [12]. Because it is based on fingerprints, the fingerprint-based biometric technology prevents anybody from accessing the other systems that are part of the biometric security system. Customers are often surprised by how straightforward and quick the fingerprint-based biometric system identification process is, despite the fact that its underlying principles are somewhat complex. The technology in question is fairly simple to use. Rapid completion of transactions is possible just by touching one's fingertip to a scanner. It is quite improbable that you would forget the information related to your personal biometrics. In order for biometric authentication to work properly, certain user behaviors must already be in place at the time of acceptance. Because a real fingerprint cannot be copied or made public online, the majority of fingerprint identification solutions must always be applied manually. This is because an actual fingerprint cannot be replicated. There is a one in 64 billion chance that someone else's fingerprint will be an exact match for yours. The vulnerability of an individual's fingerprint to hacking increases with the frequency with which it is presented. The sensor-based detection system that we tested and found to be successful warns the user and temporarily disables the ATM card if it detects suspicious activity. The hacking problem won't be an issue with the strategy we suggest since this will stop it from happening.

Figure: Fingerprint biometric security system in ATM banking

There is a disagreement between the principal user and the nominated user in the system design that is advocated [10]. This system will function correctly if the nominee user component is taken out of the equation. Our fingerprint-based biometric security system does not need an initial nominee decision since it poses a risk to the user. Simply the account holder's fingerprint will be needed in order to get access to the account. This is just another advantage that our method has. The use of a person's fingerprints as a form of biometric identification allows for their identity to be verified via the examination of their biological data. In contrast to Personal Identification Numbers (PINs) and passwords, biometric information is not only entirely unique to each person but also very difficult to guess. It is famously difficult to compromise biometric security systems. They are a well-liked replacement for the conventional security solutions that rely on a single factor or a useful supplement to multi-factor authentication, both of which are used to provide high levels of security and enterprise-level protection. The reliability and cost-effectiveness of biometric authentication systems are both expected to increase in the near future.

Chapter 6

Discussion

A desktop application that utilizes the user's fingerprint for authentication is a fingerprint-based biometric technology, which is used in ATM banking. A person may be recognized thanks to their unique finger print, which is present on every individual. More secure and safe than ATM cards are fingerprint-based ATMs. In order to make an ATM system that is more secure, this technology will employ fingerprints as an authorized form of identification. The customer puts their finger on the ATM's biometric scanner in this scenario, and if a match is made, the transaction is completed. An ATM card doesn't need to be kept in your wallet, and even if it is, you won't misplace it. To finish any financial transaction, you merely need to use your fingerprint. For a transaction to be completed, the user must first authenticate using his fingerprint. Money from the user's account may be withdrawn. Any moment might see a spike in system delays. Consequently, individuals could feel more stress. This situation, however, is quite exceptional. For manual workers who often use their hands, identification and verification might be difficult. It is challenging to ensure total security due to the system's vulnerabilities. Identification systems suffer when it is hard to differentiate between fingerprints from damp or dirty fingers, scars, or skin conditions. Biometric authentication based on fingerprints is very reliable in ATM banking, confirming that a credit card transaction was initiated by the card's authorized user. The less secure PIN may be substituted with it. A fingerprint is very hard to get and use, yet it is possible to steal a PIN. The flexible account access allows customers to access their accounts anytime they want. If hacking concerns exist, it sounds an alert. Alarm notification is sent to the bank. Both practical and swift the system. The transaction may be finished in a short amount of time. Our results suggest that an ATM banking biometric system based on fingerprints triggers the transaction to be completed. Any amount of contactless transaction may be permitted thanks to fingerprint verification, which confirms the cardholder's identity throughout every transaction. With this strategy, there will be a significant reduction in money theft from one person's account to another.

Chapter 7

Conclusion

It is essential to have a solid understanding of the foundations, which includes the advantages, disadvantages, prerequisites, and, most importantly, the practicability of a biometric security system. Scanning fingerprints, in particular, is gaining popularity as a biometric technique that is gaining favor as a realistic approach of securing access through identification and verification procedures. In addition to its use as evidence in forensic investigations, biometrics is also a reliable and ubiquitous method that may be used when identifying or authenticating persons. If a person's credit card or ATM card is lost or stolen, a malicious user often has the opportunity to deduce the correct individual passwords. In spite of the warnings, a significant percentage of individuals continue to use passwords and codes that are derived from personal information such as their birthdays, phone numbers, and social security numbers. The need for technology that can verify an individual identify has increased in recent years as a direct response to the proliferation of recent instances of identity theft. Because the biometric information of each person is one of a kind, the use of biometric identification technology that is primarily based on fingerprint identifiers may be able to circumvent this problem. In addition to being an intriguing area of research in pattern recognition, biometrics has the potential to make our society more secure, more accepting of people of all backgrounds, and less vulnerable to fraud. By restricting access to just the card's registered owner, this strategy, if completely adopted, will significantly cut down on the number of fraudulent transactions carried out at ATMs. In the not too distant future, this will be carried out.

Bibliography

1. J. O. Adeoti. 2011. Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. J Soc Sci, 27(1). 53-58. DOI: https://doi.org/ 10.1080/09718923.2011.11892905.

2. Wendy A. Rogers, Elizabeth Fraser Cabrera. 1994. AN IN-DEPTH ANALYSIS OF AUTOMATIC TELLER MACHINE USAGE BY OLDER ADULTS. PROCEEDINGS of the HUMAN FACTORS AND ERGONOMICS SOCIETY 38th ANNUAL MEETING. Vol. 3. 142- 147.

3. lexander De Luca, Marc Langheinrich, Heinrich Hussmann. 2010. Towards Understanding ATM Security System. ACM Press the Sixth Symposium - Redmond, Washington, USA. 1-10. DOI: https://doi.org/10.1145/1837110.1837131.

4. Madhukar Kale, Prof. P.G. Gawande. 2015. Effective Fusion Mechanism for Multimodal Biometric System- Palmprint and Fingerprint. Vishwakarma Institute of Information Technology, Pune, India. Vol. 1. 215-218.

5. M.Gayathri, P.Selvakumari, R.Brindha. 2014. Fingerprint and GSM-based Security System. IJESRT. Vol. 3. 1-6.

6. H. I. Seng Chun Hoo. 2019. Biometric-Based Attendance Tracking System for Education. Journal of Sensors. 1-25. DOI: https://doi.org/10.1155/2019/7410478.

7. Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar. 2013. Wireless Fingerprint Based Security System Using Zigbee Technology. International Journal of Inventive Engineering and Sciences (IJIES). Vol. 1. 14-17.

8. Ashbourne, Julian. 2002. Biometrics: Advanced Identity Verification. Springer London. Vol. 2. 10-34.

9. Muhammad-Bello B.L., Alhassan M.E., Ganiyu, S.O. 2015. An Enhanced ATM Security System using Second-Level Authentication. International Journal of Computer Applications. Vol. 111. 8-15.

10. S. Prakasam,V.Padmapriya. 2013. Enhancing ATM Security using Fingerprint and GSM. International Journal of Computer Applications. Vol. 80. 43-46.

11. Jimoh R.G. and A. Babatunde. 2014. Enhanced Automated Teller Machine Using Short Message Service Authentication Verification. World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering. Vol. 8. 14-17.

12. Prof. Selina Oko, Jane Oruh. 2012. ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS. IJCSI International Journal of Computer Science Issues. Vol. 9.352-357.

13. M. C. K. M. M. R. Nisha Bhanushali. 2017. Fingerprint based ATM System. Journal for Research. Vol.02. 31-34

14. Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani. 2012. ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. (IJACSA) International Journal of Advanced Computer Science and Applications. Vol. 03. 68-72.

15. Atar Nasrin 1, Awatade Vidya 2, Hegadkar Rani 3, Bansude Vijaysinh 4. 2016. Fingerprint Based Security System for Bank. International Research Journal of Engineering and Technology (IRJET). Vol. 03.

16. Sri Shimal Das, Smt. Jhunu Debbarma. 2011. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. International Journal of Information and Communication Technology Research. Vol. 01. 197-203.

Appendix A

Appendix

Appendices words	Description
ATM	automated teller machine (ATM) or cash machine (in British English) is an electronic telecommunications device
Passcode	a string of characters used as a password, specially to gain access to a computer or smartphone
Biometric	relating to or involving the application of statistical analysis to biological data
Nominee	a person who is nominated as a candidate for election or for an honor or award
B.Sc.	Bachelor of Science.
CSE	Computer Science and Engineering.
Access	opportunity to approach or enter a place.
Research	the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions
Supervisor	a person who is in charge of overseeing a person or an activity.
Technology	the application of scientific knowledge for practical purposes, especially in an industry
Method	a particular procedure for accomplishing or approaching something, especially a systematic or established one.

“Be secure like a fingerprint-based *ATM Baking system. Just withdrawal money and makes it empty. Or deposit cash and ensure today’s security.”*