IJSRM
INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH METHODOLOGY
An Official Publication of Human Journals

Human Journals
Review Article
April 2024 Vol.:27, Issue:4

An Innovative Security Approach for ATM-assisted Banking Operations: The Fingerprint Biometric Roadmap

IJSRM
INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH METHODOLOGY
An Official Publication of Human Journals

Anthony I. Otuonye[1], Ifeanyi Ebiringa[2], Patricia O. Onyechere[3], Edith C. Otuonye[4], Perpetual N. Ibe[5]

[1,2]Dept. of Information Technology, Federal University of Technology, Owerri, Nigeria

[3]Dept. of Management Technology, Federal University of Technology, Owerri, Nigeria

[4]Registry Unit, Federal University of Technology Owerri, Nigeria

[5]Dept. of Computer Science Technology, Imo State Polytechnic Omuma, Nigeria

Submitted: 21 March 2024

Accepted: 27 March 2024

Published: 30 April 2024

HUMAN JOURNALS

ijsrm.humanjournals.com

Keywords: Biometric Authentication**,** ATM, Banking Services, PIN Code, Fingerprint Verification.

ABSTRACT

The use of the Automated Teller machine (ATM) for easy and convenient banking transactions has gained widespread acceptance in most developing nations based on the 24-hour service it provides to the teaming bank customers. For more than a decade now since the introduction of the Automated Teller Machine in Nigeria, for instance, it has become the favored channel of financial transactions. However, the expanding and wide acceptance of the ATM by members of the public has necessitated the need to further build and enhance the security and integrity of the system. It is obvious that impostors and robbers have infiltrated the banking industry with a view to defrauding users of the ATM machine. The PIN code password and current authenticated mechanism for ATMs no longer provide enough security for the system since it is now easy to steal the PIN codes from their real owners, as well as stealing their ATM cards to make withdrawals. In fact, the limitations of the 4-digit PIN code authentication approach are quite glaring, ranging from the fact that it cannot correctly verify the holder's identity, to its inability to protect the card against theft. Above all, it cannot protect bank customers from vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machine locations. For the fact that the security of this system is easily broken and maneuvered by fraudsters, it has called for a more secured method of authentication at the ATM terminals. This research paper therefore seeks to proffer a reliable solution to the lingering challenges of the current 4-digit Personal Identification Number for our ATM-based banking services. For a more reliable authentication, we are making a proposition for a combined PIN code verification with a fingerprint biometric scheme. The study will critically explore the existing password-based system to identify the associated limitations and to justify the need for a two-level security enhancement at the client's side. Research has shown that Biometric-based authentication systems will create a good roadmap to more secured ATM use in the banking sector. The fingerprint-based identification, specifically is one of the most matured and proven biometric approaches among others. This approach is currently being used as security variables for e-voting, and for controlling access to highly secured places like offices, equipment rooms, control centers and so on. It is hoped that a diligent application of our recommendations in this research paper will help to overcome our security challenges in the banking sector.

1. INTRODUCTION

In the time past, Financial Institutions in most developing countries carried out most of their banking transactions manually, and as a result, there was obvious inefficiency, long queues in the banking halls, and a waste of precious time and effort for most bank customers. By the fast wind of IT sweeping through across the globe however, banks now make use of several electronic devices such as the Automated Teller Machine (ATM) for banking transactions without the physical presence of a bank official.

An ATM installation, as a mechanical device that has its roots embedded in the accounts and records of a banking institution, allows a bank customer to carry out most of the basic banking transactions including fund deposits, fund transfers, balance enquiries, request for bank statements, cash withdrawal, and so on. As at today, the ATM has gained wide-spread acceptance in most countries as at today owing the 24-hour service it provides to the teaming bank customers [9].

More than decade now since the introduction of the Automated Teller Machine in Nigeria for instance, it has become the favored channel of financial transaction by most Nigerians. However, the expanding and wide acceptance of the ATM by members of the public has necessitated the need to further build and enhance the security and integrity of the system. It is obvious that impostors and robbers have infiltrated the banking industry to defraud users of the ATM machine. The PIN code password and current authenticated mechanism for ATMs no more provide enough security for the system since it is now easy to steal the PIN codes of unsuspecting members of the public as well as their ATM cards to make withdrawals.

The use of the PIN code alone has many other limitations, ranging from the fact that it cannot correctly verify the holder's identity, to its inability to protect the card against theft. Above all, it cannot protect bank customers from vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machine locations.

The above limitations have called for a more secured method of authentication at the ATM terminals. Biometric-based authentication systems are potential techniques for a more secured ATM use in the banking sector in Nigeria. Specifically, among all other Biometric Approaches,

the fingerprint-based identification is one of the most matured and proven techniques of user identification.

Above all, biometric authentication systems can identify any individual in spite of variations in time, as well as provide strong authentication that can easily be implemented on existing systems. Finally, the fact that there are very less chances of two people having same fingerprint, this identification approach is quite reliable. Some of the fore-going advantages clearly underscore the surge in the use of Biometric-based user authentication system in recent years.

Biometric authentication using fingerprints is currently being used as security variables for e-voting, and for controlling access to highly secured places like offices, equipment rooms, control centers and so on. In this research work therefore, the authentication system being proposed is expected to be self-manipulative, simple, fast and much more secure.

Consequently, this study attempts to proffer a reliable solution to the lingering challenges of the current 4-digit Personal Identification Number for our ATM-based banking services. We propose a combined PIN code verification with a fingerprint biometric scheme for a more reliable authentication. Furthermore, the study promises to critically explore the existing password-based system to identify the associated limitations, and to justify the need for a two-level security enhancement at the client's side.

2. LITERATURE REVIEW

In this paper, we have reviewed a number of research works and other scholarly articles in the area of fingerprint biometric systems, and the security of banking operations in developing countries of the world. Other theoretical frameworks were also reviewed in this study that underscore the use and deployment of biometric authentication systems.

2.1. Empirical Framework for the Study

According to [15], the Automated Teller Machine (ATM) was introduced to automate the work of the traditional bank cashier and was designed to dispense cash to all identified bank customers. In some advanced countries, the ATM can take deposits of cash and cheques from customers as well as perform many other banking transactions such as paying of bills, cash transfer, recharge card and purchases, and so on. It is therefore an important aspect of the entre

banking sector and a very important phenomenon that has come to stay and cannot be ignored [15].

Another ATM framework was proposed by [10]. In their study, which was titled: "New Secured Architecture for Authentication in Banking Application", an embedded fingerprint system was utilized for ATM security applications. In their system, bankers collect customers' finger prints and cell phone numbers while opening accounts. The working of the ATM machine is such that when a customer places a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM by pressing the keys on the touch screen. After entering it checks whether it is a legitimate one or not and permits the customer further access if confirmed legit. [2] is also of the view that the issue of ATM frauds is a worldwide phenomenon and with its consequences on bank patronage, focusing the Nigerian state. According to the Author, this should be of concern to all the stakeholders in the banking industry. In his paper also, the author identified the dimensions of ATM frauds in Nigeria in particular and proposed possible solutions that will put ATM frauds in the Nigerian banking system under check. His paper employed both primary and secondary data to investigate the ATM frauds in Nigerian banks. The chi-square statistical technique was used to analyze the data obtained and test the hypothesis raised in the course of the analysis. The paper concludes that both bank customers and the bank have a joint role to play in bringing an end to the spread of ATM fraud in the banking industry. He further posited that card jamming, shoulder surfing and Stolen ATM cards constitute 65.2% of ATM frauds in Nigeria. [3] identified some ways by which fraudsters get PIN numbers from clueless cardholders by creating deceitful websites in which they post some fictitious prize in order to lure greedy customers (www.interswitchatmcard.com). On such sites, for instance, they ask customers to submit vital information which may include their PIN number. The Researcher equally reported that handheld devices that can read card information are available and has been used on a victim. According to the Researcher, certain cameras have actually been installed to record PINs as they are typed by the consumers. [11] proposed a biometric measure as a means of enhancing the security of banking system for both customer's and bankers, and advocated a total elimination of cards as the finger can serve as both password and access card.

Additionally, [12] proposed a fingerprint and PIN-based authentication arrangement to enhance the security and safety of the ATM and its users. The proposed system is a three-tier design structure in which the first tier is the verification module, concentrating on the enrollment phase, enhancement phase, feature extraction and matching of the fingerprints. The second tier is the database end which acts as a storehouse for storing the fingerprints of all ATM users preregistered as templates. The last tier presents a system platform to relate banking transactions such as balance inquiries, mini statement and withdrawal. The system is developed to run on Microsoft windows XP or higher and all systems with .NET framework employing C# programming language, Microsoft Visio studio 2010 and SQL server 2008. The simulated results showed a 96% accuracy.

Also, [6] proposed a system, which is used for ATM security applications, where Bankers are meant to collect the customer's fingerprints as well as their mobile number during an account opening process. When the customer enters ATM and after inserting his card, he must place a finger on the finger print module to get an automatically generated 4-digit code. This happens every time as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the touch screen, after only that he will be able for further transaction. In this research paper, we are of the opinion that this proposal will go a long way to solve the problem most of the problems earlier identified.

2.2. Review Summary

Our study has shown that ATM technology as a special tool for Electronic Banking Transaction, has come to stay. With the current trend of the cashless economy in Nigeria for instance, as well as in most developing countries, this approach is a step in the right direction. The ATM-based banking policy has actually rendered essential monetary services to bank customers in different nations. However, existing ATM machines that utilizes PIN (Personal Identification Number) is not highly secure as a means of authentication which has now resulted in an urgent need for more privacy and security at ATM terminals, and the fingerprint biometric feature is utilized for providing such security. The system exploits utilization of biometric database of individual as a password alongside PIN (Personal Identification Number). The security features are improved to

a great extent the stability and dependability of customer recognition. From a consideration of all authentication techniques so far reviewed in this work, both implemented and yet to be implemented, as well as from the issues identified with ATM machines, it can be reasoned that biometrics can be a good measure against ATM fraud in the Banking System.

3. CRITICAL CHALLENGES OF ATM-ASSISTED BANKING SERVICES IN DEVELOPING COUNTRIES.

3.1. Overview

ATM-assisted banking transaction is usually initiated by inserting a valid ATM card into the machine and providing the correct PIN (Personal Identification Number) for that specific card. Even though the bank allows their customers to choose their PIN, the system is not safe to use for the fact that anyone can access the system so long as they have access to the card and PIN number. Usually, the system verifies the code against a stored list of approved passwords of users. PIN codes are typically in the form of a four-digit combination of numbers and is entered via the ATM panel. If the code is correct, the system permits access at the security level approved for the bank account owner.

All that the cardholder needs to do is type in the PIN via the keypad on the ATM machine. If the PIN code is legitimate, access is granted to the user to perform any desired monetary transaction with the system.

As a security measure, however, the strength of the PIN is weakened by the likelihood of the code leaking out to others without the knowledge of the owner. In recent times, due to advancement in technology, fraudsters have gone as far as fixing ATM Card scanners in ATM Machine installations just to acquire encoded information from an ATM Card. By this acquisition, a copy of the ATM card can be created for the purpose of making fraudulent transactions. This is the primary impediment of the current system. Our ATM machines today are no more secure and the PIN code alone now poses great limitations to its use.

3.2. Major Limitations

Research has shown that the use of ATM cards and its associated PIN code as password now pose high level limitations. The following major limitations have been identified:

i. Inability to verify the Card Holder's Identity. The PIN code authentication system lacks the ability to discriminate between the card owner and an impostor who fraudulently obtains access privileges and the real account owner.

ii. The system cannot protect the ATM card against theft.

iii. Cannot protect bank customers from vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machines locations.

iv. It is easy to illicitly acquire passwords and PIN codes from card owners.

v. PIN code passwords are easily guessed with little effort such as birthday.

vi. Under duress, a card holder can easily be forced to release his PIN code to fraudsters.

vii. Malware can be placed at the ATM terminal by fraudsters to capture magnetic stripe data and PIN codes from the private memory space of transaction processing applications installed on the ATM, and so on.

The limitations as listed above have called for a more secured method of authentication at the ATM terminals. Biometric-based authentication systems are potential technique for a more secured ATM use in the banking sector.

4. OVERCOMING THE IDENTIFIED CHALLENGES FOR A MORE SECURED ATM-BANKING SERVICE

4.1. The Combined Fingerprint Biometrics and PIN Code Initiative

There are many advantages to the use of biometrics as a form of identification for access control. Some of the known merits of the Biometric systems include:

a. Biometric variable cannot be lost: You can always forget your key, access card or password, but you cannot forget your fingerprints or your eyes. If biometrics are the only means of authentication, a user can never be locked out if they are entitled to access. If you use multi-factor identification, a biometric factor is one less thing that users need to remember.

b. Biometric variables cannot be transferred or stolen: It is easy and not uncommon for people to leave access cards or notepads containing passwords lying around where unwanted personnel could get their hands on them. You cannot lose your biometrics due to carelessness, and they cannot be transferred or stolen without causing physical trauma to the user.

c. Biometric systems are person-specific: Unless a user is colluding with an unauthorized person, you can be confident that the person who is using biometrics to gain access is who they purport to be.

d. The are intuitive: Most users should have little difficulty figuring out how to press their finger onto a fingerprint scanner or look into an eye scanner. This process can be much faster and more convenient than hunting around for another password or trying to find the right way to insert an access card.

e. Different organizations have the option to make use of different kinds of biometrics according to their individual preferences. Some, for instance, may prefer fingerprint identification because it's more recognizable and user-friendly than certain other methods.

f. While you can use multiple biometrics for identification, in most cases currently, a single biometric when paired with some other authentication factor — like a key card, push notification or password — is sufficient for a secure access [15].

4.2. Analysis of the Existing 4-Digit PIN Code System

Normally, the PIN code is a four-digit combination of numbers of desired choice which is chosen after the ATM card has been given to client with a default PIN which users are encouraged to change after an initial use. Frequently used PINs are 4-digit numbers which are usually in the scope of 0000-9999 ensuing in a sum of 10,000 conceivable numbers, so an assailant would have to guess a total of 5000 times to really get the correct and right PIN. You type in your PIN via the keypad on the ATM. If the PIN code is legitimate, access is granted to the user to perform any desired monetary transaction with the system.

4.3. Design Framework for the Proposed System

a. Use case Diagram of the New System

A use case diagram is used to model the interaction between the system and the intended user. They help us to fully understand the system requirement and its instrumental in project development, planning, and documentation of system requirements. They also show the activity of the users and the responsibility of the system to its users as well as the uses of the system. It also shows the sequence of actions that can be performed within the system boundaries. In essence, the use case model tries to systematically identify both the uses and the users of the system and provides an external view of a system or application; it is directed towards the users or the "actors" of the systems, not its implementers.

In the design of the banking ATM application, the actor of the bank system is the bank customer. Figure 4.1. shows the use case diagram for the system design, where customers can perform transactions by inserting their ATM card and carry out the Approval Process by entering a PIN Number and making a confirmation via the Fingerprint. After the approval, customer is asked indicate the type of transaction they may wish to perform such as Cash Withdrawal or cash transfer. Then the transaction is carried out accordingly. After the transaction, the customer exits the Application and removes his/her card.

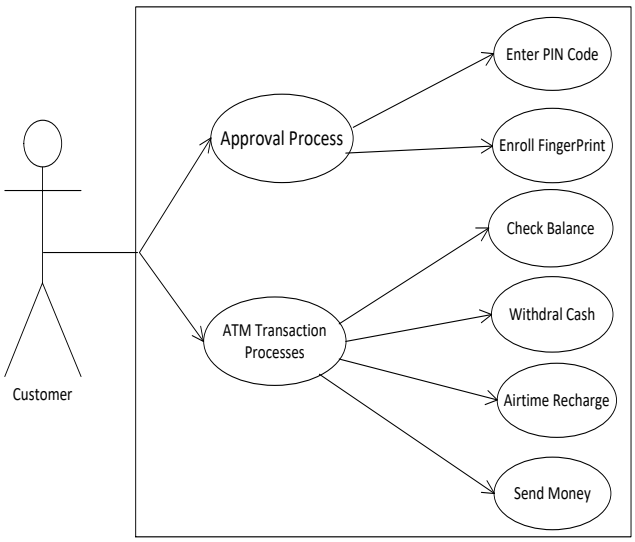

Figure 4.1 Use case diagram for the proposed ATM system.

b. Activity Diagram of the New System

The Activity Diagram in figure 4.2 shows a detailed description of the system. The business models of ATM transactions are highlights as card insertion, PIN validation, Fingerprint validation, transaction, withdrawal, deposit, fund transfer, fast cash, mini statement, and a successful removal of the ATM card after completion. An Activity Diagram is a component of the Unified Modeling Language that represents the graphical workflows of stepwise activities and actions with support for iteration, choice and concurrency, thus showing the overall flow of program control.

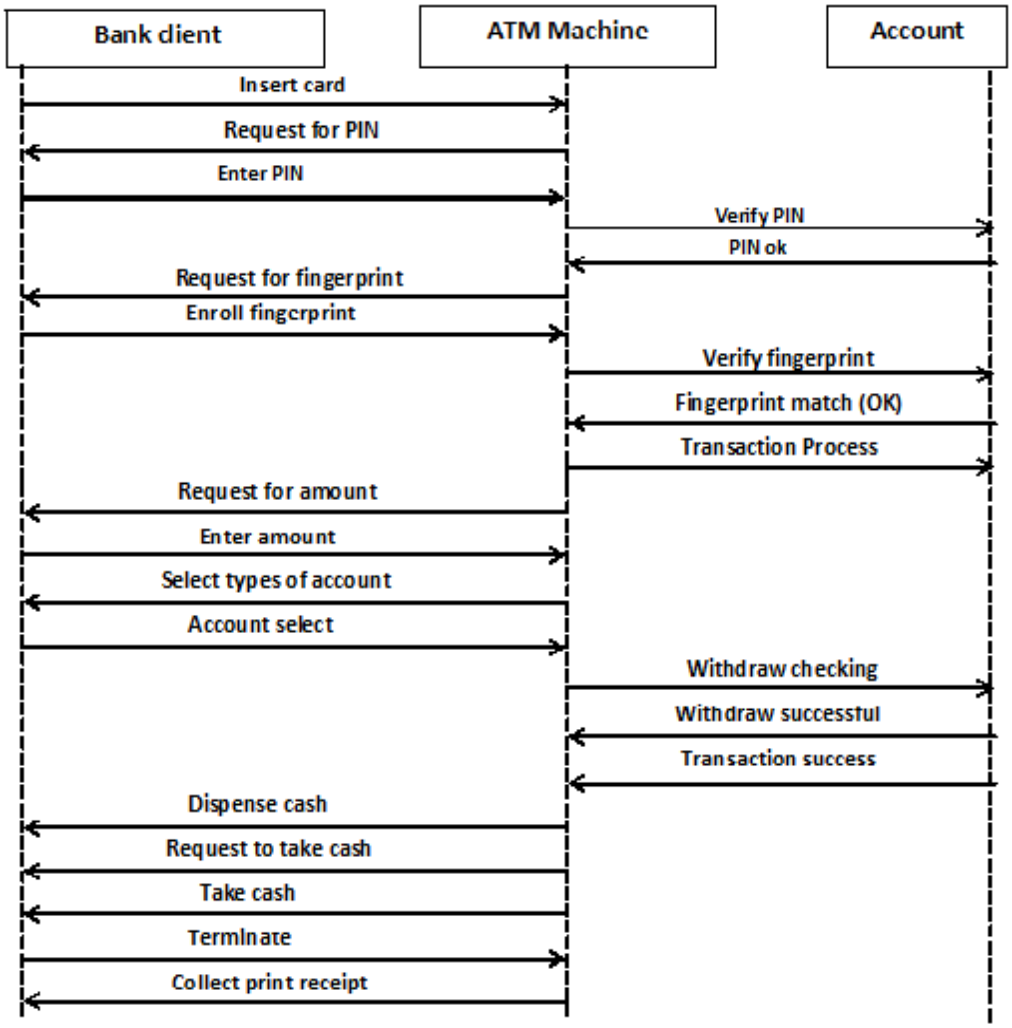

Figure 4.2. Activity Diagram of the proposed ATM

c. Flowchart of the New System

Flowcharting is a method of designing a solution to a problem by using symbols that indicate actions to be performed. It is customary to use geometric figures of certain shapes to indicate the various kinds of acts. In a flowchart these figures are diagrammed with connecting arrows, indicating a certain sequence for performing the acts in order to solve a problem. Figure 4.3. below is a program flowchart that shows the relationship between Bank client, ATM machine and the Database engine.

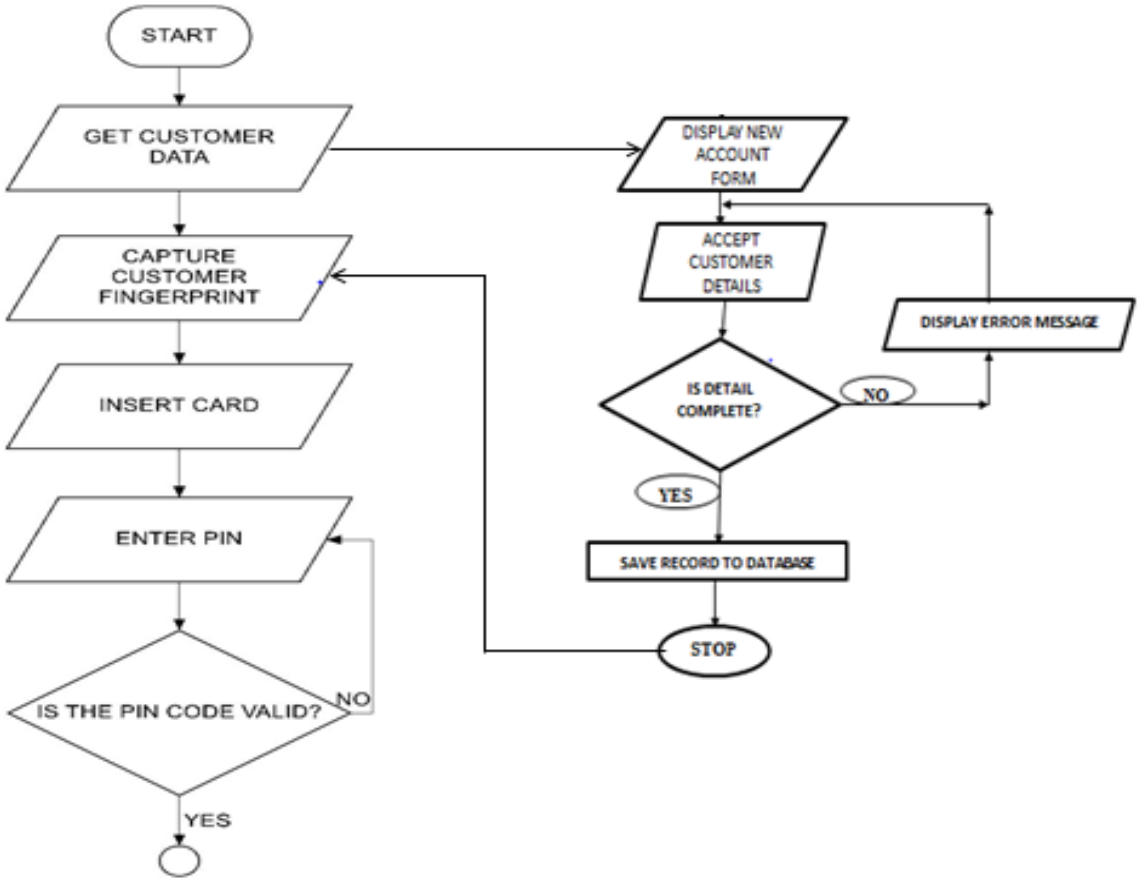

Figure 4.3. New System Flowchart

5. CONCLUSION AND RECOMMENDATIONS

In this section, we present our conclusion and recommendations for this study as well as results obtained at the various stages of this study.

5.1. Conclusion

The automated teller machine has come to stay and has the potential to trigger efficiency in banking operations if well applied. The fingerprint recognition technique has kept on gaining public acceptance as an accurate way of verifying identity. This paper has proposed a high-level model for the adjustment of traditional ATM security framework to utilize both the PIN security protocols and the Biometric fingerprint protocol to achieve better security. The Fingerprint authentication approach can be used as a biometric measure to upgrade the security peculiarities of the ATM for effective banking transactions, especially for a more reliable E-banking operation across developing countries. The model specimen of the developed application has been found exceptional on account of its sensitivity to recognition and identification of customers' fingerprints. This system when fully deployed will reduce the rate of fraudulent activities on ATM-based banking services such that only a registered owner of the card can have access to this/her bank account.

5.2. Recommendations

Fingerprint recognition is a reasonable way out of the lingering menace of Identity theft occurring at ATM terminals. When augmented with the current PIN code system, it will bring about an efficient and well-secured framework. The system can be quite user-friendly, simple to utilize, and exact. We therefore make the following recommendations stakeholders and to all ATM cardholders.

1. In the adoption of the proposed system, ATM Cardholders should ensure that they protect their Fingerprint impression from damage due to accidents.

2. ATM cardholders should use trusted relatives or friends as their nominee or alternate user.

3. Governments across developing countries should enact relevant laws to punish offenders and to discourage potential fraudsters from getting involved in bank-related fraudulent activities following the undeniable punishment it will attract.

REFERENCES

[1] Abhishek, R.L. and Nitin, C. (2021). Implementation of Recent Security Mechanism over Secured ATM Transaction. Retrieved from:
http://www.techrepublic.com/resource-library/whitepapers/implementation-of-recent-security-mechanism-over-secured-atm-transaction/
[2] Adeoti, S. (2011). An Ideal ATM Implementation in an Unsecured Environment, University of Jos, Ota Nigeria. Retrieved from:
http://dspace.covenantuniversity.edu.ng/bitstream/handle/123456789/169/An%20Ideal%20ATM%20Implementation%20in%20an%20Unsecured%20Environment.pdf?sequence
[3] Chioma J. (2020). ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. Retrieved from" http://connection.ebscohost.com/c/articles/89252739/atm-security-using-fingerprint-biometric-identifier-investigative-study
[4] Duvey, A.A. (2014). ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology: Pravara Rural engineering college, Loni, Maharashtra, India. Retrieved from:
http://www.ijetae.com/files/Volume4Issue2/IJETAE_0214_147.pdf
[5] Hamzat, O. (2011). Simulation of an Automated Teller Machine (ATM) System with Cash
Deposit Capability: Unpublished B.Sc. research work, ABU Zaria, Nigeria.
[6] James Wayman (2022): An Introduction to Biometric Authentication Systems, Retrieved from:
http://www.techrepublic.com/resource-library/whitepapers/implementation-of-recent-security-mechanism-over-secured-atm-transaction/
[7] Jaspreet, K. and Sheenam, M. (2014). An Overview of ATM Security Using Biometric Technology: Fatehgarh Sahib, Punjab, India. Retrieved from: http://www.ijarcsse.com/docs/papers/Volume_4/3_March2014/V4I3-0333.pdf
[8] Peter, A. and Sylvia, I. (2008).Report on the Literature Study of Iris Biometric Recognition:
Linköpingsuniversitetet, Sweden. Retrieved from: https://www.ida.liu.se/~TDDD17/oldprojects/2008/projects/6.pdf
[9] Khatmode R, K. (2014). ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology: Pravara Rural engineering college, loni, Maharashtra, India. Retrieved from:
http://www.ijetae.com/files/Volume4Issue2/IJETAE_0214_147.pdf
[10] Senthil, K. K. and Vijayaragavan S. (2014). New Secured Architecture for Authentication in Banking Application: Paavai Engineering College, Nammakal, India. Retrieved from:
http://www.ijirset.com/upload/2014/february/23_New.pdf
[11] Ogunsemore, M. (2019). The Formal Design Model of an Automatic Teller Machine. Retrieved from: www.crimtrac.gov.au/our_services/FingerprintAnalysis-TheBasics.html
[12] Selina O. O. (2012). Enhanced ATM Security System Using Biometrics. International Journal of Computer Science Issues.
[13] Sri Shimal, D. and Jhunu, D. (2016). Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System: Tripura Institute of Technology, Retrieved from http://esjournals.org/journaloftechnology/archive/vol1no5/vol1no5_3.pdf
[14] Santhi B., and Kumar R.K. (2020). A Novel Hybrid Technology in ATM Security Using Biometrics. Journal of Theoretical and Applied Information Technology
[15] Vacca John R. (2017): Biometric Technologies and Verification Systems Retrieved from:
http://www.techrepublic.com/resource-library/whitepapers/implementation-of-recent-security-mechanism-over-secured-atm-transaction/