DESIGN OF A MULTIFACTOR AUTHENTICATION SYSTEM FOR AUTOMATED TELLER MACHINES

BY

PETER KIBAYA

This research proposal is submitted in fulfillment of the academic requirements for the degree of Master of Engineering in Information and Communication Technology Security In the School of Engineering.

THE UNIVERSITY OF ZAMBIA

2023.

COPYRIGHT DECLARATION

All rights reserved. No part of this dissertation may be reproduced or stored in any form or by any means without prior permission in writing from the author or the University of Zambia.

As the candidate's supervisors, I have approved this research proposal for submission

Name: Charles S Lubobya

Signed:_____

Date:_____

DECLARATION

I declare that this research proposal is my own work. Where collaboration with other people has taken place or material generated by other researchers is included, the parties and/ or materials are explicitly stated with references as appropriate.

This work is being submitted for the Master of Engineering in Information and Communication Technology Security at the University of Zambia. It has not been submitted to any other university for other degrees or examinations.

_____	**5th November, 2021**
Name	**Date**

CERTIFICATE OF APPROVAL

This dissertation of Peter Kibaya has been approved as fulfilling the requirement for the award of Master of Engineering in Information and Communication Technology Security by The University of Zambia.

---------- ---------- ----------
Examiner 1 Signature Date

---------- ---------- ----------
Examiner 2 Signature Date

---------- ---------- ----------
Examiner 3 Signature Date

---------- ---------- ----------
Chairperson Signature Date
Board of
Examiner

---------- ---------- ----------
Supervisor Signature Date

DEDICATION

To my late father Mr Peter Kibaya Snr, for always believing in me and supporting me through the highs and lows of my academic journey, thank you for being a present and loving father.

ABSTRACT

This research aims to design a multi-factor authentication system for automated teller machines (ATMs) that incorporates biometric fingerprint data and One Time passwords. This is so as to reduce the impact and subsequent loss by customers to card frauds.

Banking transactions conducted through automated teller machines (ATMs) are vulnerable to fraud and identity theft. Implementing multifactor authentication (MFA) can significantly improve the security of ATM transactions. ATM debit and credit cards are susceptible to theft and card cloning making them a conduit for malicious actors to defraud bank customers. In this design, we propose the use of fingerprint authentication and One Time Passwords (OTPs) as a second and third factor in the MFA process. By requiring the user to randomly provide any one of the 10 fingerprints, OTP and the 4-digit PIN, the risk of fraudulent transactions is greatly reduced. We present a detailed design for integrating fingerprint authentication technology and OTPs for transaction authentication, including user enrolment, fingerprint capture, and verification processes. Overall, the proposed MFA system using fingerprint authentication has the potential to greatly enhance the security of ATM transactions and protect against fraudulent activity.

The design aims to capture customer fingerprint data upon account opening as well as an ongoing Know Your Customer (KYC) exercise and map these to customer accounts. Users are then authenticated through a randomised mechanism that picks any one of the 10 fingerprints samples at each authentication request, requests a PIN for final authentication and an OTP for transaction authorization.

ACKNOWLEDGEMENTS

My sincere appreciation goes to my wife Zewelanji Deidre Simwanza thank you for the support and encouragement during this journey, thank you for being the pillar you continue to be.

My supervisor Dr Lubobya for his guidance, support, and encouragement during the course of my study at the University of Zambia. My gratitude also goes to Dr Simon Tembo, Mr Shabani, Dr B. Habeenzu, for their warm help in my research work.

I would also like to thank my classmates Mr Nelson Lungu, Kamayoyo Mufuzi, Johannes Mundia and Alice Mercy Zulu.

A mighty thanks to my siblings for always believing and supporting me Mabel Kibaya, Cleopatra Kibaya, Mildred Kibaya, Bernard Kibaya and Nancy Kibaya

Thanks to my family for their prayers and encouragement.

I also appreciate the critique and advice from the members of my class and for reviewing my work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

3FA	: Two Factor Authentication
ATM	: Automated Teller Machine
OTP	: One Time Password
CBS	: Core Banking System
POS	Point Of Sale
VBV	Verified By Visa
CVV	Customer Verification Value
CVC	Customer Verification Code
KYC	Know Your Customer
HSM	Hardware Security Module
MFA	Multi Factor Authentication
AES	Advanced Encryption Standard

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1 Introduction

The principles of the research effort are introduced in this chapter, with a focus on the background, problem statement, and rationale for the research, as well as the significance of the research, its scope, ethical considerations, and operational definitions of the research work. The main goal of the study and the necessity to fill the knowledge gap in the field of multifactor authentication for automated teller machines in the Zambian banking sector are highlighted in this chapter. To avoid many security issues on POS and ATM terminals in the banking industry, multi factor authentication is essential.

Over the past three decades, the banking industry in Zambia has undergone a significant transformation from manual procedures to investments in automated processes with enormous investments in ICTs to have a competitive edge over rivals. Nearly all commercial banks in Zambia have ATMs due to the steadily increasing demand from customers to access their money. Despite calls for the nation to be less cash-dependent, it is evident that there is a demand for genuine currency.

There are numerous threats posed to the banking sector and a significant risk factor is attributed to ATM card fraud.

Some of the potential threats are.

1. Shoulder surfing, this is where a perpetrator peeks over the shoulder of a victim in order to see their PIN [1].

Figure 1 Shoulder surfing at an ATM [2]

2. Contactless Cards, the threat posed by Contactless cards is that Payments maybe be made to a certain limit without the authorisation from the rightful owner of the card and account. [3][4]
3. Spyware, Perpetrators may place a small camera at the ATM in order to capture customers' [5] [6]
4. Skimming, sophisticated equipment may be used to capture user data on the magnetic strip of the card, these devices are placed on the ATM's card reader, and perpetrators proceed to produce replica cards in order to access the victim's account. Skimming is a method of stealing card information by attaching a device to an ATM that captures the data from the card's magnetic stripe. This data can then be used to create a counterfeit card that can be used to withdraw cash from the victim's account. Card stealing can occur when criminals find lost or stolen cards and use them to withdraw cash from ATMs. Another form of ATM card fraud is using counterfeit cards. These cards are created using stolen card data and can be used to withdraw cash from ATMs [7] [8]

Figure 2 POS machine card skimmer/cloner [9]

Figure 3 ATM card skimmer [10]

5. Lost or Stolen cards pose a threat as malicious individual may either clone the cards or proceed to make online payments with the customers' authorization. [11]

6. Card Trapping/Phishing, attackers use fraudulent card readers that are placed on the ATMs card reader, these devices capture the customer's card, deceiving them into thinking the card has been captured by the machine when in fact not. [7]

It is evident from the above identified and cited threats to the current system in the banking sector, measures need to be implemeted that factor in multifactor authentication for ATM and POS transactions in order to enhance security.

1.1. Background

There is absolutely no doubt that security in the Automated Teller Machine (ATM) network and card system is paramount. With the advancement of technology and knowledge on the internet, adversaries have continued to come up with ways and means of bypassing the safe nets of ATM transactions and accessing user accounts. Major card companies such as VISA and MASTERCARD have chip and PIN cards which aim to provide the much-needed security than cards without chips, this is because of the high level encryption provided by the Chip and PIN concept [12]. However even with this in place, ATM/POS transactions are not 100% immune to card fraud. For instance, once in possession of your card, a malicious person could carry out online transactions using the card Number and CVV/CVC because services such as VBV (Verified by Visa) [13] are not mandatory for vendors to implement on their e-commerce sites for legitimate users to authorise transactions as some transactions may bypass this safeguard. VBV is a security feature that gives online credit and debit card transactions an additional measure of security. By requesting further authentication from the cardholder before the transaction is allowed, it is intended to prevent fraudulent use of a card.

How Verified by Visa functions is as follows:

1. The option to sign up for Verified by Visa will be presented to you when you make an online purchase from a participating retailer. Typically, this entails setting up a username, password, or responding to security queries.
2. After enrolling, extra authentication will be needed before you may make online purchases from participating retailers. You can accomplish this in several ways, including by entering a one-time code that was provided to your phone or email, or by using a biometric scanner on a device to recognize your face or fingerprint.

3. The transaction will be accepted, and the sale will go forward if the extra authentication is successful.

Overall, by demanding additional validation before transactions are allowed, Verified by Visa helps to guard against fraudulent use of a card. By doing this, the possibility of fraud may be decreased, and the security of online card transactions can be increased.

Also, in cases where a once trusted person that may know the ATM PIN may at any time get possession of the ATM card without the knowledge of the card holder and be able to make ATM withdraws and POS transactions.

This research will focus on the design of an ATM 3FA (Three Factor Authentication System) using a 4-digit PIN, fingerprint biometric data and OTPs. This design aims to curb the challenges faced by the current ATM set up. A basic ATM network comprises of an ATM, a Transaction switch to handle the transactions and the core banking system. Information is exchanged between the ATM and the CBS through the Transaction switch.

1.1 Problem Statement

Zambia is a highly cash dependent country,hence most bank account holders access cash via ATMs. This high dependance on cash makes most bank account holders make them prone to ATM card frauds.

The magnetic strip still in use today even on CHIP based cards makes them all prone to cloning/Skimming. [4][12]

Stolen cards/ stolen card information can be used to make online purchases using card details such as card number, date and CVV/CVC.[13]

Contactless cards which enable users to transact without the need for a PIN gives malicious actors the ability to make unauthorised payments/purchases.[15]

Fraudsters can bypass safety nets such as VBV for stolen cards or stolen card details becuase such mechanisms are no mandetory for ecommerce sites to implement.[13]

The implementation of a randomised mechanism of finger print authentication, PIN and One time passwords could provide the advantages of both going cashless and having one’s funds safe.

1.1.1. Advantages and Disadvantages of ATM debit cards

ATM cards come with benefits and drawbacks. They come with some risks, but they can also be a reasonable way to get money.

Among the benefits of using an ATM card are:

Convenience: ATM cards allow users to withdraw money from machines at any time, day or night. In an emergency or when you require rapid cash, this can be useful.

Anytime, day or night, ATM cards can be used to withdraw money from an ATM. In an emergency or when you require rapid cash, this can be useful. You can access the money in your checking or savings account with an ATM card. If you need to make a purchase but don't have any cash on hand, this may be beneficial.

You can use an ATM card to access the money in your savings or checking account. This may come in handy if you need to buy anything but don't have any cash on hand. Safety: It is generally safer to carry an ATM card than cash. You can inform your bank and request the cancellation of your ATM card if you lose it.

Nevertheless, there are certain drawbacks to using an ATM card, such as:

Fees: For using an ATM, many banks impose fees, particularly if you use one that is not connected to your bank. It's critical to understand these fees because they might mount up.

Someone could access your account and withdraw money if you lose your ATM card if it is stolen. This can put you in a precarious financial position. Access is restricted: ATM cards can only be used in establishments that accept them to withdraw cash or make purchases. If you need to make a purchase but there isn't an ATM nearby, this may be inconvenient.

Overall, using an ATM card can make it easier to get cash, but there are also certain risks. Before selecting if an ATM card is best for you, make sure to consider the advantages and disadvantages.

1.2 Research Aim

With a yearly increase in card based fraudulent activities there is a great need to address the disadvantages of ATM debit and credit cards. In an event that an ATM card is stolen, with only the CVV/CVC, unauthorised online payments may be made

against the funded account. Lost/Stolen ATM contactless cards, if not reported stolen, can still be used to make payments without the owner's consent [4]. This research is aimed at highlighting the loopholes in the security of ATM debit/Credit cards from fraudulent card activities as well as to contribute towards the advancement of ATM security using Biometric fingerprint data.

1.3 Application of the Research

ATM cards have evolved with time, with new security features such as the Chip has seen a reduction in the number of card fraud activities. The Chip and PIN implementation is a more secure means of ATM and POS transactions as high-level encryption is involved as opposed to the magnetic strip that stored data in an unsafe manner. [16]

The introduction of contactless cards has not gone without risk; contactless payments may be made without authorization from the intended card owner. Also, contactless cards still use the magnetic strip as card companies have not yet fully eliminated it, this makes them susceptible to the same risks as cards without the chip.

This research is aimed at offering a solution to the day-to-day challenges of carrying ATM cards and the risk that comes with it in the event of theft or one loses it. I strongly feel, the way to have more secure POS and ATM transactions, we not only need to be a cashless society but also a card-less one. Each individual has unique fingerprints, even identical twins have completely different prints [17] This research aims to harness this uniqueness to ensure safe and convenient POS and ATM payments.

1.4 Research Objectives

The main objective of this project is to design a model of an ATM/POS 3FA System using Biometric fingerprint data, 4-digit PIN and OTPs for the University of Zambian community and those living outside the campus. The specific objectives shall be to:

1) To design a biometric ATM system with randomised fingerprint authentication capability.

2) To introduce a system of One Time Passwords for transaction authentication.

3) To introduce a secure cardless system to replace the use of conventional debit/credit cards.

1.5 Research Questions

In this research, we will address some questions regarding our proposed ATM/POS MFA System using Biometric fingerprint data, PIN and OTPs. The fundamental questions at the core of this research are:

1) How will the fingerprint data be captured and translated so that the ATM Transaction switch will understand, interpret and authenticate against other stored biometric data.
2) How will the system further enhance secure cardless ATM/POS transactions.
3) How will the system prove to be better than the conventional card-based ATM/POS transactions.

1.6 Significance of the study

With an increase in the number of card-based transactions and the consequent number of card fraud cases, there rises a need to ensure that the accounts and funds of bank customers are secured by all means possible. The realm of biometrics and technology has played a great role in enforcing measures to curb forced entry from malicious people / hackers [18]. This is due to the uniqueness of fingerprint data. No one individual has matching fingerprints with another individual, not even identical twins have the same fingerprints. This feature makes it ideal for identifying bank customers as well as authenticate them [19].

It is pertinent to note that ATM cards have security features that have improved over the years, but all have not been without risks. Users sometimes tend to keep their cards with their PIN together, this is in a case when a PIN was issued and written on a piece of paper for the customer alone to know, there is also a reluctance on the part of customers to change their ATM pins regularly. Also, many customers normally opt to pick their year of birth as first choice for a PIN. This could be maliciously obtained [20] or easily be guessed if a wallet or purse were to be stolen/found by a malicious individual. Chip and Pin cards and Magnetic strip cards may easily be cloned [6] and contactless cards may permit PIN free transactions to

the limit set by the acquiring bank overriding any limits placed by the issuing bank on the customer cards[3][21]. A lot of risks still exist with the ever-changing ATM debit and credit card standards, hence the usage of fingerprint data would bridge this gap and greatly reduce the risk and potential loss on the customer.[22]

1.6.1. Why Use OTP

OTPs have been used in the authentication space as is curtails the aspect to guessing by a malicious individual wanting to access a user's account. OTPs are safe since they can only be used once, and they are frequently used in conjunction with other security measures like a user's login information (such as a username and password) to add an extra layer of security.

Here are several ways that OTPs can improve security.:

1. They cannot be reused: An attacker who intercepts an OTP would not be able to utilize it to enter a system because OTPs can only be used once.
2. They are difficult to predict: It is extremely challenging for an attacker to guess the right OTP because OTPs are normally created using a secure algorithm and are frequently lengthy and complex.
3. They are often transmitted through a different channel: OTPs are frequently sent to a user's phone number or email address, which adds an extra degree of security because a hacker would also need access to the user's phone or email account in order to guess the OTP.
4. OTPs are stored in a database as they are valid for one time use only, this makes them immune to attacks such as key logging and brute force attacks. [23] [24].

Overall, OTPs are an effective way to secure systems and protect against unauthorized access, particularly when used in conjunction with other security measures such as a strong password

1.6.2. Why use Fingerprint authentication

The use of fingerprint data for the purposes of authentication is to harness the attribute of being distinct from person-to-person. The unique traits of fingerprints is because of a characteristic known as minutiae which are simply curve track finishes. Due to how much harder it is to fabricate a fingerprint than it is to guess or steal a static PIN, fingerprint authentication is typically regarded as being more secure than static PIN authentication. While a static PIN may be

quickly and easily determined using numerous techniques like social engineering or shoulder surfing, a fingerprint is a unique physical trait that is exceedingly difficult to duplicate. Even though ways to copy one's fingerprints such as wax copies exist, the proposed system circumvents this by utilizing all 10 fingerprints and requesting the users' prints at random. [25][19]

1.6.3. Why use Multifactor authentication (MFA)

MFA is simply the combination of more than one way to identify a user, MFA usually comprises of something the user has such the OTP, what the user knows., such as PIN and who the user is such as Fingerprint in our case. This makes it difficult for malicious actors to compromise and eventually have access to users' accounts. [26] [27]. MFA is a security procedure where a user must supply numerous pieces of proof (or "factors") in order to prove their identity. In order to access sensitive systems or data, an attacker would need to breach a number of criteria, which can help to lower the risk of unauthorized access.

There are several advantages to using MFA:

Enhanced security: Multiple authentication factors (MFA) make it far more difficult for hackers to access a system since they must compromise several factors rather than just one.

1. Protection from credentials being stolen: Even if a user's login information, such as their password, is stolen, MFA can still stop a hacker from accessing the system since they lack the second necessary element (s).
2. Greater convenience: MFA eliminates the need for users to remember several sets of login credentials for various systems by replacing them with just one single pair (for example, a username and password).
3. Better compliance: MFA is frequently necessary for compliance with rules or business requirements that demand strong security measures.
4. MFA can, in general, give an extra layer of security and safeguard against unauthorized access to sensitive systems.

1.7 Scope of the Project

The following are the limitations that delineate the scope of the project.

1) This research does not include individuals with damaged or missing fingers, loss through accident or congenital.

2) Individuals involved in heavy labour-intensive jobs with their hands tend to have their fingerprints change with time as well as cuts or scars may affect the detection of an authentic fingerprints.
3) The system is not immune to noise and distortion due to dirt and twists, this could affect the authentication of the user.
4) The system is unable to distinguish between an authentic fingerprint and an artificial finger made out of wax
5) This is research is purely simulated and as such does not include any physical components or works done on a physical ATM/POS terminal neither does the simulation involve transactions routed through external payment systems such as VISA, Master Card, Union Pay as the simulation and implementation of that is beyond the scope of the project etc.
6) The research is also limited to only ATM and POS transactions and does not include online card payments.
7) The simulation is merely a proof of concept and does not include critical aspects of the transaction flow such as the Transaction switch, CBS and HSM but only simulates aspects of the Switch that are relevant to the research.

1.8 Ethical Considerations

In ensuring that the objectives of the research are met, the researcher shall not.

1. Experiment with any Automated teller machine without any prior approval from bank's management.
2. That no actual user data will be used during this research to maintain the norm of keeping user data private in the banking sector.
3. The researcher promises to make the research and its results readily available to other researchers as well as organizations that may have interest in the field.

CHAPTER TWO

LITERATURE REVIEW

This chapter covers work previously done by other researchers in the area of multi factor authentication on POS and ATM terminals in order to enhance security. The chapter focuses on related research done and the knowledge gap that exists which t research shall be birthed from the reviewed projects.

2. Introduction

Conventional ATMs are fitted with card readers which have the sole responsibility of accepting a card and authenticating a user using the customer's name stored on the card's magnetic strip or chip. Most recently, with the introduction of contactless ATMs and POS machines, the contactless capability has been embedded which makes use of NFC technology which makes it possible for a debit/credit card to be read by the card reader without having to insert the card into it [28][16][29] .

Contactless payments raise security issues because it is possible for someone to use a contactless card to make a payment without the cardholder's knowledge. Most contactless payment systems do, however, have security measures in place to stop illegal transactions, such as requesting a PIN for transactions above a particular amount. Additionally, there is a chance of fraud: Using a contactless debit card has the same risk of fraud as using any other form of payment. To help stop illegal transactions, some banks in Zambia have fraud prevention mechanisms in place, and they often repay customers any money lost to fraud because they take on the liability for contactless payments authorised without requesting a PIN.

Card security technology has been evolving over the years and it still is as researchers are still researching on how to make card transactions even safer for the customers. Hence, the area of Information communication security that harnesses the power of biometrics to enhance the authentication and identification of bank customers is second to none.

A lot of research has been done in the field of biometrics in ATMs and in this chapter, the researcher aims to identify projects of similar traits then identify and highlight the gaps that the research aims to fill.

2.1. Literature Reviewed

1. [39] developed a biometric-based fingerprint verification system for ATM machines. Choudhary et al. [40] implemented an integrated security system using biometric authentication to enhance security in ATM machines.
2. Bhattacharyya et al. [41] reviewed the use of biometric authentication as a security measure in various applications, including ATM machines. Karovaliya et al. [42] proposed an enhanced security system for ATM machines that incorporates One-Time Password (OTP) and facial recognition features. Yadav et al. [43] proposed a secure card-less ATM transaction system using a combination of biometric authentication and OTP. Sankhwar et al. [44] developed a safeguard against ATM fraud using biometric authentication.
3. Kumar [45] proposed securing ATM with OTP and biometric authentication. Soares and Guedes [46] developed a self-banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP. Soares and Guedes [47] also proposed a fingerprint and iris biometric-controlled smart banking machine embedded with GSM technology for OTP. Mahansaria and Rathore [48] proposed secure authentication for ATM transactions using NFC technology. Masram [49] proposed an advanced biometric ATM machine with AES 256 and steganography implementation.
4. Overall, the reviewed literature suggests that biometric authentication is an effective measure for enhancing security in Card-less EATMs. The use of biometric authentication, coupled with OTP and other security features, provides a multi-layered security approach that can significantly reduce the risk of fraud and improve ATM performance. The reviewed literature highlights the importance of continuous research and development in the area of biometric authentication to address emerging security threats and challenges in the ATM industry.
5. Okereafor et al. [60] proposed a biometric anti-spoofing technique that uses randomized 3D multi-modal traits for secure authentication. Similarly, Steven and Arokiasamy [61] proposed a fingerprint-based ATM that enhances security and eliminates the need for bank cards. Okereafor et al. [62] also proposed randomized multi-biometric liveness detection as a technique for secure authentication, while Reddy [63] proposed a multi-banking transaction ATM system that uses biometric and GSM authentication.

6. Ometov et al. [64] conducted a survey on multi-factor authentication techniques and identified biometrics as one of the most secure methods. Additionally, Sivaraman [65] proposed a fingerprint-based biometric ATM authentication system, and Onyesolu and Ezugwu [66] investigated the use of fingerprint biometric identifiers in securing ATMs. Kamble and Gawande [67] proposed fingerprint verification of ATM security systems using hybrid biometric techniques, while Lasisi et al. [68] developed stripe biometric-based fingerprint authentication systems for ATMs.
7. Jaiswal et al. [69] proposed enhancing ATM security using fingerprint and GSM technology, while Mandal [70] reviewed the use of fingerprint techniques in securing money transactions in ATM systems. Finally, Taralekar et al. [73] proposed a one-touch multi-banking transaction ATM system using biometric and GSM authentication. Overall, these studies highlight the importance of biometric authentication in securing ATMs, with fingerprint-based techniques being the most explored.
8. Nawaya et al. [82] proposed a biometric authentication system based on multispectral imaging to enhance ATM security in Nigeria. They designed a finger biometric system that captures the multispectral images of the finger to verify the user's identity. The system achieved an accuracy rate of 97.5% in authenticating the users.
9. Kaur et al. [83] discussed the ethical considerations related to ATM card cloning. They highlighted that banks need to ensure the privacy and security of customers' information while implementing security measures to prevent cloning of ATM cards. The authors emphasized that ATM card cloning can be prevented by using advanced security measures such as biometric authentication and encryption.
10. Ajayi [84] highlighted the challenges and ways to overcome ATM fraud in Nigeria. The study suggested that the banks should enhance their security measures by deploying biometric authentication and video surveillance systems to deter the criminals. The author also suggested that customer awareness programs could be conducted to educate them about the risks associated with ATM usage.
11. Abiew et al. [85] proposed a cost-effective multi-factor authentication framework for ATM systems. The framework includes biometric

authentication, OTP (One-Time Password), and security questions. The authors implemented the framework using a Raspberry Pi and achieved an accuracy rate of 98.9% in authenticating the users.

12. Twum et al. [86] proposed a multi-factor authentication system to improve the security of ATMs. The system included a smart card, fingerprint, and OTP authentication. The authors claimed that the system was more secure than the traditional ATM authentication methods and could deter various types of ATM frauds.
13. Aloul et al. [87] proposed a two-factor authentication system using mobile phones. The system included a PIN and a mobile phone as authentication factors. The authors claimed that the system was more convenient and user-friendly than traditional authentication methods.
14. Oklilas et al. [88] developed a multi-factor authentication-based cardless electronic payment system. The system included face recognition, OTP, and QR code authentication methods. The authors claimed that the system was more secure than the traditional card-based payment systems.
15. Kayode et al. [89] proposed a multi-factor authentication model by integrating iris recognition into the ATM system. The system included iris recognition, smart card, and PIN authentication methods. The authors claimed that the system was more secure and efficient than the traditional ATM authentication methods.
16. Olatunji et al. [91] proposed a multi-factor authentication system for ATM security. The system included facial recognition, fingerprint, and OTP authentication methods. The authors implemented the system using Raspberry Pi and claimed that the system was more secure than traditional ATM authentication methods.
17. Melange [92] proposed a multi-factor authentication system for ATM security. The system included facial recognition, fingerprint, and OTP authentication methods. The author claimed that the system was more secure and could prevent various types of ATM frauds.
18. Ojewale et al. [93] proposed a fingerprint-based debit card system with multi-factor authentication. The system included fingerprint recognition and OTP authentication methods. The authors claimed that the system was more secure and user-friendly than traditional debit card systems.

19. Madara et al. [94] proposed a fingerprint and pin authentication system for ATMs. The system uses a fingerprint scanner to verify the user's identity and a pin to authenticate the transaction. The study showed that the system was effective in preventing unauthorized access to the ATM.
20. Poonacha and Bhat [95] reviewed the use of biometrics in ATMs and highlighted the need for a more robust authentication mechanism to improve security. They discussed the use of various biometric technologies, including fingerprint, iris, and face recognition, and concluded that a combination of these technologies would be more effective than a single biometric system.
21. Aithal [96] proposed a multifactor authentication model using fingerprint hash code, password, and one-time password (OTP) for ATMs. The study showed that the proposed model was effective in preventing unauthorized access to the ATM.
22. Karani et al. [97] proposed a multifactor authentication model using fingerprint hash code and iris recognition for ATMs. The study showed that the proposed model was effective in preventing unauthorized access to the ATM.
23. Oruh [98] proposed a three-factor authentication system for ATMs, which included a fingerprint scanner, a pin, and a smart card. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
24. Iyabode and Nureni [99] proposed a card-less electronic ATM (EATM) with biometric authentication. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
25. Onyesolu and Ocholi [100] proposed a three-tier authentication system for ATMs, which included a fingerprint scanner, a pin, and a security question. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
26. Gyamfi and Mensah [101] proposed a system to enhance the security features of ATMs in Ghana, which included a fingerprint scanner, a pin, and a smart card. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
27. Pravinthraja and Usha [102] proposed a multimodal biometric system for ATMs, which included fingerprint, iris, and face recognition. The study showed

that the proposed system was effective in preventing unauthorized access to the ATM.

28. Okokpujie et al. [103] proposed the integration of iris biometrics in ATMs for enhanced user authentication. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
29. Awodele [104] proposed a system to combat ATM fraud using biometrics. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
30. Ameh et al. [105] proposed a bimodal authentication system for securing cardless ATM transactions. The study showed that the proposed system was effective in preventing unauthorized access to the ATM.
31. [108] proposed a highly secured ATM system that uses Aadhaar card and fingerprint biometrics for user authentication. The system ensures secure authentication and reduces the risk of fraudulent transactions.
32. Babaei et al. [109] developed a face recognition application for ATM that uses facial recognition technology to authenticate users. The application uses a camera to capture an image of the user's face, which is then compared with the database to verify their identity. A systematic review by Jindal et al. [110] compared different security measures used in ATMs. The review analyzed various security measures such as biometrics, encryption, and firewalls used to secure ATM transactions.
33. Ochang and Oluwasegun [111] proposed an enhanced ATM security prototype that uses fingerprint biometric authentication to secure the ATM. The prototype uses a fingerprint scanner to authenticate the user's identity before granting access to the ATM. Coventry et al. [112] studied the usability and biometric verification at the ATM interface. The study evaluated the usability of biometric authentication techniques such as fingerprint and facial recognition at the ATM interface.
34. Alzamel et al. [113] proposed a point of sale (POS) network with embedded fingerprint biometric authentication for secure transactions. The system uses fingerprint biometrics to authenticate the user before authorizing any transaction. The study by Jaiyeoba [114] analyzed the effects of ATMs on the performance of Nigerian banks. The study evaluated the impact of ATMs on bank performance, including customer satisfaction and transaction costs.

35. Takawale and Mane [115] conducted a survey on cardless ATM transactions. The study analyzed the advantages and disadvantages of using cardless ATM transactions and discussed the challenges and opportunities for future research. Sisat et al. [116] proposed a secured ATM and cash deposit machine (CDM) that uses multiple security measures such as biometric authentication, encryption, and firewalls to ensure secure transactions.
36. Choudhury et al. [117] proposed a hybrid approach to enhance the security of ATM transactions. The system uses a combination of biometric authentication, encryption, and firewalls to ensure secure transactions. The study by Choudhury et al. [118] further explored the hybrid approach to enhance the security of ATM transactions. The study proposed a system that uses a combination of facial recognition, fingerprint biometrics, and OTP (one-time password) authentication to secure ATM transactions.
37. Choudhury et al. [118] proposed a hybrid approach that combines hardware-based and software-based security mechanisms to enhance the security of ATMs. The hardware-based mechanism involves the use of a security module to store cryptographic keys, while the software-based mechanism uses encryption algorithms to protect the data transmitted between the ATM and the bank's server.
38. In a similar study, Choudhury et al. [119] proposed a security framework that uses a combination of cryptographic techniques and biometric authentication to secure ATM transactions. The framework integrates fingerprint recognition and One-Time Password (OTP) to verify the identity of the user.
39. Ohta and Akazawa [121] emphasized the importance of promoting universal design of ATMs to ensure their usability by a diverse range of users, including the elderly and persons with disabilities. The authors suggested several design features such as audio guidance, large fonts, and braille labels to enhance the accessibility and usability of ATMs.
40. Awotunde et al. [122][123] proposed a secure ATM system that uses fingerprint authentication and short-code message verification. The system generates a unique short-code message for each transaction, which is sent to the user's registered mobile number for verification. The system also uses fingerprint authentication to verify the identity of the user.

41. Dimaunahan et al. [124] proposed a Raspberry Pi and IoT-based ATM security system that uses fingerprint recognition with Fast Fourier Transform image enhancement and multi-stage minutia extraction. The system also uses biometric verification to authenticate the user and prevent unauthorized access to the ATM.
42. Ogihara et al. [125] proposed a biometric verification system that uses keystroke dynamics to authenticate the user. The system captures the timing and duration of each keystroke and compares it with the user's baseline profile to verify the identity of the user.

2.2. Related Works

2.3.1 Face Recognition and Fingerprint-Based New Generation ATM

In this research, the authors created another method of account access using face recognition and fingerprints for the system. In this method, the authentication process uses both facial and fingerprints. Before fingerprint recognition, the face image of the subject is matched to a database image. Access to that account is granted when both recognition schemes match the same individual. In this instance, the controlling portion uses a Raspberry Pi microcontroller. The face ID and fingerprint ID are checked in a database that also contains the user account's other information. The database search is carried out by the raspberry pi microcontroller, which also sends the required data to a display device.

The process of recognizing, verifying, and identifying facial photographs uses open CV libraries. The procedure for fingerprinting uses fingerprint libraries. Python is used to code the process program. [34].

2.3.2. Card-Less Electronic Automated Teller Machine (EATM) With Biometric Authentication

In this research, the authors appreciate the advantages of card less ATM transactions and proposed that mainly uses the already existing components of the ATM except for the card reader which is replaced with a fingerprint scanner. The proposed system makes use of biometric finger data and the alphanumeric PIN as well as a 4-digit PIN to authenticate a user. The system covers two types of activities, these being, A transactions such as cash withdraws and fund transfers, B includes balance inquiry and fund transfers whose accounts are not linked to the account on the ATM. With the exception of the fingerprint scanner,

which replaces the card reader. The authors proposed a system that uses a four digit PIN in addition to an alphanumeric PIN and biometric finger data to authenticate users. The system supports two different kinds of activities: A transactions, such cash withdrawals and fund transfers, and B transactions, including balance inquiries and fund transfers for accounts that aren't linked to the ATM's account. [35]

2.3.3. AES Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using FPGA Implementation.

The authors of this research provided a design for an AES system comprising a fingerprint reader, fingerprint display, and AES algorithm. The fingerprint scanner is used to capture the user's fingerprint data, which is later encrypted using the AES technique. The multi-touch display screen shows the user input possibilities. The system under consideration uses FPGA, which provides high performance and high throughput for feedback. The authors of the research appreciate the need for more secure card-less ATM transactions because all known attacks may be defended against with AES [36].

2.3.4. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System

The researcher designed a system that uses a client/server architecture of which there is a connection between the customer information, identification and account information. The researcher then highlights the fact that the system is a three-factor authentication system that uses the User ID, PIN and biometric feature.

The main goal of this research was to create a three-factor authentication system that uses the ATM ID number, the PIN number, and the biometric feature (both the cardholder's and nominee's fingerprint). Customers are supposed to have an ATM card, be familiar with and remember their PIN, and register their fingerprint with the system's fingerprint reader adaptor. The customer's live sample is then compared to a template in the database by the fingerprint database. Access to the ATM system is then granted to the user after verification that the information provided is accurate [37].

2.3.5. Finger Eye: improvising security and optimizing ATM transaction time based on iris-scan authentication.

The system leverages on Iris scanning technology to enhance the processing time as well as for stable and accurate results during authentication. The Researcher designed and implemented the system on an already existing windows computer to cut down on additional hardware costs.

The registration phase includes capturing the customer's personal information such as their full names, date of birth and their respective Iris biometric data using a digital camera. This biometric data is stored in binary form in the database for cross referencing during the verification process.

The researchers found that this approach worked excellently, especially when a consumer requests a sizable cash withdrawal. The ATM only prints out the initial amount the user requested then logs out, which is a drawback. What happens if the customer changes their mind and wants to withdraw less money or more money? One must either make a new request to withdraw the old one, or one must withdraw the old request and make a new one. For the customer, this could be difficult. Considering this, the authors suggest the second approach, in which the client just notifies his bank of his need to conduct a transaction; he is then validated as soon as he arrives at the ATM and given full control of the ATM [38].

2.4. Summary

This chapter has reviewed the various proposed systems that incorporate biometric verification coupled with other methods of authentication .An extensive literature review was conducted and it was note that no research has yet been conducted that leverages all 10 fingerprint samples where any one sample is requested at random at each authentication request, coupled with OTPs for transaction authentication and PIN for user authorization to form a multifactor authentication system .The proposed system bridges the knowledge gap and further adds to the body of knowledge.

CHAPTER THREE

RESEARCH METHODOLOGY

3. Introduction

This section gives a description of the research process and an explanation of the methods used to gather data and some of the variables that will have an impact on results. Among the section heading in this chapter are the research design, the research area, research tools and the justification for this research then the chapter shall be summed up in the Conclusion.

A detailed literature review on the Design of ATM MFA systems using Biometrics and OTP has been done and is ongoing. In each review, the contribution made, research not done, and limitations have been documented. Some of the missing achievements are being investigated in this research as well.

A simulated approach to this research was adopted to demonstrate the design of the project. The simulation tool was adopted for this project.is Proteus Isis which includes all components required to fully capture the desired results.

3.3. Simulation and Development Tools

The tools and technologies used are as below;

- Proteus Isis Professional 8
- Arduino IDE version 1.8.18
- C Programming language

3.4. Research Design

The processes to be undertaken during the design will be as follows.

3.3.1. Fingerprint capture Phase

This phase will constitute capturing the customer fingerprint data in two stages.

3.3.1.1. User Registration stage

At this stage, user data is captured including fingerprint data in line with KYC (Know Your Customers) norms. The data is captured using a

fingerprint sensor at the accounts opening station in a bank branch and is stored in a database accessible by the ATM Transaction switch.

3.3.1.2. ATM/POS transaction stage

At this stage, user authentication is done, scanned fingerprints are captured and converted to a machine-readable form which is later conveyed to the ATM Transaction switch where the fingerprint data is compared with stored fingerprint data for purposes of determining the authenticity of the customer transacting.

3.3.1.3. Algorithm

The ATM application software randomises the 10 capture fingerprint samples to curb the risk of predictability. Upon transacting, the user is prompted to place a random finger on the sensor, and it captures and converts the data to machine-readable format and encrypts the data which is then authenticated against a database of all the fingerprint samples of the bank's entire customer base.

Upon authentication, the system either rejects the ATM transaction requests if the fingerprint data does not match any sample in the database or allows for a transaction if there is a match. Communication is then made to the CBS for further information and instructions.

3.4. Proposed System

The proposed system provides an enhanced system of verifying the bank's customers using fingerprint data ,PIN and One Time passwords (OTPs) as opposed to the current conventional use of ATM debit/credit card and an alphanumeric PIN only. The ATM randomly asks for any one of the 10 fingerprint samples and not just one thumb as is the case in most proposed designs. A biometric fingerprint scanner is to be incorporated into the ATM in a similar way in which the card reader works.

The concept of randomized fingerprint authentication is a security feature that involves the use of multiple, randomly generated fingerprints to verify a user's identity. This can be an effective way to enhance security because it makes it much more difficult for an attacker to forge a user's fingerprint.

Here are some specific advantages of using randomized fingerprint authentication:

1. Increased security: Because the fingerprints used for authentication by the are requested for at random by the transaction switch, it is much more difficult for an attacker to forge a fingerprint that will be accepted by the system. This makes it much harder for an attacker to gain unauthorized access.
2. Greater convenience: Randomized fingerprint authentication can be more convenient for users because they do not need to remember a separate login credential (such as a PIN or password). They simply need to place their finger on the scanner to log in.
3. Improved accuracy: Randomized fingerprint authentication can be more accurate than other forms of authentication, such as a PIN or password, because a fingerprint is a unique physical characteristic that is exceedingly difficult to replicate.

Overall, randomized fingerprint authentication is a secure and convenient way to verify a user's identity and protect against unauthorized access.

The ATM through the fingerprint scanner scans the random fingerprint and passes the data to the Transaction switch, then the transaction switch verifies whether the fingerprint data is maintained and mapped to a particular customer in the system. The fingerprint data is verified as either one in the database or not. If it does exist, a message is sent to the core banking system to fetch the customer account details such as account number, balance etc.

This information is relayed back to the Transaction switch, the Transaction switch sends an OTP to the customer’s mobile phone to authorize the withdrawal after a withdrawal has been initiated by the customer. Upon completing the transaction, the customer enters the OTP which is temporarily stored on the Transaction switch to authenticate and authorize the cash-out.

This system aims at ensuring that the authorized and intended user of the account is the one transacting at each instance, consequently curbing fraud on customer accounts.

The flow diagram below shows how the message flow in the proposed system**.**

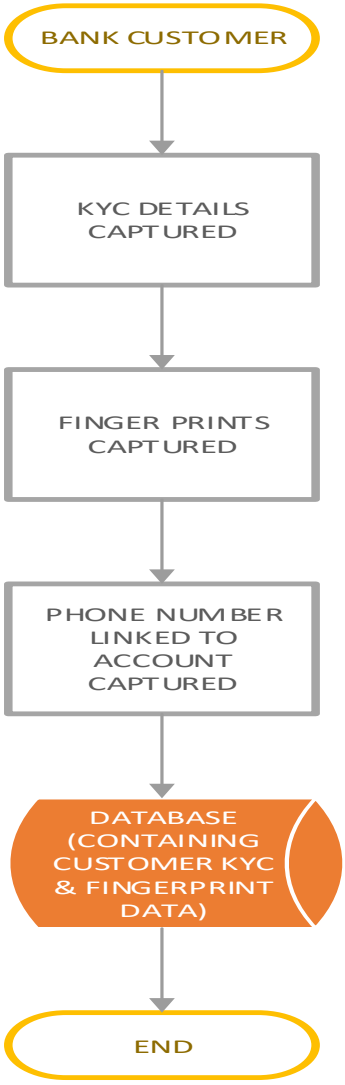

Figure 4 – User Registration phase

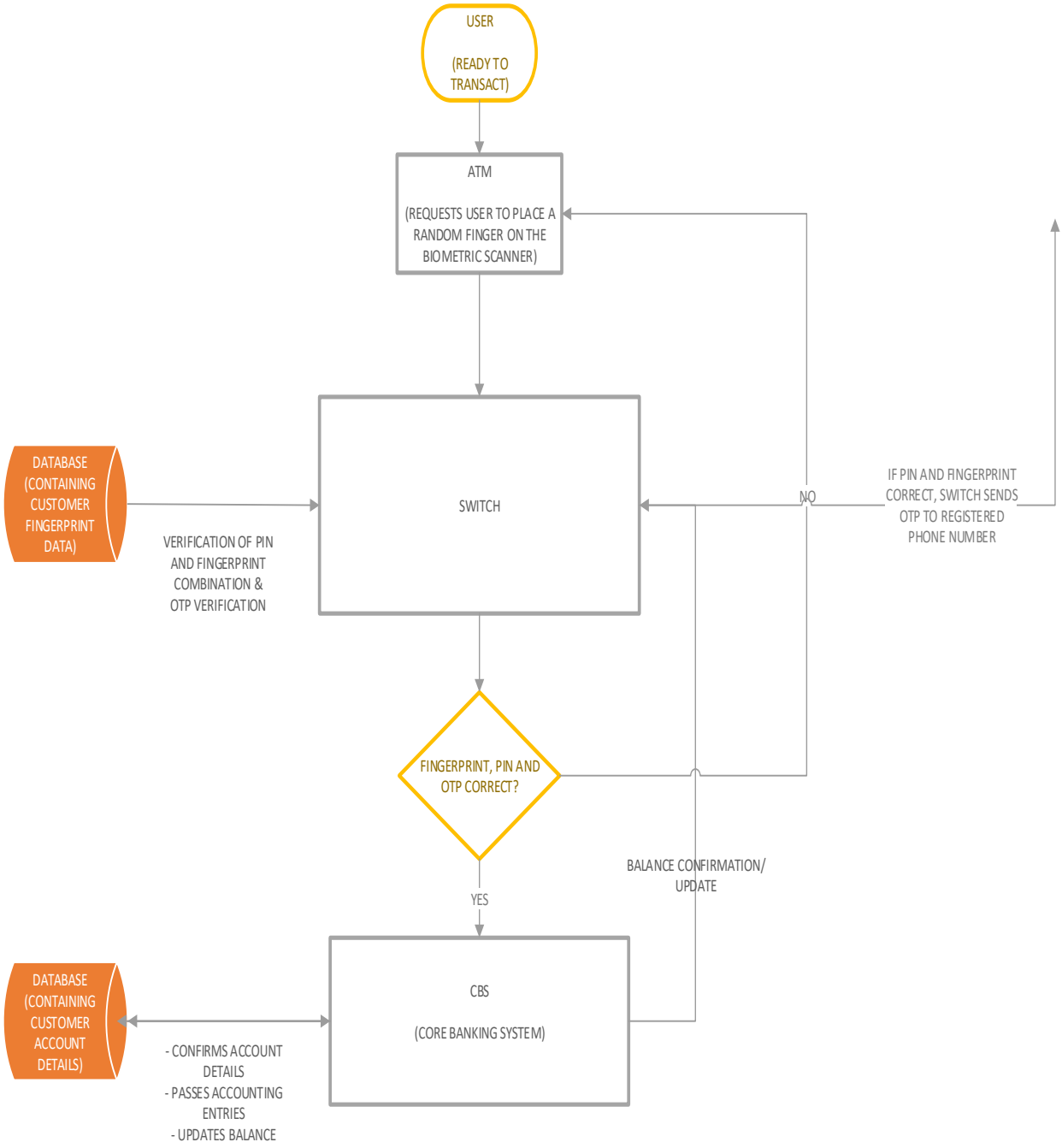

Figure 5. Proposed System Flow chart

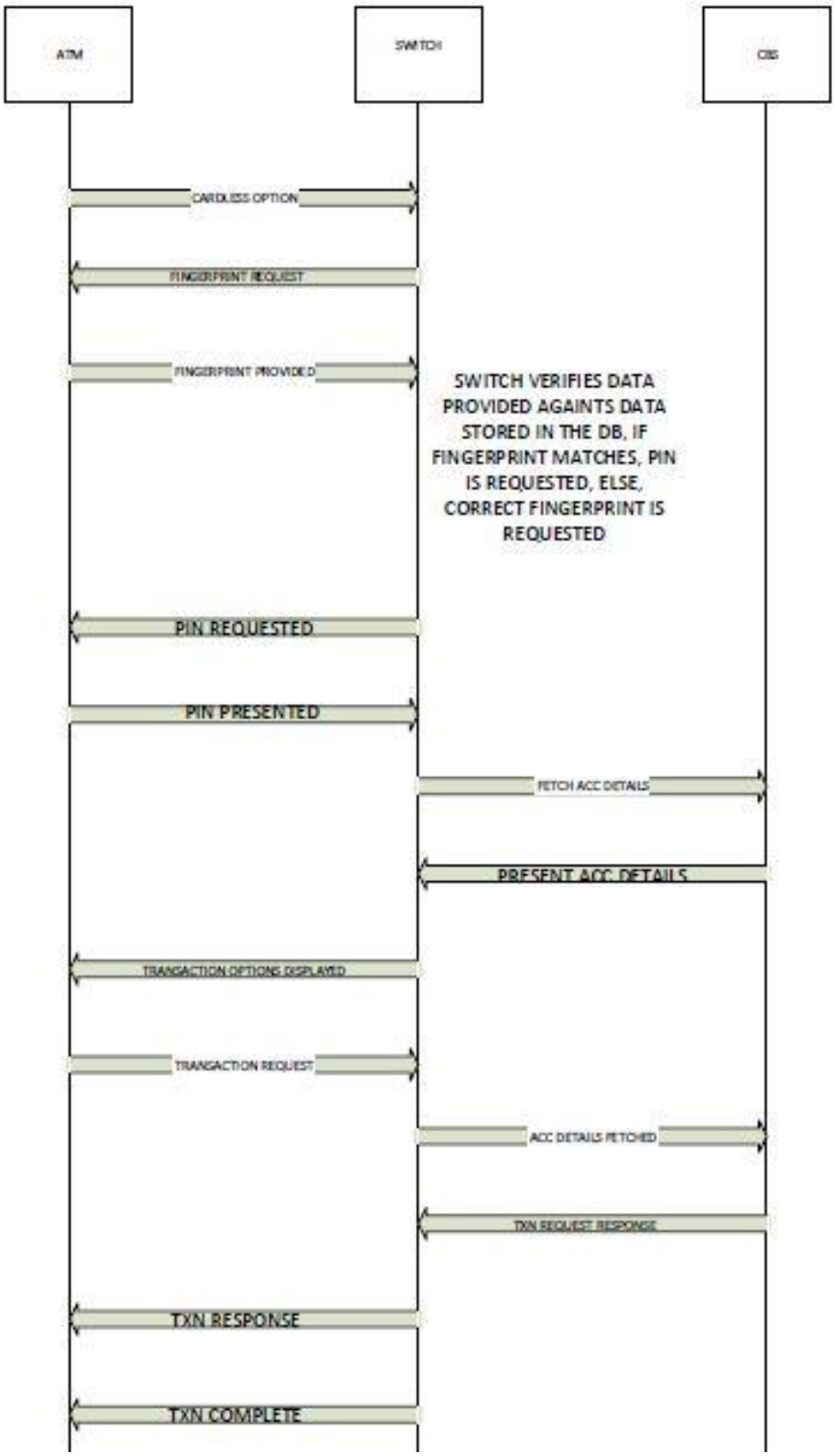

Figure 6 Sequence Diagram

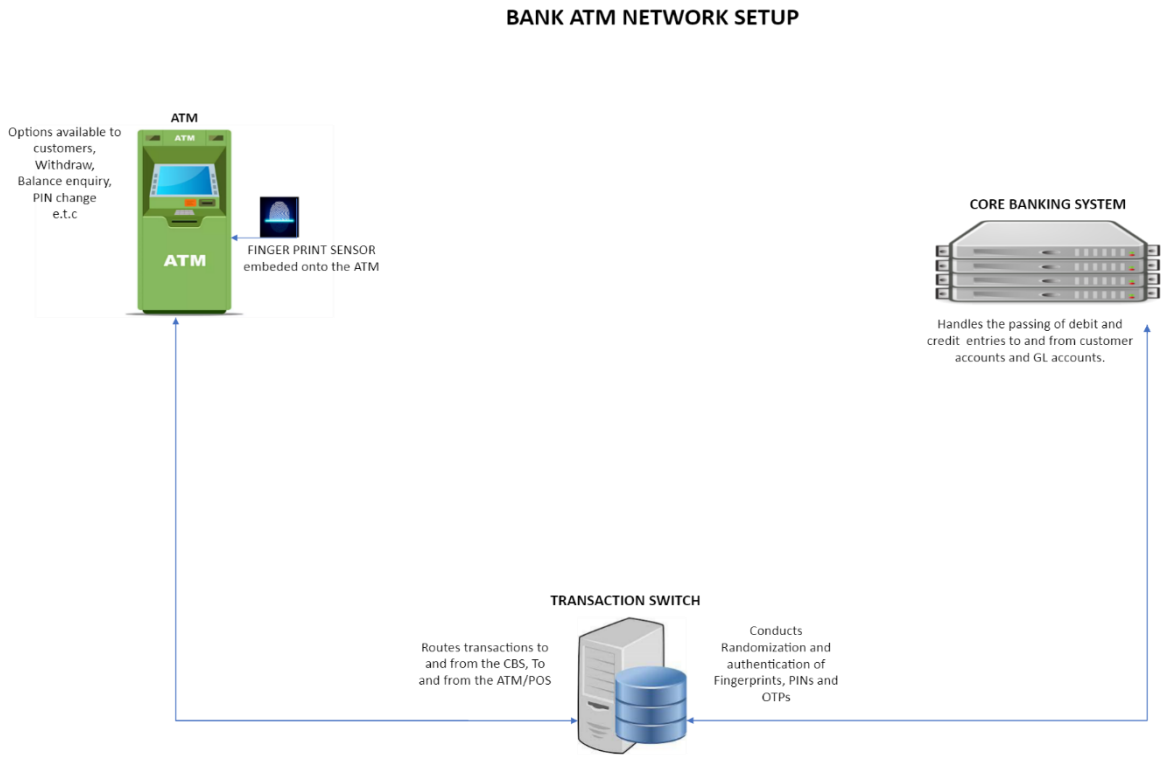

Figure 7 Bank ATM Pictorial setup overview

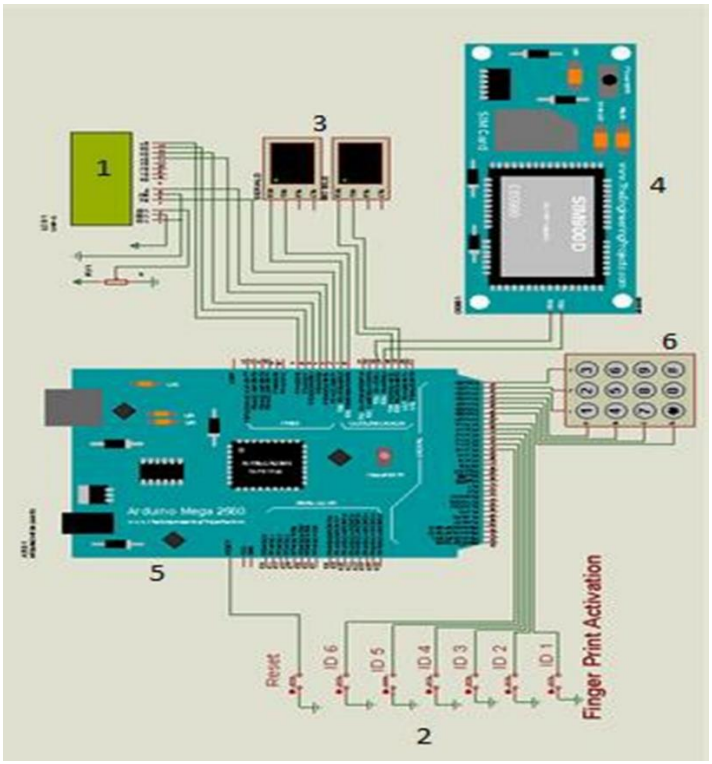

Figure 8 Proteus Isis Design of MFA

1. LCD screen for the purpose of displaying results, this simulates the screen on an ATM.
2. Buttons labelled ID 1 to 6 and including RESET. These buttons simulate a fingerprint sensor embedded on the ATM for fingerprint scanning, this is so because Proteus Isis does not have a fingerprint scanner to achieve the goal of the project.
3. Two sensors: Mobile for the GSM module to simulate a customer's mobile device and how an OTP is sent to them and Serial for the 7 buttons to be accurately captured when pressed.
4. GSM module: this simulates a customer's mobile device to receive the OTP sent by the MFA system for transaction authorization by the customer.
5. Arduino: This houses the logic of the Fingerprint randomization mechanism and simulates the ATM.
6. Keypad: To capture user input

3.5. Simulation and Analysis

The system's reliability will be evaluated in respect to typical card ATM/POS transactions, and conclusions will be made based on the findings. The researcher must make sure to employ fingerprint recognition and randomization at the user verification stage at the ATM . Data analysis will be more qualitative because conclusions can be made, and interpretations made based on the simulation's data.

CHAPTER FOUR

4. RESULTS AND ANALYSIS OF FINDINGS

This chapter presents results from the simulated design of the multifactor authentication system for automated teller machines. The results of this simulation were obtained from Proteus Isis Pr0fessional. The simulation being a proof of concept was mainly focused of the three-tier authentication backbone of the design which are fingerprint, PIN and OTP.

Below are image results of the design simulation and various use cases and tests conducted.

4.3. Assumptions

For simulation of the user authentication as well as transaction authorization to be made successfully, a few assumptions were made such as;

1. The HSM is a Hardware security module, whose sole responsibility is to ensure that encryption keys are exchanged between the Switch and hosts such as POS terminals and ATMs. HSM s comes in all sorts of brands but consequently they basically play the same role. HSMs are highly sophisticated hardware and software suites. Including them in this research would render the research highly complex and expensive. There is no need to re-invent the wheel as there are multiple bespoke solutions in production today.

2. Transaction Switch, this is different from a networking switch. The Switch referred to in the research is a highly complex software suite that handles acquired and issued transactions by a financial institution with other institutions. It is through these switches that banks issue and acquire VISA, Union Pay, American Express, MNO, Mastercard transactions. Further, these suites are responsible for PIN issuance, wallet creations and many other. In this research we only simulate certain aspects of the switch, in this case, PIN issuance and biometric authentication which are both simulated in the Proteus design and housed in the Arduino device.

3. The CBS or core banking system is a highly sophisticated system (software) that in this simulation is assumed to be at play. Certain aspects of it are simulated through the code housed in the Arduino.

4. Assumes that users' fingerprint samples are captured at user registration stage together withal other KYC details and stored on a database.

5. Designing /redesigning of a relational database for the Transaction Switch is outside the scope of this research, hence the database is assumed to be in play.

6. It is also assumed that the system uses the already existing infrastructure in the ATM data flow. These include integrations with bulk SMS providers for OTP, HSM, Switch and CBS which are assumed to be at play and there is therefore no need to re-invent the wheel.

7. The simulation focuses on demonstrating the algorithm for the randomization feature at user authentication stage, transaction authentication via OTP and PIN authentication at user authentication stage. Variables and input used would be replaced with appropriate variables in a real-world scenario.

4.4. Random Fingerprint Request and PIN Authentication

Among the three core features of the design is the concept of randomised fingerprint request. Among the 10 fingerprint samples provided by the customer to the bank, the ATM requests the user to place any one of the 10 fingerprints by using a randomization function to pick with finger. The fingerprint once recognised and the correctly requested one, then the user is requested to enter their static 4 digit PIN.

Below is the schematic view of the design which includes and Arduino Mega 2560, a GSM module to simulate a mobile phone to receive OTPs, a keypad, 6 buttons that constitute the fingerprint sensor i.e. ID1, ID2, ID3, ID4, ID5, ID6 and a reset button that resets that random fingerprint sequence and an LCD screen to display all outputs.

The figure below shows a prompt for the user to enter their fourth (4^{th}) finger onto the fingerprint reader for the purposes of authentication, if the user places any other fingerprint other than the one requested for, the ATM does not request for the 4-digit PIN but with prompt the user to instead provide another randomly requested fingerprint.

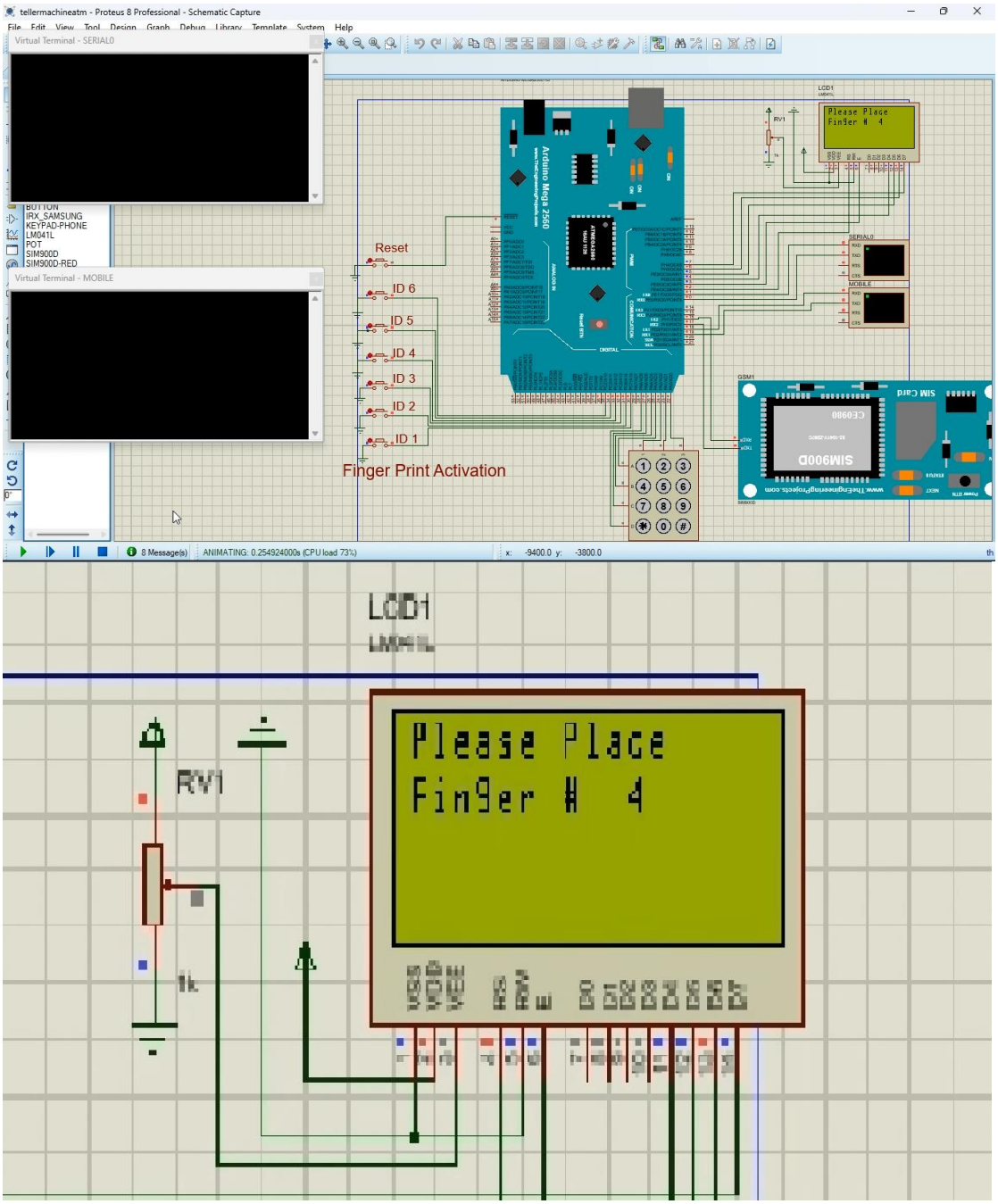

Figure 9 User prompted to place the fourth finger print on fingerprint scanner

Once the user provides the correct fingerprint, the ATM recognizes the user and requests for their 4-digit PIN as can be seen in Figure 14.

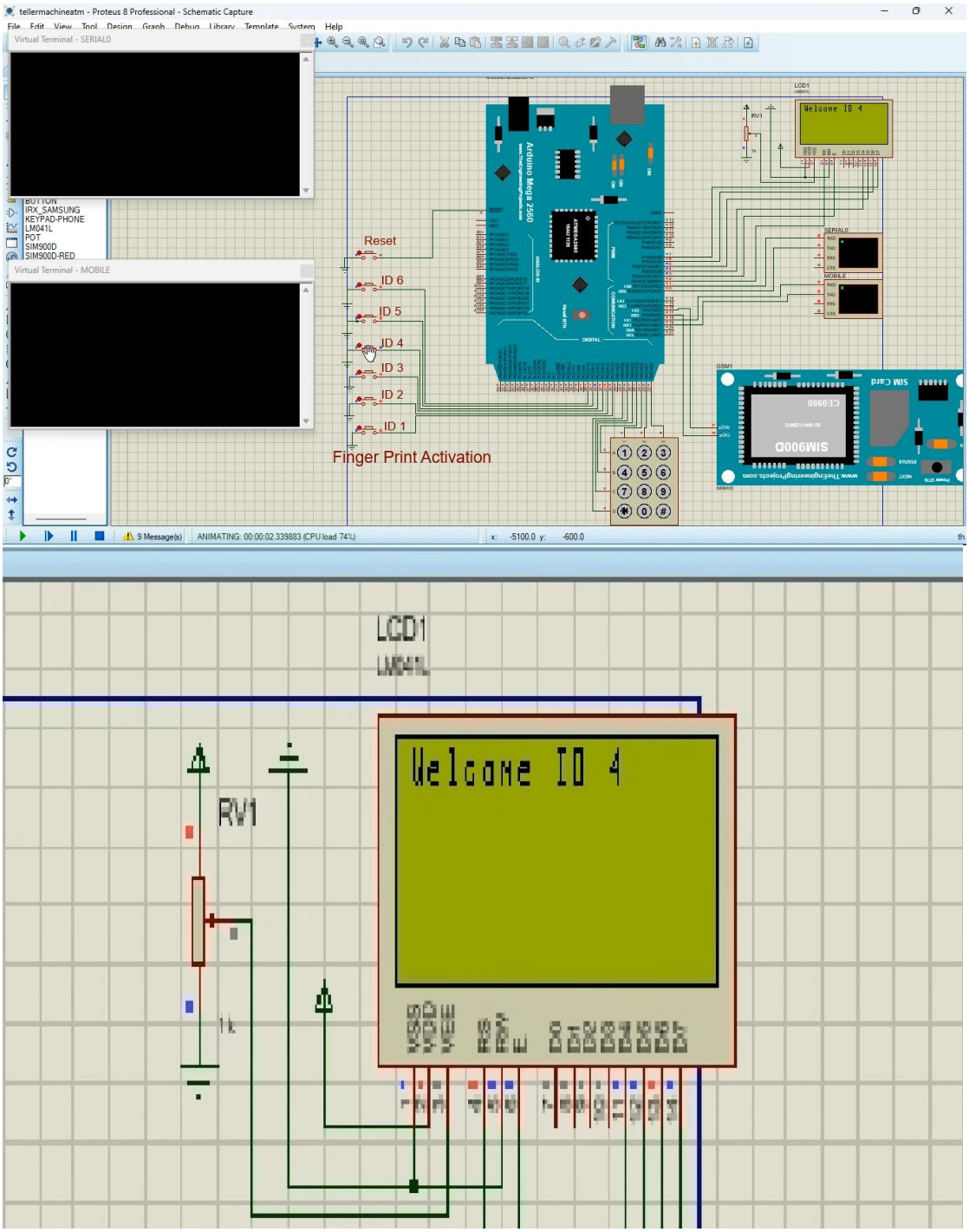

Figure 10 customer authenticated with fourth fingerprint

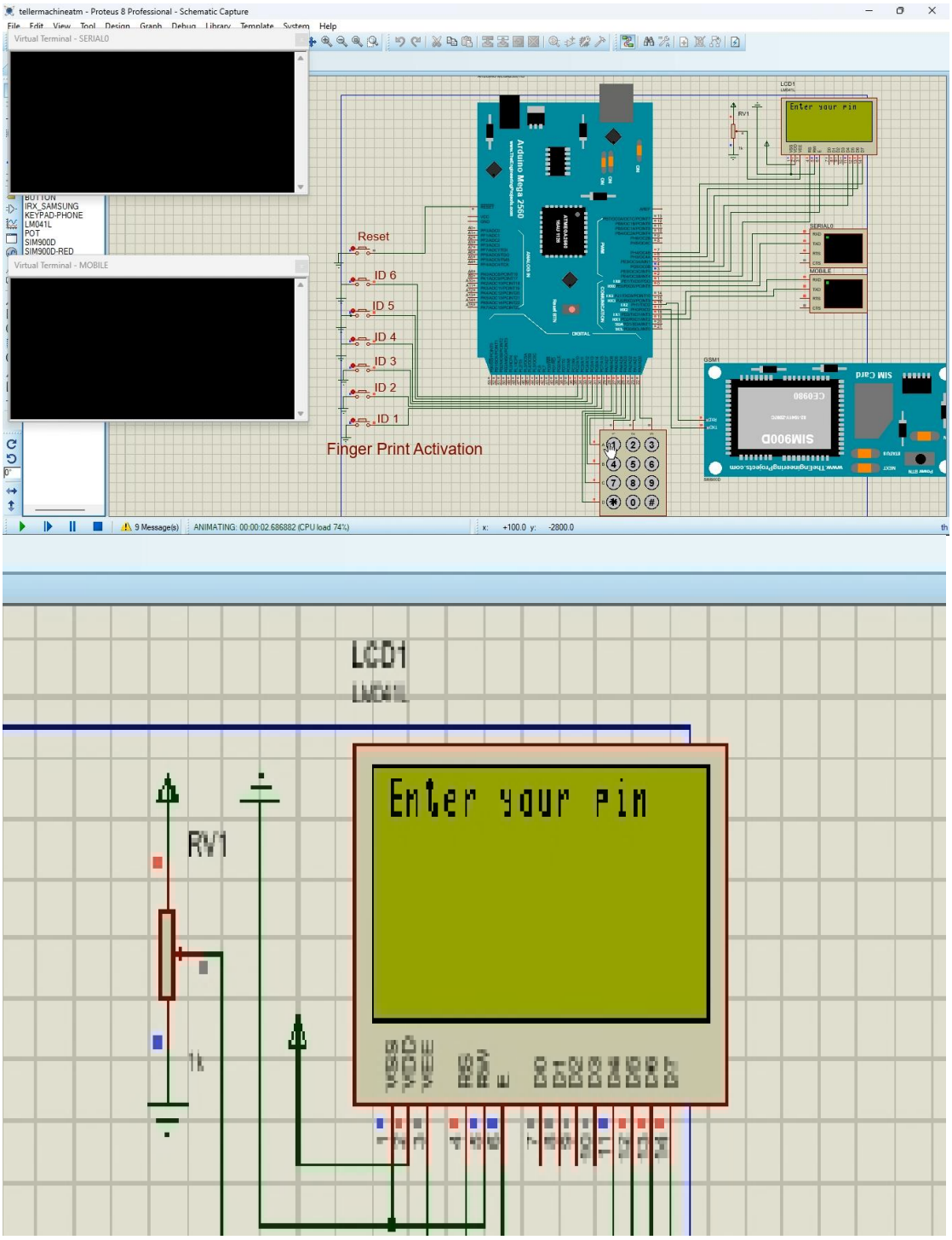

Figure 11 ATM screen prompting user for 4 digit PIN

Figure 14 shows the ATM screen prompting the user to provide the user's 4-digit PIN, anything other than the user's correct PIN will flag an error and will not fully authenticate.

Once successfully authenticated with the correct requested for fingerprint and the user's correct 4-digit PIN, the user is provided with all the ATM options.

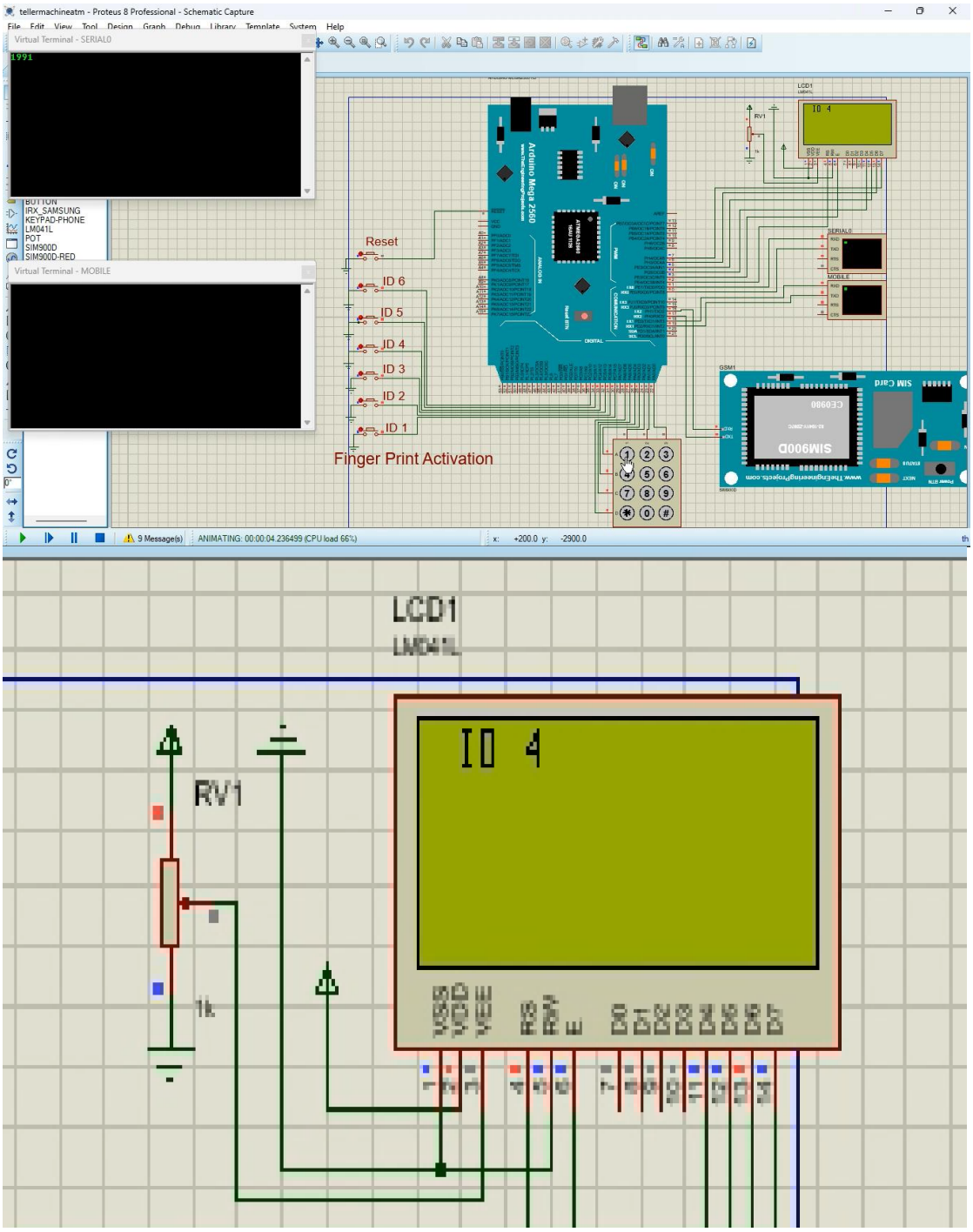

Figure 12 User successfully authenticated with forth fingerprint and PIN

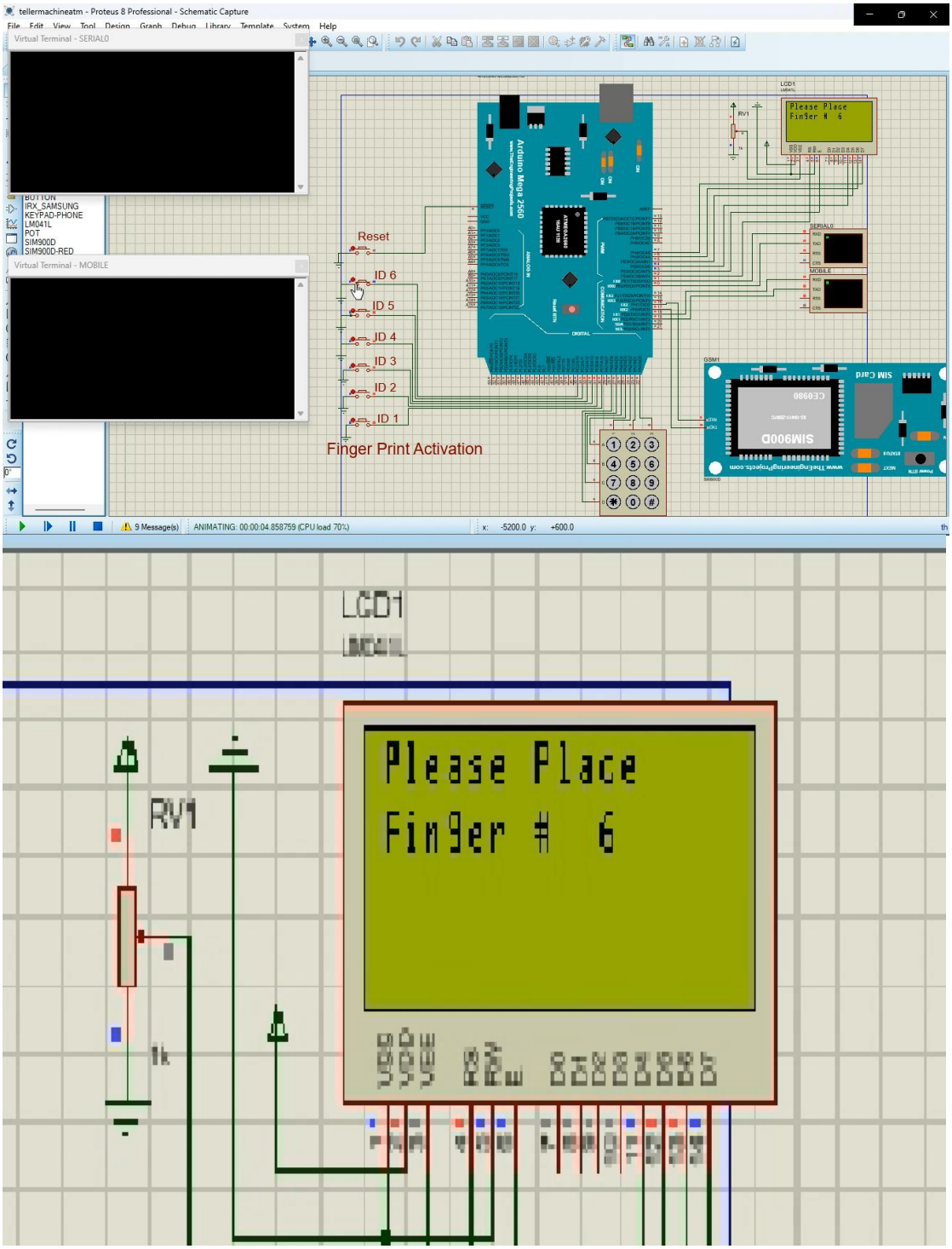

Figure 13 User prompted to place the sixth fingerprint on fingerprint scanner

The user is prompted with a random fingerprint request (6) as seen above in Figure 16.

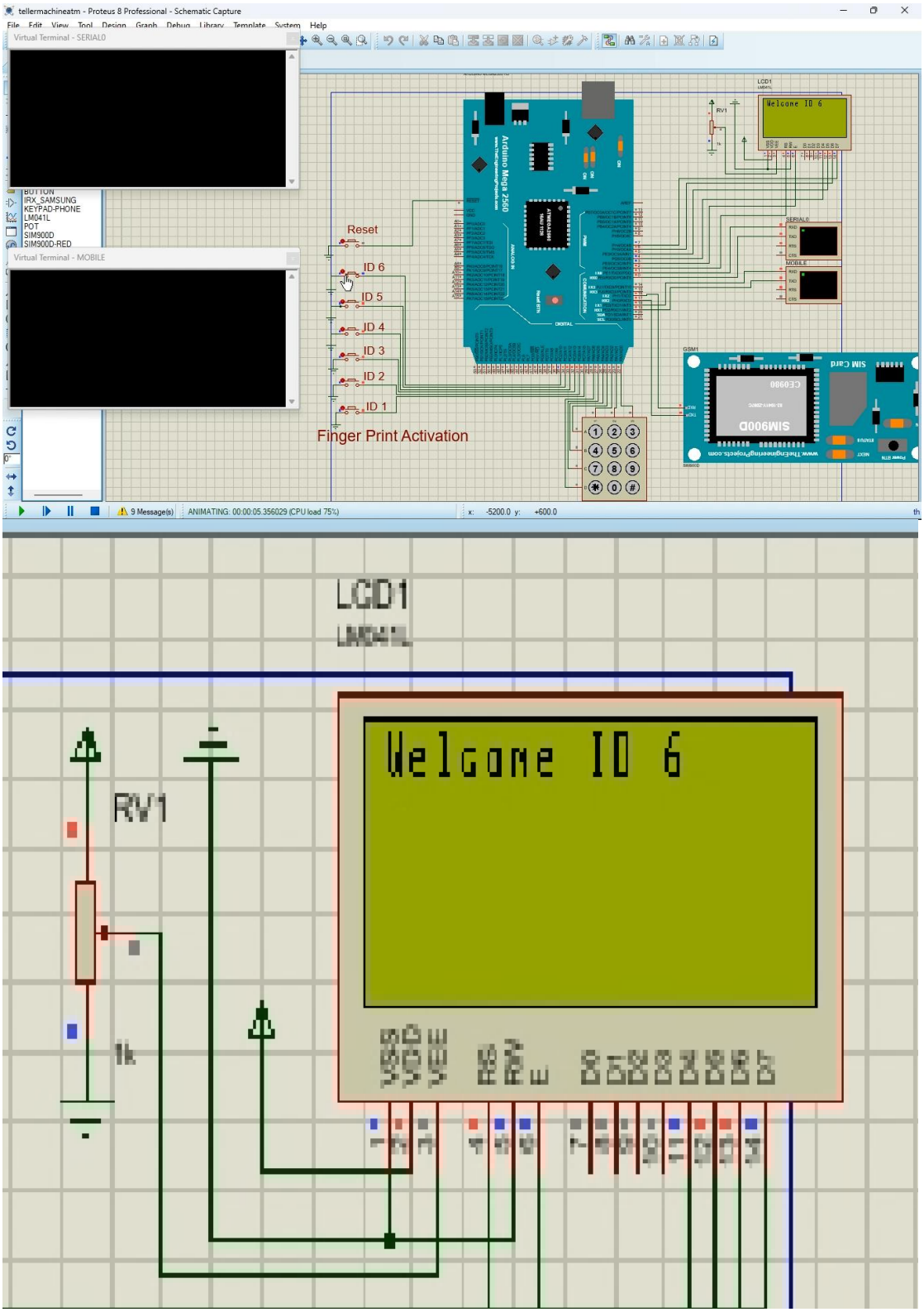

Figure 14 customer authenticated with sixth fingerprint.

Once successfully authenticated, the user is directed to the welcome screen as can be seen above in Figure 17.

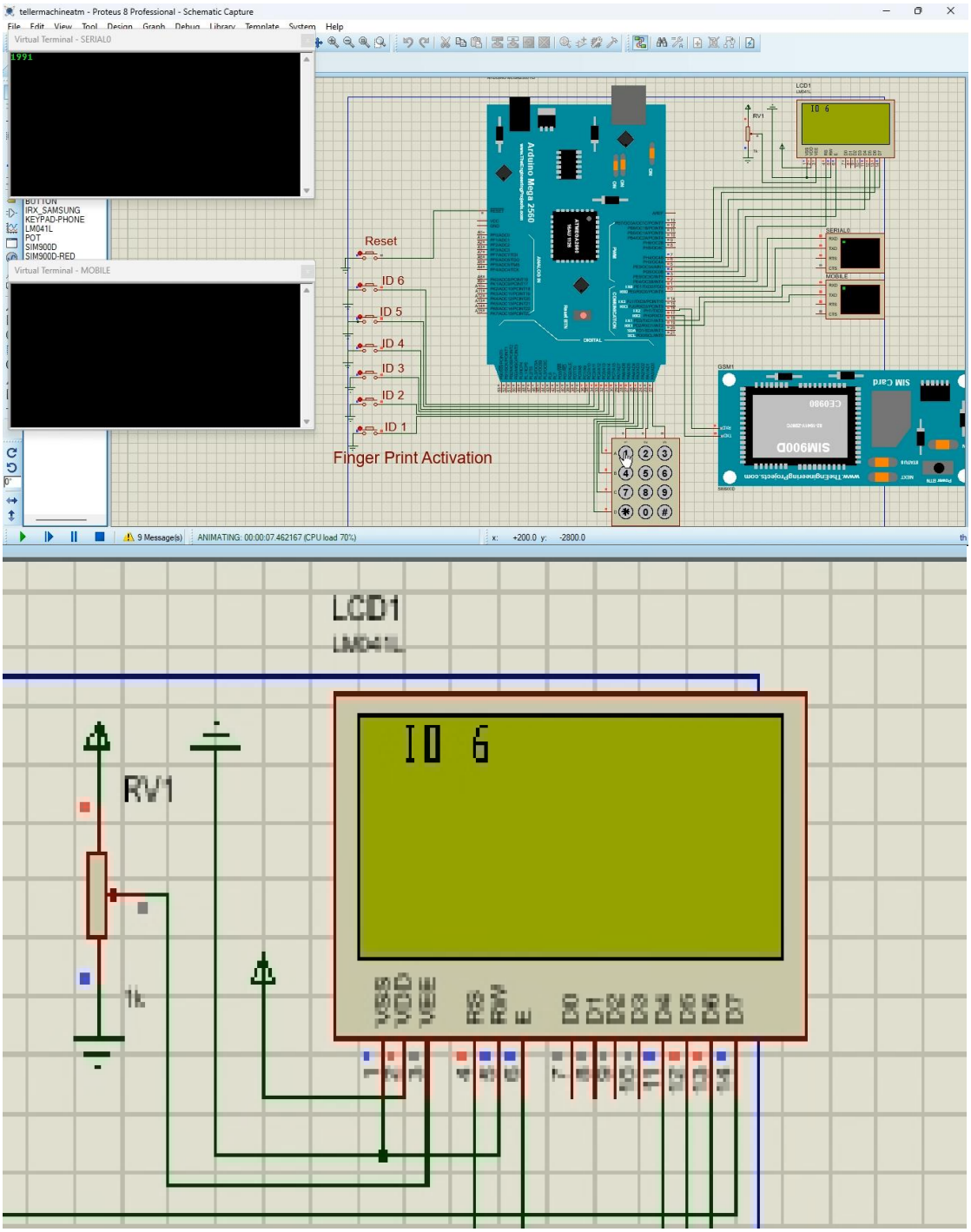

Figure 15 User successfully authenticated with sixth fingerprint and PIN

The user is prompted with the above screen once authenticated with the correct fingerprint and correct PIN.

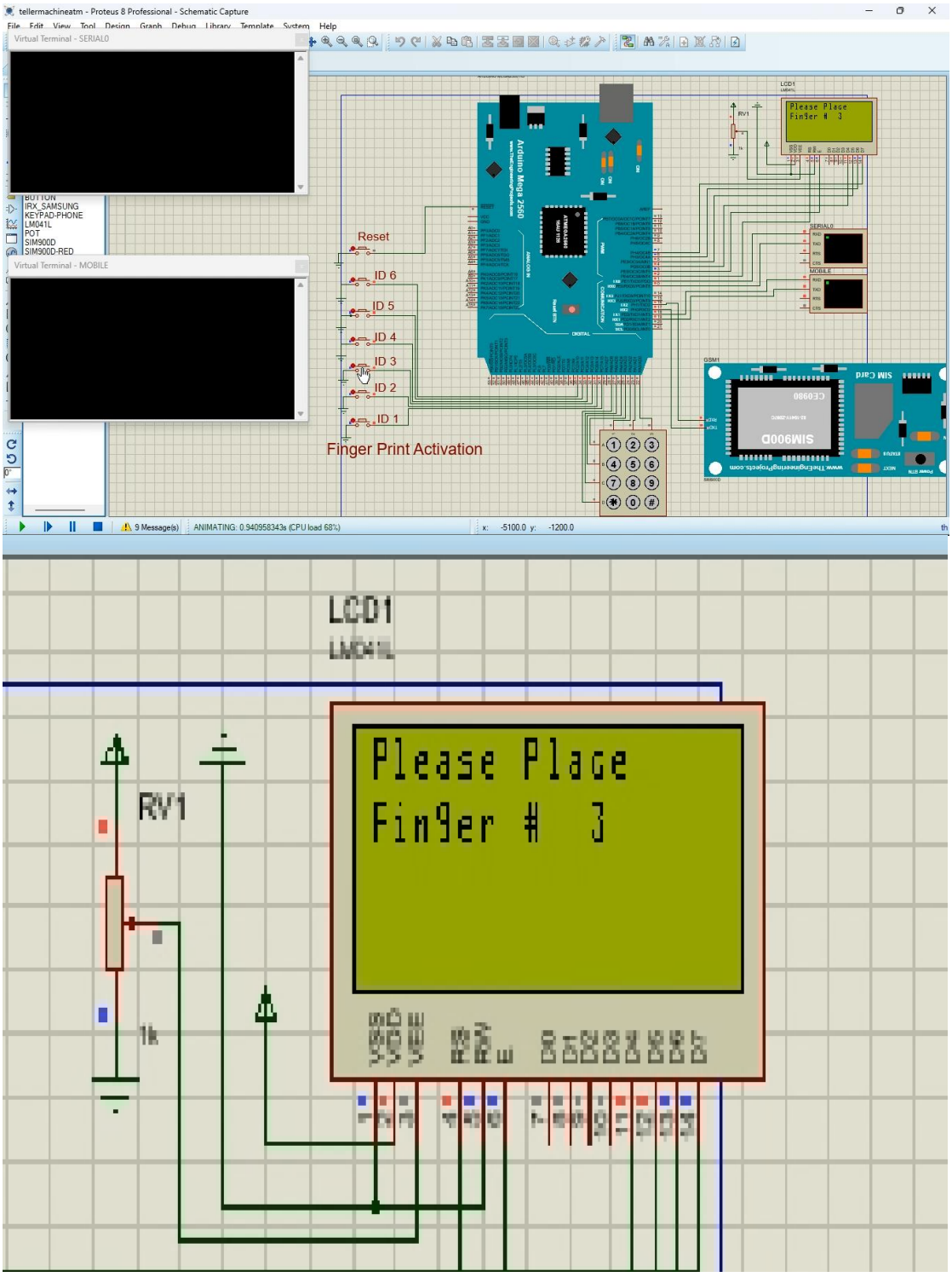

Figure 16 User prompted to place the third fingerprint on fingerprint scanner

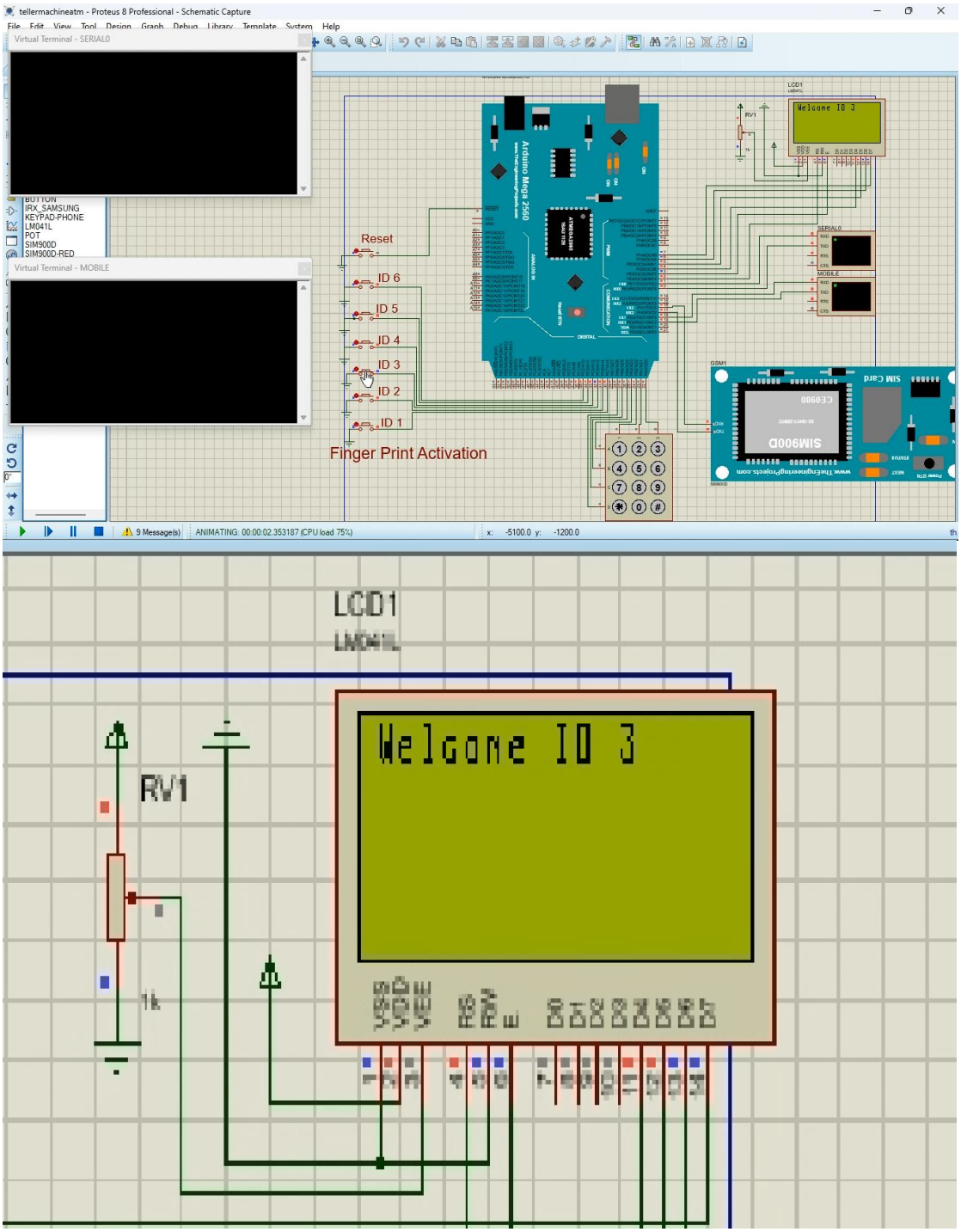

Figure 17 customer authenticated with third fingerprint

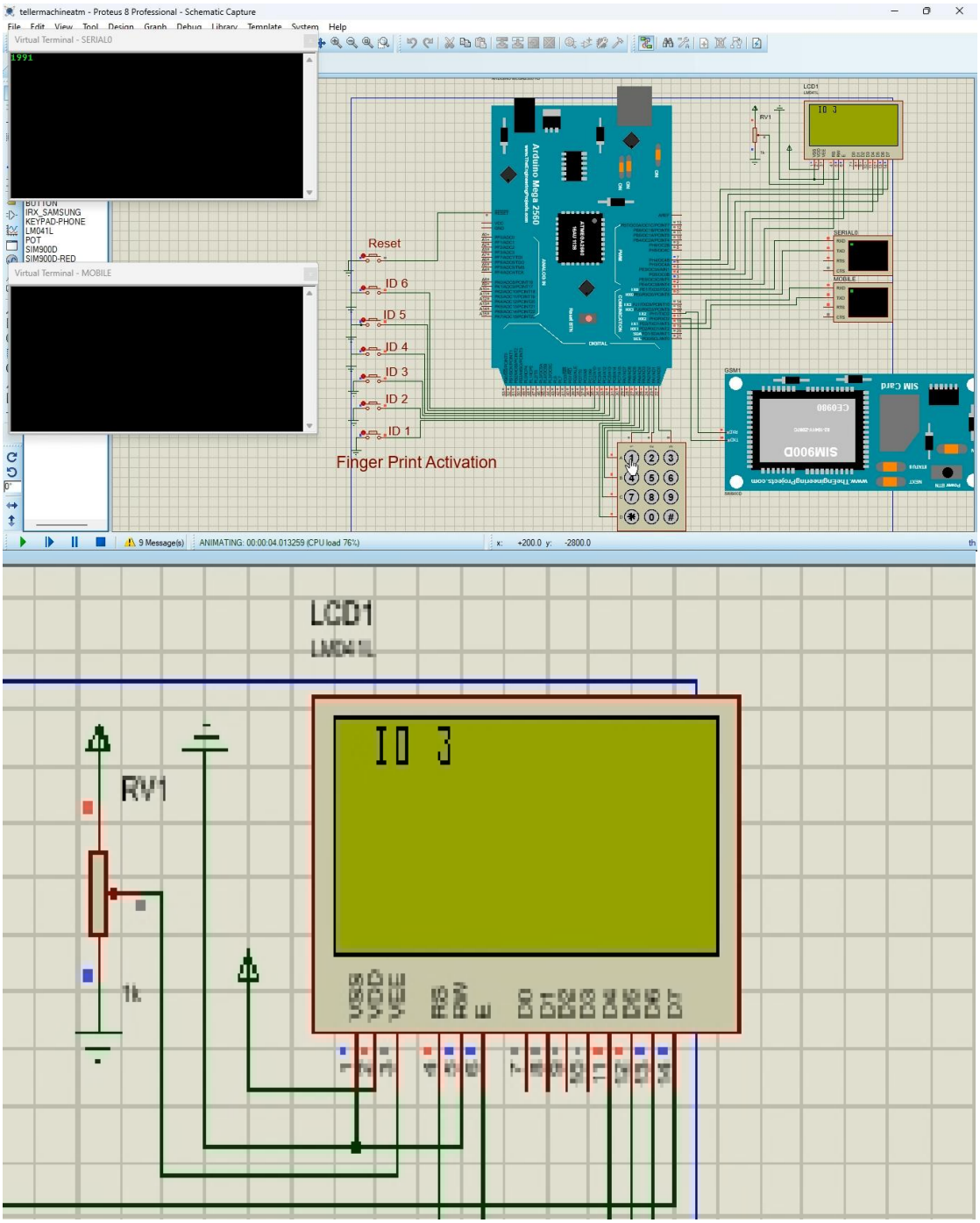

Figure 18 User successfully authenticated with third fingerprint and PIN

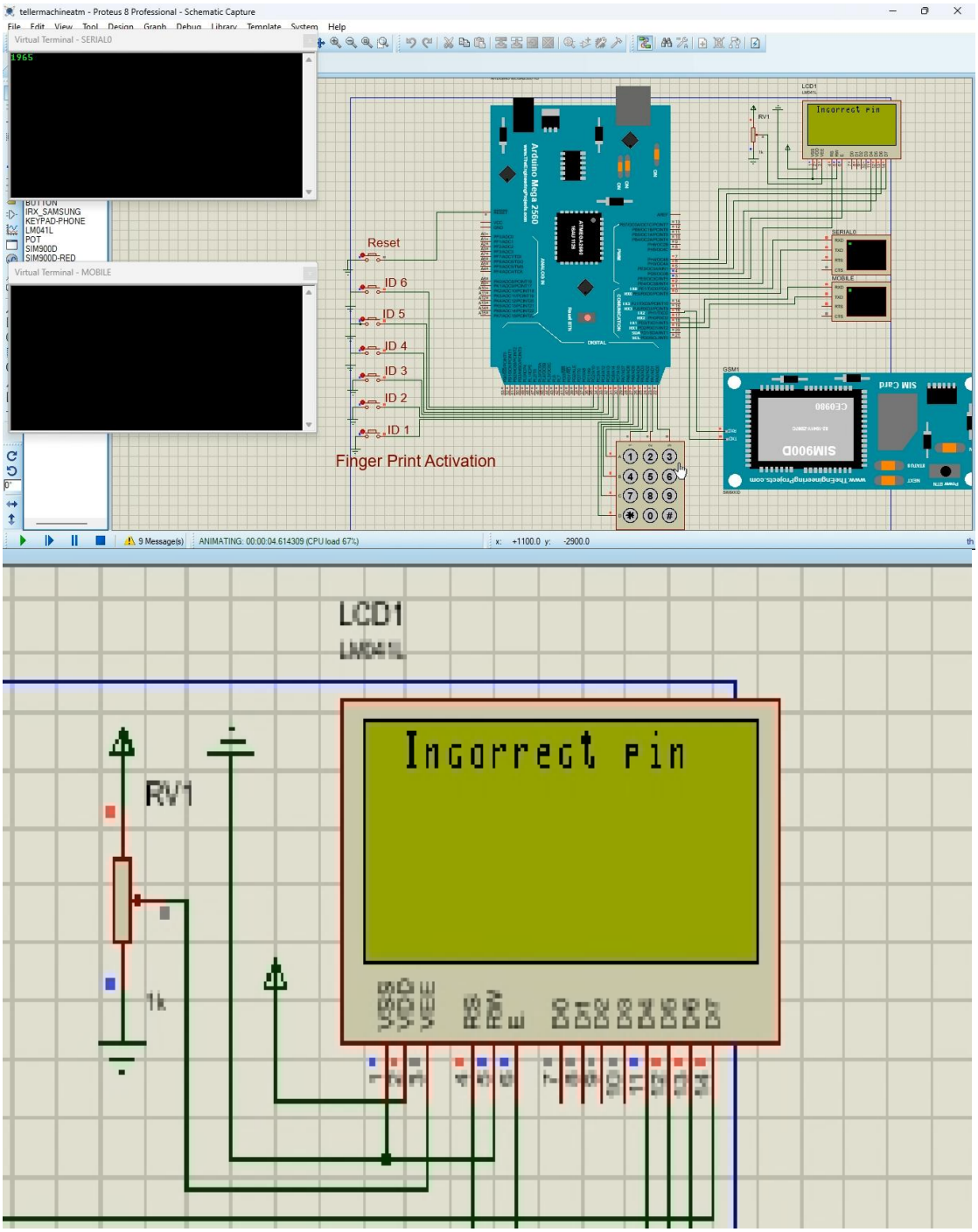

Figure 19 Failed authentication – wrong PIN

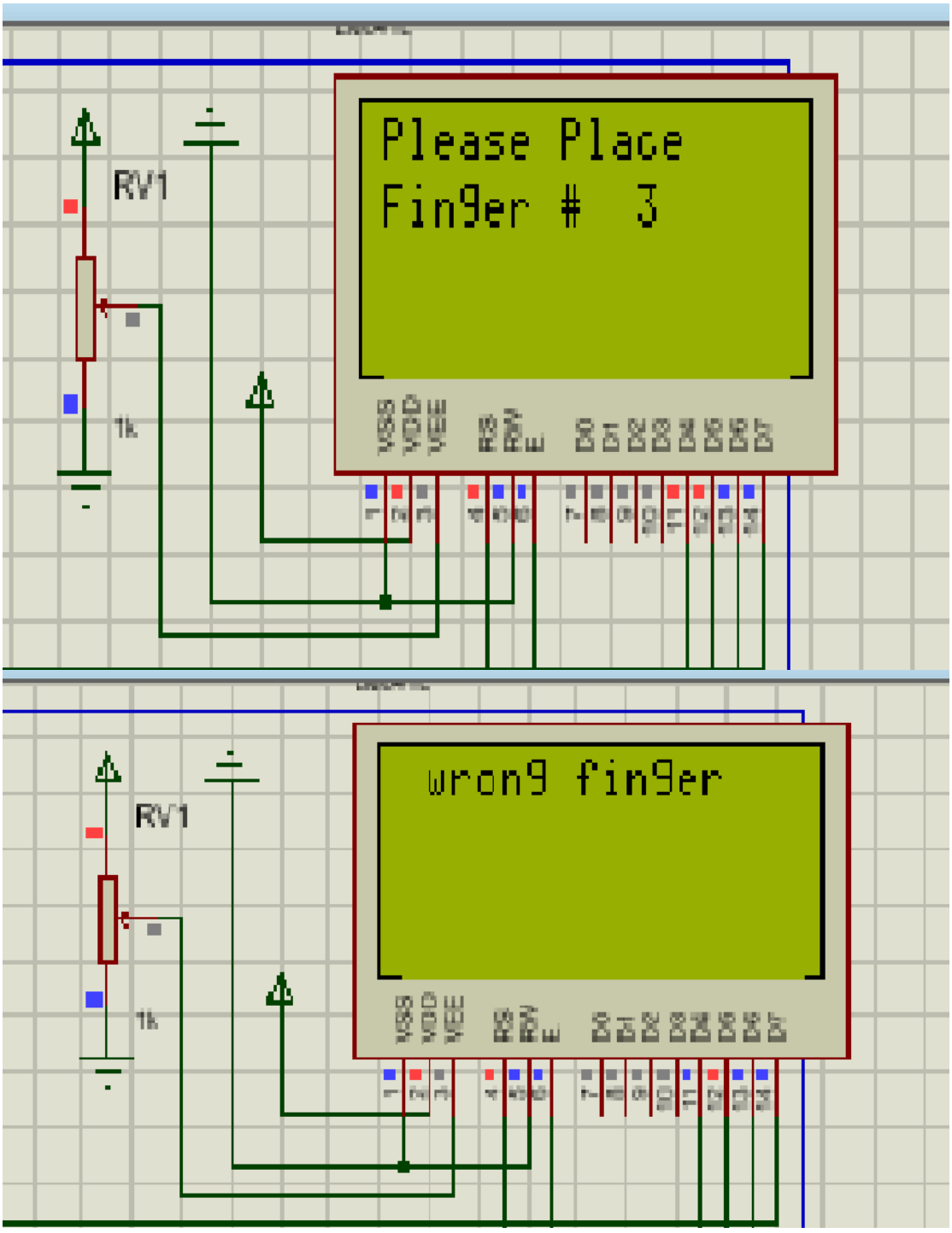

Figure 20 Incorrect Finger error

When the user supplies the wrong finger requested by the ATM, despite the customer being the legitimate owner of the account, will not be authenticated as it does not conform to the random fingerprint request. In case above in Figure 22, the terminal requested the user for finger number 3 but the user placed their finger number 3 and hence, was not authenticated.

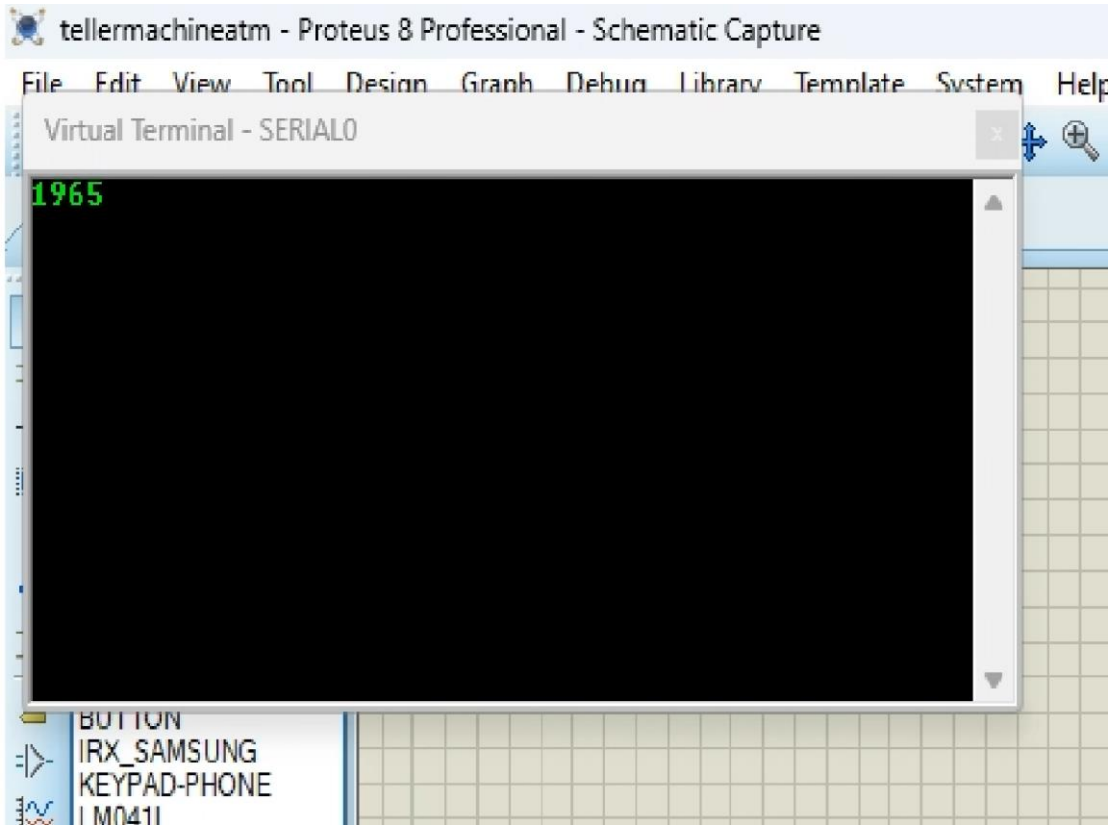

Figure 21 Incorrect PIN

As can be seen above The user entered PIN *1965* instead of *1991* and was not authenticated because of this.

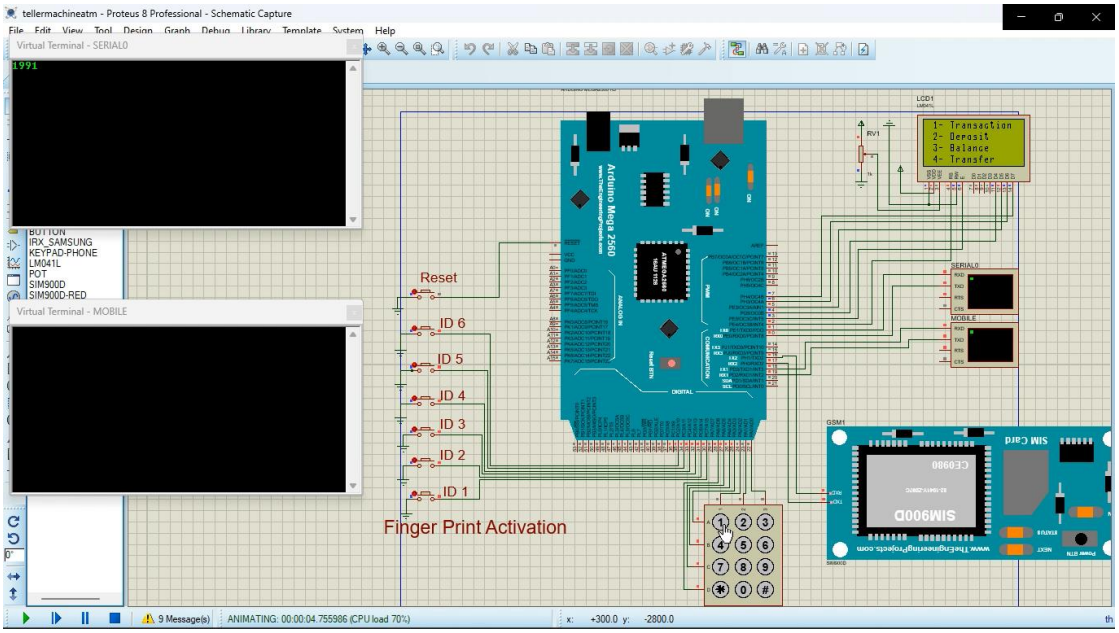

Figure 22 ATM user options.

4.5. OTP Authentication

The third feature of the authentication process is the use of OTPs to authenticate ATM transactions as an added layer of security. The OTP is a random 4-digit PIN that user needs to enter in order to authenticate transactions such as withdraws and balance inquiries from the ATM. The OTP has a short lifespan and will eventually expire if not consumed withing a specified period of time.

The figure below shows the OTP request screen that the user is shown once they need to perform a transaction on the ATM.

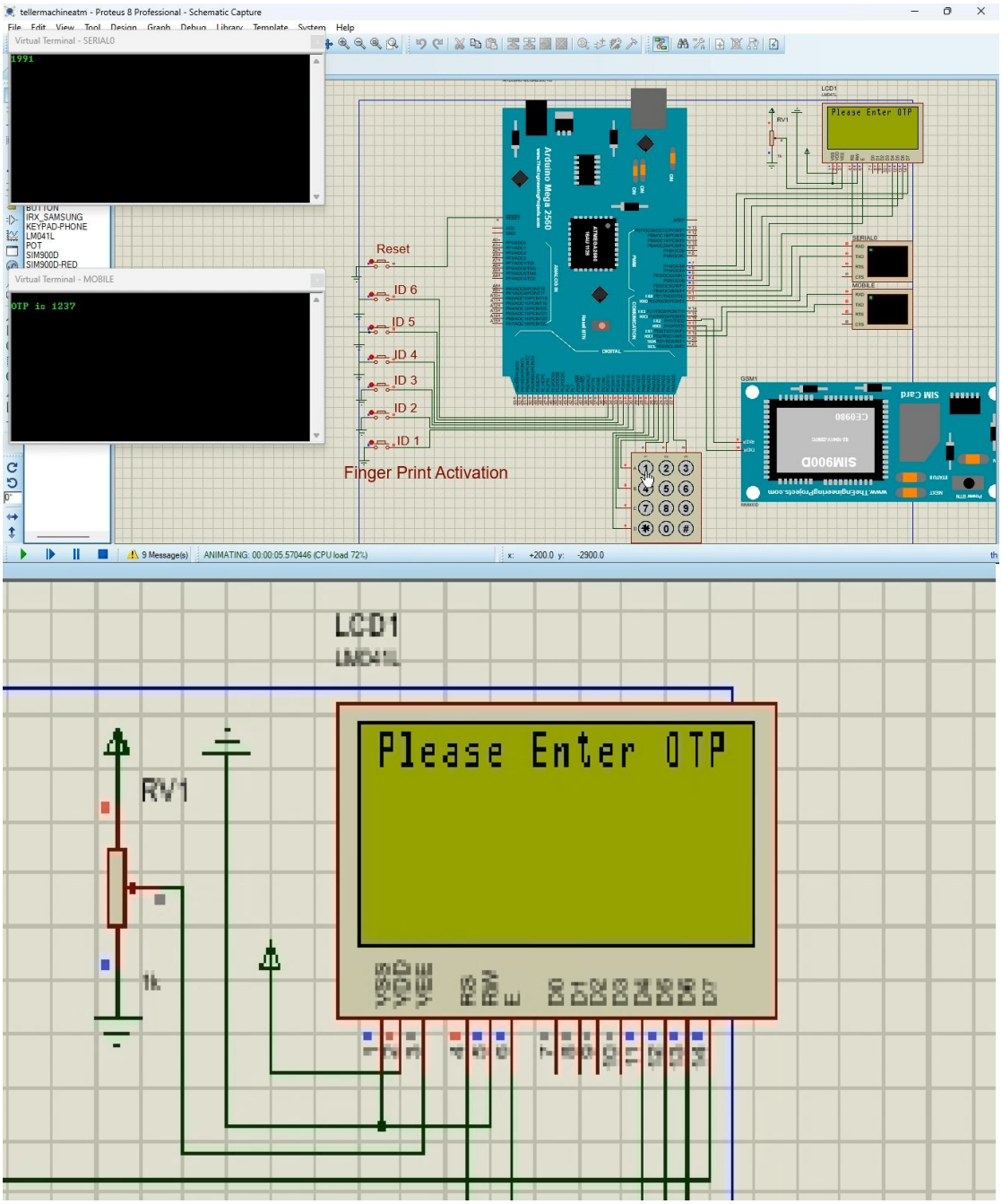

Figure 23 OTP prompt

Figure 26 shows the user being requested to enter the OTP ***1237*** on their mobile device simulated by the GSM module in Proteus Isis. Figure 18 shows an error screen when the user enters an incorrect OTP.

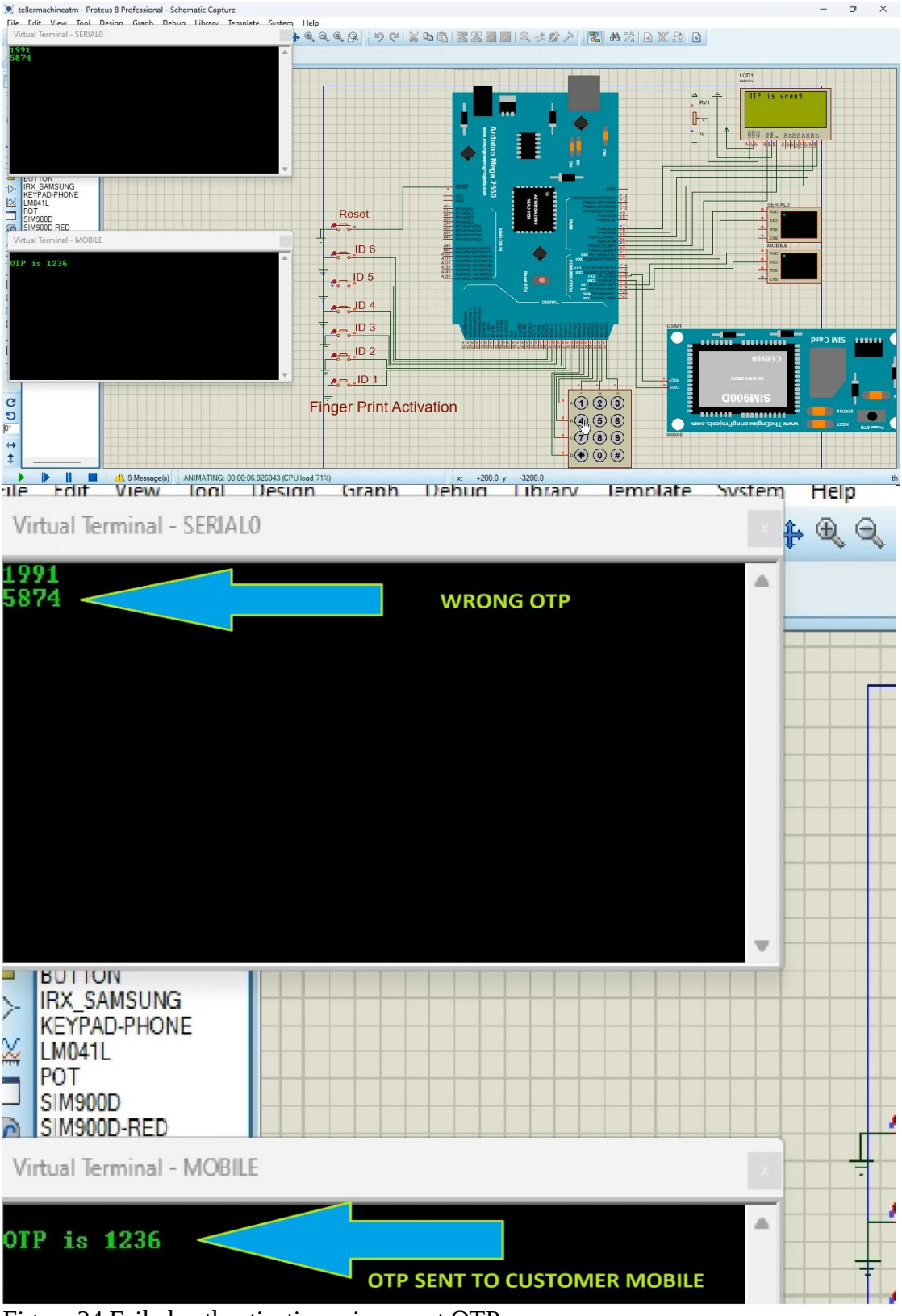

Figure 24 Failed authentication – incorrect OTP

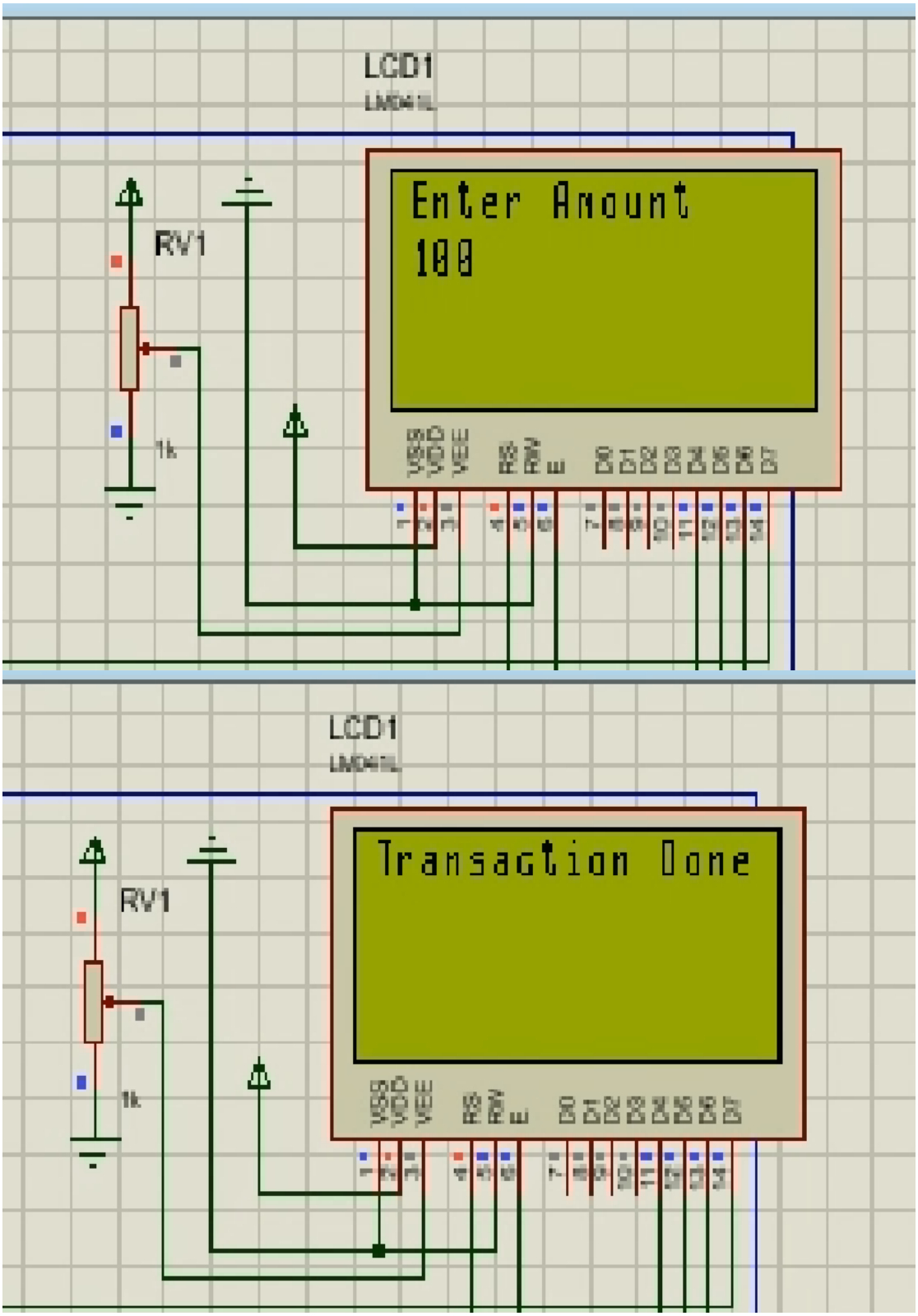

Figure 25 Successful Transaction after OTP authentication

The results from the various simulation tests that were conducted were summarized in the tables below.

Test No.	Finger requested	Fingerprint Provided	Result	Status
1	4	4	Authenticated, user requested to enter PIN	Success
2	6	6	Authenticated, user requested to enter PIN	Success
3	3	3	Authenticated, user requested to enter PIN	Success
4	3	1	Not authenticated, User requested to place correct finger	Failed

Table 1 Table summary of fingerprint simulation tests

Type	Correct Parameter	User Input	Result	Status
PIN	1991	1965	Wrong Pin	Failed
OTP	1236	5874	Wrong OTP	Failed
PIN	1991	1991	User Logged in	Success
OTP	1236	1236	Transaction complete	Success

Table 2 OTP and PIN authentication table summary

Tier	Fingerprint	PIN	OTP	Transaction Status
1	Wrong	x	x	Incomplete
1,2	Correct	Wrong	x	Incomplete
1,2,3	Correct	Correct	Wrong	Incomplete
1,2,3	Correct	Correct	Correct	Complete

Table 3 Authentication matrix

4.6. Chapter Summary

The design simulation was conducted showing all use cases for the proposed design showing the core functionalities. The system randomly requested the user to place any one of 10 fingerprints for authentication. Once successfully recognised as the particular user's fingerprint, the ATM proceeded to request the user for their 4-digit PIN. Upon entering their correct PIN, the user got access to their account and various ATM options such as withdraw and balance inquiry. The design simulation also depicted failed authentication for when a user provides incorrect input such as wrong request finger, wrong 4-digit PIN and wrong OTP.

CHAPTER FIVE

5. CONCLUSION AND DISCUSSION

Based on the results from the previous chapter of the design simulation, in this chapter, the researcher provides a comprehensive design and model of an enhanced and secure cardless withdraw mechanism that encompasses a three-tier authentication model. The researcher designed a system that would not only provide a secure means to transact on ATM and POS channel but also a convenient way to make transaction a financial sector whose current trajectory is cashless and cardless.

5.3. Discussion

The researcher set out to design a system that addressed the two research questions as well as objectives and through the results of the design simulation satisfied them.

The research endeavoured design and demonstrate the core functionalities of the system in order to address the current challenges and limitations of the current ATM/POS setup.

The research highlighted the limitations of the improved ATM debit/credit cards from the old cards with magnetic strip only. The researcher found that chip and PIN cards were still prone to card skimming/cloning due to their continued reliance on the magnetic strip. Card companies have not yet abandoned the magnetic strip because many countries as well as system have not fully migrated to the Chip and Pin concept. The research also highlighted the side effects of the contactless cards which when stolen can be used to carry put unauthenticated purchases and ATM withdraws. ATM terminals and POS terminals have also been known in the past to be compromised by malicious actors who have placed nefarious tools on ATM card readers and POS terminals for the malicious intent of harvesting ATM card data.

The researcher proposed a cardless system that utilizes a multi factor authentication mechanism in order to avert those challenges of the current systems. The research proposed a migration to a cardless system for day-to-day ATM/POS purchases and withdraws through the use of biometric authentication (fingerprint) PIN and OTP.

The design of proposed system incorporates a fingerprint reader to the ATM that works like the ATM card reader and authenticates fingerprints.

Upon providing the correct random fingerprint requested by the system the and correct PIN, the user was fully authenticated and had access to the system prior to conducting any transactions. The simulation demonstrated the first two step authentication process

by flagging appropriate errors where incorrect feedback was provided. The simulation also showed that the system asked for a further authentication process upon conducting an ATM transaction by sending an OTP to the GSM module which simulated the user's mobile device. Upon inputting the correct OTP, the user proceeded to transact successfully and flagged an incorrect OTP error when anything other than the correct OTP was entered. The results showed all the authentication processes.

5.4. Conclusion

In conclusion it is important to note the limitations, challenges and risks that the current payment systems and various mediums have such as card skimming/cloning, shoulder surfing, unauthorised online/ATM/POS transactions after theft of the debit/credit card and PIN and unauthorised contactless transactions among many others. Solutions and systems that offer countermeasures such as the proposed system design are required to address the ever-looming fraudulent activities in the payments and card industry in the financial sector. Zambia has not been an exception to such fraudulent acts as was highlighted in an earlier chapter. A system that implements multifactor authentication and incorporates a biometric system makes it difficult for threat actors to predict or circumvent the inherently strong security features that biometrics have, coupled with random fingerprint requests to avoid fraudsters from predicting in an event that the manage to form a wax copy of the user's fingerprint and finally an OTP that is random and only sent to the customer's mobile device for the final authentication. Card companies such as VISA and Mastercard still have the magnetic strip in use, until such a time that it's completely done away with will issue of card skimming/cloning will come to an end as the chip will offer the much-needed security due to its high level encryption. But as it stands, solutions such as the proposed system design will not only offer the convenience of safe and cardless access to one's account but will also eradicate the risks that come with magnetic striped cards and PIN only.

5.5. Recommendations

After conducting the research, running the simulation tests and obtaining the results, we wish to make a number of recommendations to the proposed design and the current systems in order to enhance the safety of customer accounts.

1. To explorer other circuit design and simulation software that can adequately simulate the fingerprint sensor and capture as well as store biometric data on a centralised database.
2. Alternatively, physical components maybe use used to actualise the design and appreciate it's results.
3. More effort to be made by relevant authorities to carry out comprehensive user engagements and sensitization on the risks prone to card holders and how one may secure their cards physically and online for various payments and purchases.
4. Further, we recommend that bank customers with contactless cards use RFID/NFC proof wallets in order to shield unauthorised/fraudulent POS purchases on their accounts via their contactless cards.
5. We also wish to recommend that an encryption method be employed during fingerprint capture and authentication during a transaction at each terminal, this will add another layer of security.

Further, the researcher recommends implementing a real-world scenario of the proposed design to fully appreciate it's benefits.

5.6. Future Works

For works to be conducted in future the following will need to be considered.

1. Explore means by which fingerprint data will be translated into machine readable for and inserted into the ISO8583 message for relay to the transaction switch for authentication.
2. Embed a fingerprint sensor onto a Physical ATM and implement a real would simulation.
3. Explorer means of incorporating this concept to online purchases instead of the use of a card on ecommerce platforms.

REFERENCES

[1] P. Chandra, M. B. Bank, R. Deb, N. Adnan, P. Chandra Mondal, and M. N. Adnan, "On reinforcing automatic teller machine (ATM) transaction authentication security process by imposing behavioral biometrics," *ieeexplore.ieee.org*, pp. 28–30, doi: 10.1109/ICAEE.2017.8255383.

[2] "Cash machine fraud | Barclays." https://www.barclays.co.uk/fraud-and-scams/cash-machine-fraud/ (accessed Jan. 02, 2023).

[3] M. E.-H. 2011: H. W. and Happiness and undefined 2011, "Practical attack on contactless payment cards," *eprints.ncl.ac.uk*.

[4] "Pros and cons of contactless bank cards." https://www.indiastudychannel.com/resources/168260-Pros-and-cons-of-contactless-bank-cards.aspx (accessed Jan. 02, 2023).

[5] M. M. Rahman, J. Kabi, K. Nazrul, and A. R. Saha, "Automated Teller Machine Card Fraud of Financial Organisations in Bangladesh," *researchgate.net*, 2018, doi: 10.15226/2474-9257/3/1/00126.

[6] P. Kaur, K. Krishan, S. K. Sharma, and T. Kanchan, "ATM Card Cloning and Ethical Considerations," *Sci Eng Ethics*, vol. 25, no. 5, pp. 1311–1320, Oct. 2019, doi: 10.1007/S11948-018-0049-X.

[7] M. Rahman, A. S.-J. of I. Security, and undefined 2019, "A comparative study and performance analysis of ATM card fraud detection techniques," *scirp.org*.

[8] O. Nathaniel, M. O.-G.-I. R. J. of, and undefined 2018, "A Comparative Study of PIN Based and Three-factor Based Authentication Technique for Improved ATM Security," *academia.edu*.

[9] "Scammers using skimmers to get your debit and credit card info - WTOP News." https://wtop.com/crime/2022/10/scammers-using-skimmers-to-get-your-debit-and-credit-card-info/ (accessed Jan. 07, 2023).

[10] "Information Security Hygiene - Credit Card Skimming." https://www.siue.edu/its/news/2021/06/credit-card-skimming.shtml (accessed Jan. 07, 2023).

[11] K. Vengatesan, A. Kumar, S. Yuvraj, V. D. A. Kumar, and S. S. Sabnis, "CREDIT CARD FRAUD DETECTION USING DATA ANALYTIC TECHNIQUES," *JOURNAL Advances in Mathematics: Scientific Journal*, vol. 9, no. 3, pp. 1857–8438, 2020, doi: 10.37418/amsj.9.3.43.

[12] "Chip-And-PIN Card Definition." https://www.investopedia.com/terms/c/chipandpin-card.asp (accessed Jan. 02, 2023).

[13] "Verified by Visa | Secure Online Payment | Visa." https://www.visa.co.in/pay-with-visa/featured-technologies/verified-by-visa.html (accessed Jan. 02, 2023).

[14] "Credit Card Cloning: Definition and Ways To Protect Yourself." https://www.investopedia.com/terms/c/cloning.asp (accessed Jan. 02, 2023).

[15] D. Singh, P. Kushwaha, P. Choubey, … A. V.-P. of the world, and undefined 2011, "A proposed framework to prevent financial fraud through ATM card cloning," *iaeng.org*.

[16] B. Gupta, S. N.-J. of G. I. Management, and undefined 2020, "A survey on contactless smart cards and payment system: technologies, policies, attacks and countermeasures," *igi-global.com*, vol. 28, doi: 10.4018/JGIM.2020100108.

[17] J. Kalunga, S. T.-A. J. of B. Research, and undefined 2016, "Development of fingerprint biometrics verification and vetting management system," *academia.edu*.

[18] … L. M.-F. U. of P. and M. (Gumel and undefined 2011, “Use of biometrics to tackle ATM fraud,” *ipedr.com*.
[19] L. Narayan, S. G, and S. M, “Fingerprint Recognition and its Advanced Features,” *International Journal of Engineering Research and*, vol. V9, Apr. 2020, doi: 10.17577/IJERTV9IS040393.
[20] A. S.-2014 I. C. on Circuits, undefined Power, and undefined 2014, “Biometrics to control ATM scams: A study,” *ieeexplore.ieee.org*.
[21] S. A.-S. C. A. Paper, undefined November, and undefined 2006, “The what, who and why of contactless payments,” *securetechalliance.org*, 2006.
[22] V. B.-A. J. F. C. I. T. (AJCT) and undefined 2018, “FINGER PRINT BASED BIOMETRIC AUTHENTICATION SYSTEM FOR ATM SYSTEM,” *asianssr.org*.
[23] Shally, G. Aujla, and S. Aujla, “A REVIEW OF ONE TIME PASSWORD MOBILE VERIFICATION,” *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, vol. 4, pp. 113–118, Jun. 2014.
[24] M. Al Imran, M. Mridha, … M. N.-I. C. on, and undefined 2019, “OTP based cardless transction using ATM,” *ieeexplore.ieee.org*, doi: 10.1109/ICREST.2019.8644248.
[25] O. K. Afriyie and V. Arkorful, “Enhancing security of automated teller machines using biometric authentication: A case of a Sub-Saharan University,” vol. 9, no. 7, 2019, doi: 10.7176/IKM.
[26] N. Alyousif and S. Alhabis, “The Necessity of Multi Factor Authentication,” Apr. 2022, doi: 10.5281/ZENODO.6472757.
[27] O. Ebenezer, M. O-Genseleke, E. N. Osuigbo, and C. Chigozie-Okwum, “Implementation of multifactor based authentication scheme for enhanced atm security,” *researchgate.net*, vol. 181, no. 1, pp. 975–8887, 2018, doi: 10.5120/ijca2018917400.
[28] N. Akinyokun and V. Teague, “Security and privacy implications of NFC-enabled contactless payment systems,” *ACM International Conference Proceeding Series*, vol. Part F130521, Aug. 2017, doi: 10.1145/3098954.3103161.
[29] D. Mahansaria, U. R.-2019 I. Carnahan, and undefined 2019, “Secure Authentication for ATM transactions using NFC technology,” *ieeexplore.ieee.org*.
[30] “2 Chinese men in court for theft, ‘ATM fraud’ - Zambia: News Diggers!” https://diggers.news/courts/2019/07/17/2-chinese-men-in-court-for-theft-atm-fraud/ (accessed Jan. 07, 2023).
[31] “ATM skimming fraud: DEC arrest Chinese gang cloning bank cards in Zambia – Mwebantu.” https://www.mwebantu.com/atm-skimming-fraud-dec-arrest-chinese-gang-cloning-bank-cards-in-zambia/ (accessed Jan. 02, 2023).
[32] “Barclays Bank Zambia hit by ATM fraud - PC Tech Magazine.” https://pctechmag.com/2013/03/barclays-bank-zambia-hit-by-atm-fraud/ (accessed Jan. 02, 2023).
[33] “Zambia : US$ 4 million stolen through ATMs in Zambia-Police.” https://www.lusakatimes.com/2013/06/14/us-4-million-stolen-through-atms-in-zambia-police/ (accessed Jan. 02, 2023).
[34] D. Ranjitham, S. Manoharan, V. Murugesan, S. Sabaresan Ravi, and A. Professor, “Face Recognition and Fingerprint Based New Generation ATM,” *ijisrt.com*, vol. 3, no. 3, 2018.

[35] A. Iyabode, Y. Nureni, … A. A.-I. J. of, and undefined 2015, "Card-less electronic automated teller machine (EATM) with biometric authentication," *Citeseer*, vol. 30, no. 2, 2015.

[36] S. M. Shuhidan *et al.*, "AES cardless automatic teller machine (ATM) biometric security system design using FPGA implementation," *iopscience.iop.org*, doi: 10.1088/1757-899X/160/1/012113.

[37] S. Das, J. D.-I. J. of I. and, and undefined 2011, "Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system," *Citeseer*.

[38] A. Omolara, A. Jantan, … O. A.-… J. of E., and undefined 2019, "Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication.," *researchgate.net*.

[39] T. Sangeetha, M. Kumaraguru, … S. A.-J. of P., and undefined 2021, "Biometric based fingerprint verification system for atm machines," *iopscience.iop.org*, doi: 10.1088/1742-6596/1916/1/012273.

[40] P. Choudhary, A. Tripathi, A. K. Singh, and P. C. Vashist, "Implementation of integrated security system by using biometric function in ATM machine," *Advances in Intelligent Systems and Computing*, vol. 1125, pp. 33–42, 2020, doi: 10.1007/978-981-15-2780-7_5.

[41] D. Bhattacharyya, R. Ranjan, A. A. Farkhod, and M. Choi, "Biometric authentication: A review," *biometrie-online.net*, vol. 2, no. 3, 2009, Accessed: Jan. 07, 2023. [Online]. Available: https://www.biometrie-online.net/images/stories/dossiers/generalites/International-Journal-of-u-and-e-Service-Science-and-Technology.pdf

[42] M. Karovaliya, S. Karedia, … S. O.-P. C., and undefined 2015, "Enhanced security for ATM machine with OTP and facial recognition features," *Elsevier*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915004093

[43] K. Yadav, S. Mattas, … L. S.-2020 F. I., and undefined 2020, "Secure card-less atm transactions," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9242713/

[44] S. Sankhwar, D. P.-2016 I. 6th International, and undefined 2016, "A safeguard against ATM fraud," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7544924/

[45] M. K.-I. J. on R. and I. Trends and undefined 2015, "Securing ATM with OTP and Biometric," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/48577673/Securing_ATM_with_OTP_and_Biometric.pdf

[46] J. Soares, A. G.-2016 I. C. on, and undefined 2016, "A self banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7754189/

[47] J. Soares, A. G.-2016 I. C. on, and undefined 2016, "Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7877618/

[48] D. Mahansaria, U. R.-2019 I. Carnahan, and undefined 2019, "Secure Authentication for ATM transactions using NFC technology," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8888427/

[49] R. M.-2012 F. I. C. on and undefined 2012, "Advanced biometric ATM machine with AES 256 and steganography implementation," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6416799/

[50] J. Shamdasani, P. M.-I. J. of E. Trends, and undefined 2014, "ATM Client Authentication System Using Biometric Identifier & OTP," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/34110774/N044057478.pdf

[51] M. Rahman, A. S.-J. of I. Security, and undefined 2019, "A comparative study and performance analysis of ATM card fraud detection techniques," *scirp.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.scirp.org/html/6-7800599_94090.htm

[52] J. A.-J. of S. Sciences and undefined 2011, "Automated teller machine (ATM) frauds in Nigeria: The way out," *Taylor & Francis*, vol. 27, no. 1, pp. 53–58, Apr. 2011, doi: 10.1080/09718923.2011.11892905.

[53] L. M.-K. F. U. of P. and Minerals and undefined 2011, "Use of biometrics to tackle ATM fraud," *ipedr.com*, Accessed: Jan. 02, 2023. [Online]. Available: http://ipedr.com/vol1/71-G00018.pdf

[54] S. Sankhwar, D. P.-2016 I. 6th International, and undefined 2016, "A safeguard against ATM fraud," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7544924/

[55] P. Kaur, K. Krishan, S. Sharma, T. K.-S. and engineering, and undefined 2019, "ATM card cloning and ethical considerations," *Springer*, Accessed: Jan. 02, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11948-018-0049-x

[56] S. Nashwan, B. A.-I. journal of computer and, and undefined 2014, "Mutual chain authentication protocol for span transactions in Saudi Arabian banking," *researchgate.net*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Shadi-Nashwan/publication/271305390_Mutual_Chain_Authentication_Protocol_for_SPAN_Transactions_in_Saudi_Arabian_Banking/links/580fd26508ae009606bb8ce3/Mutual-Chain-Authentication-Protocol-for-SPAN-Transactions-in-Saudi-Arabian-Banking.pdf

[57] M. A. A. Singaraj *et al.*, "2-FACTOR AUTHENTICATION FOR AVOIDING FRAUDULENCES IN ATM SERVICES BY MMBS," *EPRA International Journal of Research & Development (IJRD)*, vol. 2, no. 1, pp. 1–1, 2017, Accessed: Jan. 02, 2023. [Online]. Available: https://eprajournals.com/IJSR/article/382

[58] S. Bhosale, … B. S. A. T. & E., and undefined 2012, "Security in e-banking via cardless biometric ATMs," *researchgate.net*, vol. 2, no. 4, 2012, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Satish-Bhosale-2/publication/260982820_SECURITY_IN_E-BANKING_VIA_CARD_LESS_BIOMETRIC_ATMS/links/00b7d532d7f6589912000000/SECURITY-IN-E-BANKING-VIA-CARD-LESS-BIOMETRIC-ATMS.pdf

[59] S. Acharya, A. Polawar, … P. P.-J. of C. E., and undefined 2013, "Two factor authentication using smartphone generated one time password," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/32109225/L01128590.pdf

[60] K. Okereafor, O. Osuagwu, C. O.- IJSSST, and undefined 2018, "Biometric Anti-spoofing Technique Using Randomized 3D Multi-Modal Traits," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/70915745/e8941430006cf9800e6c20e714a39a025548.pdf

[61] A. STEVEN and L. AROKIASAMY, "FINGERPRINT BASED AUTOMATIC TELLER MACHINE," *core.ac.uk*, Accessed: Jan. 02, 2023. [Online]. Available: https://core.ac.uk/download/pdf/275672242.pdf

[62] K. Okereafor, O. Osuagwu, … S. A.-J. H., and undefined 2020, "RANDOMIZED MULTI-BIOMETRIC LIVENESS DETECTION: PROSPECTS AND APPLICATIONS FOR SECURE AUTHENTICATION," *researchgate.net*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Habeebullah-Hussaini-Syed/publication/359274703_RANDOMIZED_MULTI-BIOMETRIC_LIVENESS_DETECTION_PROSPECTS_AND_APPLICATIONS_FOR_SECURE_AUTHENTICATION/links/6232889d4ba65b248137396d/RANDOMIZED-MULTI-BIOMETRIC-LIVENESS-DETECTION-PROSPECTS-AND-APPLICATIONS-FOR-SECURE-AUTHENTICATION.pdf

[63] T. REDDY, "Multi-Banking Transaction ATM System using Biometric and GSM Authentication," 2019, Accessed: Jan. 02, 2023. [Online]. Available: http://14.99.188.242:8080/jspui/handle/123456789/10761

[64] A. Ometov, S. Bezzateev, N. Mäkitalo, S. A.- Cryptography, and undefined 2018, "Multi-factor authentication: A survey," *mdpi.com*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.mdpi.com/251356

[65] D. S.-I. journal of engineering inventions and undefined 2014, "Fingerprint based biometric ATM authentication system," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/34056378/D030112228.pdf

[66] M. Onyesolu, I. E.-I. J. of Advanced, and undefined 2012, "ATM security using fingerprint biometric identifer: An investigative study," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/86244636/38638acaa21bcabc9c3b517c43a780e444c2.pdf

[67] P. Kamble, B. G.-I. J. of S. and, and undefined 2012, "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/40340132/ijsrp-nov-2012-print.pdf#page=260

[68] H. Lasisi, … A. A. A. in C. T. for, and undefined 2012, "Development of stripe biometric based fingerprint authentications systems in Automated Teller Machines," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6462860/

[69] A. Jaiswal, … M. B.-J. of C. S. and M., and undefined 2014, "Enhancing ATM security using Fingerprint and GSM technology," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/33382432/V3I4201409.pdf

[70] S. Mandal, "A Review on Secured Money Transaction with Fingerprint Technique in ATM System," Jul. 2013, Accessed: Jan. 02, 2023. [Online]. Available: http://arxiv.org/abs/1307.8043

[71] S. M. preprint arXiv:1307.8043 and undefined 2013, “A Review on Secured Money Transaction with Fingerprint Technique in ATM System,” *arxiv.org*, vol. 2, no. 4, 2013, Accessed: Jan. 02, 2023. [Online]. Available: https://arxiv.org/abs/1307.8043

[72] M. Gayathri, P. Selvakumari, … R. B. engineering sciences &, and undefined 2014, “Fingerprint and GSM based security system,” *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/33658384/75.pdf

[73] A. Taralekar, G. Chouhan, … R. T.-… C. on B., and undefined 2017, “One touch multi-banking transaction ATM system using biometric and GSM authentication,” *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8336574/

[74] D. M.-I. J. of S. and Research and undefined 2014, “Face recognition technique: Enhanced safety approach for ATM,” *Citeseer*, Accessed: Jan. 02, 2023. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=73959ddd6a7ee6aa33ced32f9259b96d9a25e1f3

[75] B. Sahar, … A. R.-… on E. and S., and undefined 2018, “Fingershield atm–atm security system using fingerprint authentication,” *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8605473/

[76] M. Kassem, N. Mekky, R. E.-A.-I. J. of, and undefined 2014, “An enhanced ATM security system using multimodal biometric strategy,” *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/63829651/144204-7171-IJECS-IJENS.pdf

[77] B. W.-I. ABEC and undefined 2021, “Design and Implementation of an Arduino Based Smart Fingerprint Authentication System for Key Security Locker,” *abecindonesia.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://abecindonesia.org/iabec/index.php/iabec/article/view/15

[78] S. Oko, J. O.-I. J. of C. S. Issues, and undefined 2012, “Enhanced ATM security system using biometrics,” *researchgate.net*, 2012, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Jane-Oruh/publication/344966848_ENHANCED_ATM_SECURITY_SYSTEM_USING_BIOMETRICS/links/602cd571a6fdcc37a830192e/ENHANCED-ATM-SECURITY-SYSTEM-USING-BIOMETRICS.pdf

[79] Y. Yang, J. M.-2010 2nd I. C. on Computer, and undefined 2010, “ATM terminal design is based on fingerprint recognition,” *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5486288/

[80] D. Ranjitham, S. Manoharan, V. Murugesan, S. Sabaresan Ravi, and A. Professor, “Face Recognition and Fingerprint Based New Generation ATM,” *ijisrt.com*, vol. 3, no. 3, 2018, Accessed: Jan. 02, 2023. [Online]. Available: https://ijisrt.com/wp-content/uploads/2018/04/Face-Recognition-and-Fingerprint-Based-New-Generation-ATM.pdf

[81] F. Han, J. Hu, X. Yu, Y. Feng, and J. Zhou, “A novel hybrid crypto-biometric authentication scheme for ATM based banking applications,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3832 LNCS, pp. 675–681, 2006, doi: 10.1007/11608288_90.

[82] J. Nawaya, N. Jemimah, N. O.-D. of C. Science, and undefined 2019, "Designing a Biometric (Finger) Using Multispectral Imaging Biometric Authentication Measures for Enhancing ATM Security in Nigeria," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/61339401/V8I1120191120191126-22730-exzf5d.pdf

[83] P. Kaur, K. Krishan, S. K. Sharma, and T. Kanchan, "ATM Card Cloning and Ethical Considerations," *Sci Eng Ethics*, vol. 25, no. 5, pp. 1311–1320, Oct. 2019, doi: 10.1007/S11948-018-0049-X.

[84] J. A.-J. of S. Sciences and undefined 2011, "Automated teller machine (ATM) frauds in Nigeria: The way out," *Taylor & Francis*, vol. 27, no. 1, pp. 53–58, Apr. 2011, doi: 10.1080/09718923.2011.11892905.

[85] N. A. K. Abiew, M. D. Jnr., and S. O. Banning, "Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems," *Asian Journal of Research in Computer Science*, vol. 5, no. 3, pp. 7–20, Apr. 2020, doi: 10.9734/AJRCOS/2020/V5I330135.

[86] F. Twum, K. Nti, M. A.-I. J. of S. and, and undefined 2016, "Improving security levels in Automatic Teller Machines (ATM) using multifactor authentication," *ijsea.com*, vol. 5, pp. 2319–7560, 2016, Accessed: Jan. 02, 2023. [Online]. Available: http://www.ijsea.com/archive/volume5/issue3/IJSEA05031003.pdf

[87] F. Aloul, S. Zahidi, W. E.-H.-2009 I. international, and undefined 2009, "Two factor authentication using mobile phones," *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5069395/

[88] A. Fali Oklilas *et al.*, "Developing a Multi-Factor Authentication-Based Cardless Electronic Payment System," *iopscience.iop.org*, doi: 10.1088/1755-1315/665/1/012009.

[89] E. A. Kayode, … Y. A.-I., and undefined 2019, "Multi-factor authentication model for integrating iris recognition into an automated teller machine," *publication.babcock.edu.ng*, vol. 181, no. 45, pp. 975–8887, 2019, Accessed: Jan. 02, 2023. [Online]. Available: https://publication.babcock.edu.ng/asset/docs/publications/COSC/9457/3998.pdf

[90] O. A.-I. J. of C. S. Issues and undefined 2012, "Evaluating the performance of two-factor authentication solution in the banking sector," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/79499610/IJCSI-9-4-2-457-462.pdf

[91] K. Olatunji, C. Afolalu, O. A.-J. Multidiscpl. Eng. Sci. Technol., and undefined 2016, "Design and Implementation of a Multifactor Authentication System In ATM Security," *jmest.org*, vol. 3, pp. 2458–9403, 2016, Accessed: Jan. 02, 2023. [Online]. Available: http://www.jmest.org/wp-content/uploads/JMESTN42351785.pdf

[92] S. S.- Melange and undefined 2020, "Multifactor Authentication for ATM Security System," *iirjet.org*, vol. 5, pp. 2456–1983, 2020, Accessed: Jan. 02, 2023. [Online]. Available: http://iirjet.org/index.php/home/article/view/93

[93] M. Ojewale, P. Y.-U. P. J. of Engineering, and undefined 2019, "Multi-Factor Authentication and Fingerprint-based Debit Card System," *cister.isep.ipp.pt*, vol. 5, no. 2, pp. 19–28, 2019, doi: 10.24840/2183-6493_005.002_0003.

[94] D. Jacqueline Akinyi Madara, G. Okeyo, and M. Kimwele, “A Fingerprint &Pin Authentication to Enhance Security At The Automatic Teller Machines,” 2017, Accessed: Jan. 02, 2023. [Online]. Available: http://197.136.134.32/handle/123456780/4294

[95] P. S.-B. technology today and undefined 2017, “Biometrics at the ATM,” *Elsevier*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0969476517300152

[96] P. Aithal, “A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP,” 2018, Accessed: Jan. 02, 2023. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097480

[97] K. P. Karani, S. Aithal, K. Prasad, K. #1, and P. S. Aithal, “A STUDY ON MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE AND IRIS RECOGNITION,” *researchgate.net*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Sreeramana-Aithal/publication/332763949_A_STUDY_ON_MULTIFACTOR_AUTHENTICATION_MODEL_USING_FINGERPRINT_HASH_CODE_AND_IRIS_RECOGNITION/links/5cc8763492851c8d220ffcb0/A-STUDY-ON-MULTIFACTOR-AUTHENTICATION-MODEL-USING-FINGERPRINT-HASH-CODE-AND-IRIS-RECOGNITION.pdf

[98] J. O.-I. J. of C. S. and and undefined 2014, “Three-factor authentication for automated teller machine system,” *researchgate.net*, vol. ISSN, no. 6, pp. 2249–9555, 2014, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Jane-Oruh/publication/339552950_Three-Factor_Authentication_for_Automated_Teller_Machine_System/links/604b6178299bf1f5d841728d/Three-Factor-Authentication-for-Automated-Teller-Machine-System.pdf

[99] A. Iyabode, Y. Nureni, … A. A.-I. J. of, and undefined 2015, “Card-less electronic automated teller machine (EATM) with biometric authentication,” *Citeseer*, Accessed: Jan. 02, 2023. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0075f13c9c4c2c8bc1a6d4a4cbc5680aafe9b332

[100] M. Onyesolu, A. O.-I. J. of Computer, and undefined 2017, “Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM).,” *mecs-press.com*, vol. 10, pp. 50–56, 2017, doi: 10.5815/ijcnis.2017.10.06.

[101] N. Gyamfi, … M. M.-I. J. of, and undefined 2016, “Enhancing the security features of automated teller machines (ATMs): A Ghanaian perspective,” *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/48365655/15.pdf

[102] S. Pravinthraja, K. U.-B. I. Journal, and undefined 2011, “Multimodal biometrics for improving automatic teller machine security,” *researchgate.net*, vol. 1, 2011, doi: 10.9756/BIJAIP.1005.

[103] K. Okokpujieemail, N.-O. Okesolaosemwegie, O. Okerekesamuel, and J. P. Okokpujie, “Integration of iris biometrics in automated teller machines for enhanced user authentication,” *Springer*, 2018, Accessed: Jan. 02, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-13-1056-0_23

[104] O. Awodele, A. A.-I. J. of E. T. and, and undefined 2012, “Combating automated teller machine frauds through biometrics,” *Citeseer*, Accessed: Jan.

02, 2023. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=add3eb244cb24f6d674f4e305b92d992dfad3c5a

[105] A. Ameh, O. Olanyi, O. A.-J. of A. Security, and undefined 2016, "Securing cardless automated teller machine transactions using bimodal authentication system," *Taylor & Francis*, vol. 11, no. 4, Accessed: Jan. 02, 2023. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/19361610.2016.1211846

[106] A. I. Ameh, O. M. Olanyi, and O. S. Adewale, "Securing Cardless Automated Teller Machine Transactions Using Bimodal Authentication System," *Journal of Applied Security Research*, vol. 11, no. 4, pp. 469–488, Oct. 2016, doi: 10.1080/19361610.2016.1211846.

[107] S. Aljuaid, A. A.-Comput. Syst. Sci. Eng., and undefined 2022, "Automated Teller Machine Authentication Using Biometric.," *researchgate.net*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Arshiya-Ansari-2/publication/357492150_Automated_Teller_Machine_Authentication_Using_Biometric/links/63065df65eed5e4bd1181420/Automated-Teller-Machine-Authentication-Using-Biometric.pdf

[108] A. Kale, S. N.-I. J. of A. R. in, and undefined 2014, "A Review Paper on Design of Highly Secured Automatic Teller Machine System by using Aadhaar card and Fingerprint," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/34193910/V2I1-0085.pdf

[109] H. Babaei, O. Molalapata, AA Pandor - ICIKM, and undefined 2012, "Face Recognition Application for Automatic Teller Machines (ATM)," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/33481389/041-ICIKM2012-M0080.pdf

[110] A. J.-T. J. of C. and Mathematics and undefined 2021, "A systematic review comparing different security measures adopted in automated teller machine," *turcomat.org*, vol. 12, no. 13, pp. 388–393, 2021, Accessed: Jan. 02, 2023. [Online]. Available: https://www.turcomat.org/index.php/turkbilmat/article/view/8302

[111] P. Ochang, P. O.-I. J. of Advanced, and undefined 2017, "An Enhanced Automated Teller Machine Security Prototype using Fingerprint Biometric Authentication," *search.proquest.com*, Accessed: Jan. 02, 2023. [Online]. Available: https://search.proquest.com/openview/f2c4d0dab1e0ffbd74d7496c3710d537/1?pq-origsite=gscholar&cbl=886380

[112] L. Coventry, A. de Angeli, and G. Johnson, "Usability and biometric verification at the ATM interface," *Conference on Human Factors in Computing Systems - Proceedings*, pp. 153–160, 2003, doi: 10.1145/642611.642639.

[113] H. Alzamel, … M. A.-H. A. A., and undefined 2019, "Point of Sale (POS) Network with Embedded Fingerprint Biometric Authentication," *papers.ssrn.com*, Accessed: Jan. 02, 2023. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3464825

[114] C. J.-A. J. of A. M. and and undefined 2014, "Effects of automated teller machine on the performance of Nigerian banks," *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/56056332/ajams-2-1-7.pdf

[115] M. Takawale and M. Mane, “A SURVEY ON CARDLESS AUTOMATED TELLER MACHINE (ATM),” 2019, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/59893840/IRJET-V6I4121420190629-56092-13vd7uv.pdf
[116] S. Sisat, V. Barbudhe, P. B.-I. J. of, and undefined 2014, “Secured Automatic Teller Machine (ATM) and Cash Deposit Machine (CDM),” *academia.edu*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.academia.edu/download/48439789/1.pdf
[117] S. Choudhury, S. Bandyopadhyay, S. Chatterjee, R. Dutta, and S. Dutta, “A hybrid approach to enhance the security of automated teller machine,” *Advances in Intelligent Systems and Computing*, vol. 508, pp. 699–709, 2017, doi: 10.1007/978-981-10-2750-5_71.
[118] S. Choudhury, S. Bandyopadhyay, … S. C.-… on C. and, and undefined 2017, “A Hybrid Approach to Enhance the Security of Automated Teller Machine,” *Springer*, Accessed: Jan. 02, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-10-2750-5_71
[119] S. Choudhury, S. Bandyopadhyay, … S. C.-… on C. and, and undefined 2017, “A Hybrid Approach to Enhance the Security of Automated Teller Machine,” *Springer*, Accessed: Jan. 02, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-10-2750-5_71
[120] O. H.-2021 T. I. C. on Intelligent and undefined 2021, “A Proposed Approach to Secure Automated Teller Machine-Based Financial Transactions,” *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9694249/
[121] V. Ohta, V. A.-F. Sci. Tech. J, and undefined 2005, “Promoting universal design of automated teller machines (ATMs),” *fujitsu.com*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol41-1/paper12.pdf
[122] J. Awotunde, R. Jimoh, O. M.-I. 2015, and undefined 2015, “SECURE AUTOMATED TELLER MACHINE (ATM) USING FINGERPRINT AUTHENTICATION AND SHORT-CODE MESSAGE IN A CASHLESS SOCIETY,” *researchgate.net*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Orunsolu-Abdul/publication/323320213_A_CRYPTOGRAPHIC_ANTI-PHISHING_SCHEME/links/5ab3b4d60f7e9b4897c69a38/A-CRYPTOGRAPHIC-ANTI-PHISHING-SCHEME.pdf#page=104
[123] J. Awotunde, R. Jimoh, O. M.-I. 2015, and undefined 2015, “SECURE AUTOMATED TELLER MACHINE (ATM) USING FINGERPRINT AUTHENTICATION AND SHORT-CODE MESSAGE IN A CASHLESS SOCIETY,” *researchgate.net*, Accessed: Jan. 02, 2023. [Online]. Available: https://www.researchgate.net/profile/Orunsolu-Abdul/publication/323320213_A_CRYPTOGRAPHIC_ANTI-PHISHING_SCHEME/links/5ab3b4d60f7e9b4897c69a38/A-CRYPTOGRAPHIC-ANTI-PHISHING-SCHEME.pdf#page=104
[124] E. D. Dimaunahan, A. H. Ballado, and F. R. G. Cruz, “Raspberry Pi and IOT Based-automated teller machine security for the DSWD 4P’s biometric system using fingerprint recognition with fast-fourier transform image enhancement, multi-stage minutia extraction,” *ACM International Conference Proceeding Series*, vol. Part F132084, pp. 3–8, Aug. 2017, doi: 10.1145/3127942.3127945.

[125] A. Ogihara, … H. M.-… S. on I., and undefined 2005, “Biometric verification using keystroke motion and key press timing for atm user authentication,” *ieeexplore.ieee.org*, Accessed: Jan. 02, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4212259/

Appendix A: Gantt Chart

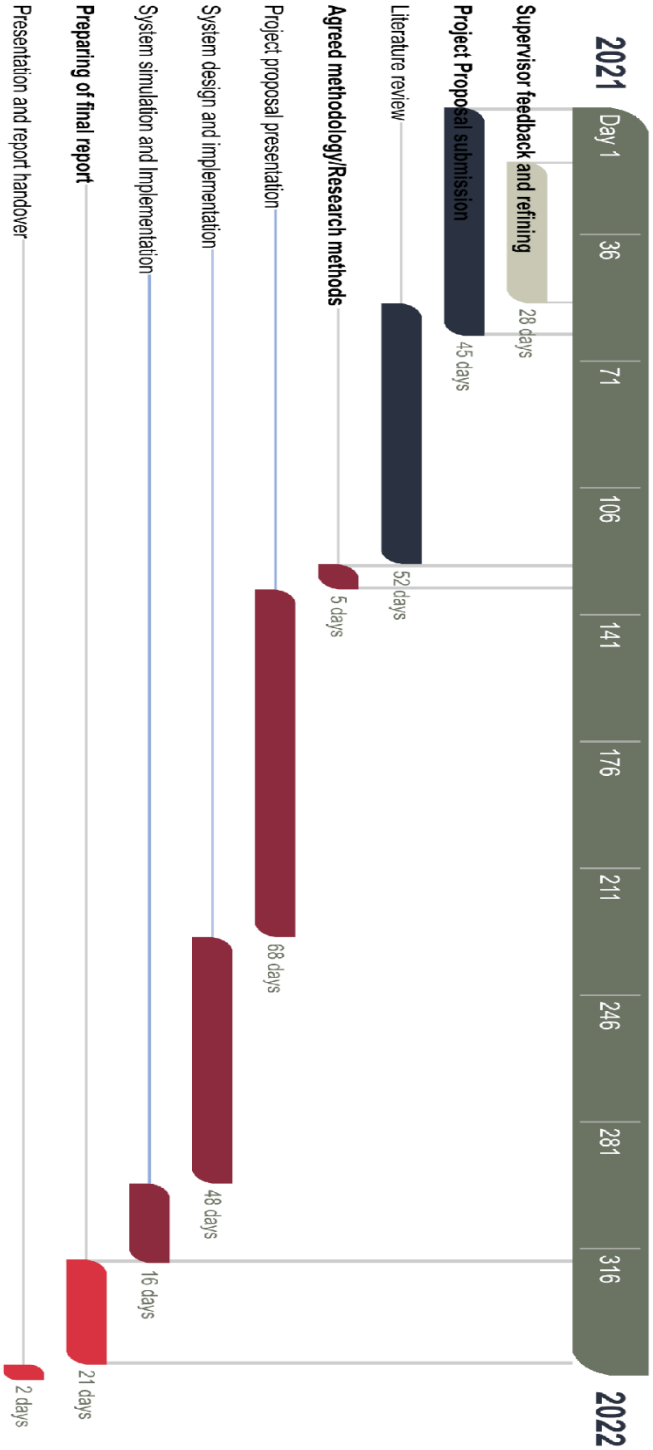

Figure 26 Gantt Chart of Project timelines

Appendix B: Budget

The Research budget is projected to be more than **ZMW 9,689.20,** the breakdown of the costs may be reviewed in table 1 below.

Activity	Approximate Cost (ZMW)
Proteus License	$248 @17.9 **K 4,439.20**
Transport	**K 1,500.00**
Printing and Binding	**K 1,700.00**
Talk time and Bundles	**K 1,300.00**
Bond paper	**K 750.00**
TOTAL	**K 9,689.20**

Table 4. Research Budget

Appendix C: Publication Certificate

Appendix D: Source code

The program source code for the Arduino was coded in the C language and is provided below;

```
#include <Wire.h>
#include <LiquidCrystal.h>
#include <Keypad.h>
 const byte ROWS = 4; //four rows
const byte COLS = 3; //three columns
int count = 0;
int back; int op;
int back1; int op1;
int back2; int op2;
int back3; int op3;
int back4; int op4;
int back5; int op5;
int back6; int op6;
int count1 = 0;
int ask=0;
```

```
int new1=0;
char key;
int choice;
int amount;
char PIN [4];
char OTP [4];
int n; int randn;
int balance = 10000;


char keys[ROWS][COLS] = {
  {'1','2','3'},
  {'4','5','6'},
  {'7','8','9'},
  {'*','0','#'}
};

byte rowPins[ROWS] = {25, 26, 27, 28}; //connect to the row pinouts of the keypad
byte colPins[COLS] = {24, 23, 22}; //connect to the column pinouts of the keypad

Keypad keypad = Keypad( makeKeymap(keys), rowPins, colPins, ROWS, COLS );

// for the lcd pins
const int rs = 2, en = 3, d4 = 4, d5 = 5, d6 = 6, d7 = 7;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);
int s1,s2,s3,s4,s5,s6;

void setup(){
pinMode(30,INPUT_PULLUP);
pinMode(31,INPUT_PULLUP);
pinMode(32,INPUT_PULLUP);
pinMode(33,INPUT_PULLUP);
pinMode(34,INPUT_PULLUP);
pinMode(35,INPUT_PULLUP);
```

```
pinMode(36,INPUT_PULLUP);
Serial.begin(9600);
 Serial1.begin(9600);
 Serial2.begin(9600);
lcd.begin(16, 4);
lcd.setCursor(0,0);
 lcd.print("Welcome to ");
lcd.setCursor(0,1);
 lcd.print("UNZA Bank");
 lcd.setCursor(0,2);
 lcd.print("ATM");
delay(200);
randomSeed(2);

}

// main loop
void loop (){
s1 = digitalRead(30);
s2 = digitalRead(31);
s3 = digitalRead(32);
s4 = digitalRead(33);
s5 = digitalRead(34);
s6 = digitalRead(35);
//Serial.println(s2);
    lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Place");
lcd.setCursor(0,1);
lcd.print("Finger #  ");
randn = random(1, 7);
lcd.print(randn);
delay(1000);
back:
```

```
count=0;
if ( randn == 1 && s1 == 0 && s2 == 1 && s3 == 1 && s4 == 1 && s5 == 1 && s6
== 1){
lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Welcome ID 1");
  delay(180);
  lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Enter your pin");
    delay(100);
while(ask<=1){
    char key = keypad.getKey();
    if (key) {
            lcd.setCursor ( PIN[count],1);
            PIN[count]=key;
            lcd.print(PIN[count]);
            Serial.print(PIN[count]);
            count++ ;
                  if (count ==4){
                   lcd.clear();


    if ( PIN[0] == '1' && PIN[1] == '9'&& PIN[2] == '9' && PIN[3] == '1' )
        {
       lcd.print("Welcome");
       delay (100);
       lcd.clear();
         lcd.setCursor(1,0);
        lcd.print("ID 1");
        delay(500);
        code:
       lcd.clear();
       lcd.setCursor(0,0);
```

```
        lcd.print( " 1- Transaction ");
        lcd.setCursor(0,1);
        lcd.print (" 2- Deposit");
         lcd.setCursor(0,2);
        lcd.print( " 3- Balance ");
        lcd.setCursor(0,3);
        lcd.print(" 4- Transfer");
         delay(500);
         lcd.clear();
lcd.setCursor(0,0);
lcd.print(" 5- Exit");
int take= 0;
while (take<=1 ){
 char key = keypad.getKey();
if (key){
if(key !=NO_KEY ){
if (key=='1'){
op:
Serial1.println("");
Serial1.print("OTP is 1234");
Serial.println("");

lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Enter OTP");
count1=0;

while(new1<=1){
char key1 = keypad.getKey();
if (key1){
OTP[count1]=key1;
Serial.print(OTP[count1]);
count1++ ;
if (count1 ==4){
```

```
if ( OTP[0] == '1' && OTP[1] == '2'&& OTP[2] == '3' && OTP[3] == '4' )
{
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Enter Amount  ") ;
int j =0;
int k =0;
while (j<=1){
char key = keypad.getKey();
if (key) {
lcd.setCursor ( k ,1);
lcd.print(key);
k ++ ;
if (k==6){
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction in  ") ;
lcd.setCursor(0,1);
lcd.print( " Process.. ") ;
delay(700);
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction Done  ") ;
delay(1000);
goto code;
}
}
}
}
else {
  lcd.clear();
  lcd.print("OTP is wrong");
  delay(1000);
  goto op;
```

```
}

}
}
}
}
}
if (key!=NO_KEY){
if (key=='2'){
int allow=0;
lcd.clear();
lcd.setCursor(0,0);
lcd.print ( "Enter the amount" );
lcd.setCursor(0,1);
int b=0;
int a =0;
while (a<=1){
char key = keypad.getKey();
if (key){
lcd.setCursor ( b ,1);
lcd.print(key);
b ++ ;
if (b ==6){
lcd.clear();
lcd.print ("Done Deposit ");
delay(1000);
goto code;
}
}
}
}
}
if (key!=NO_KEY){
if (key=='3'){
```

```
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..");
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Your Balance is");
delay (200);
lcd.setCursor(0,1);
lcd.print(balance);
delay(1000);
goto code;
}
}
if (key!=NO_KEY){
if (key=='4'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..") ;
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Transfer done.");
delay (1000);
goto code;
}
}
if (key != NO_KEY){
if (key=='5'){
lcd.clear();
lcd.setCursor(0,0);
delay (100);
lcd.print("Take your card");
delay (1000);
```

```
lcd.clear();
goto back;
}
}



}
}
}
else{
    lcd.print(" Incorrect pin");
    delay(1000);
    lcd.clear();
    lcd.setCursor(0,0);
    count=0;
    count1=0;
    goto back;
    }
}
}
}
}


back1:
count=0;
if ( randn == 2 && s1 == 1 && s2 == 0 && s3 == 1 && s4 == 1 && s5 == 1 && s6
== 1){
lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Welcome ID 2");
  delay(180);
  lcd.clear();
    lcd.setCursor(0,0);
```

```
    lcd.print("Enter your pin");
    delay(100);
while(ask<=1){
    char key = keypad.getKey();
    if (key) {
            lcd.setCursor ( PIN[count],1);
            PIN[count]=key;
            lcd.print(PIN[count]);
            Serial.print(PIN[count]);
            count++ ;
                  if (count ==4){
                   lcd.clear();


    if ( PIN[0] == '1' && PIN[1] == '9'&& PIN[2] == '9' && PIN[3] == '1' )
        {
       lcd.print("Welcome");
       delay (100);
       lcd.clear();
        lcd.setCursor(1,0);
       lcd.print("ID 2");
       delay(500);

        code1:
       lcd.clear();
       lcd.setCursor(0,0);
       lcd.print( " 1- Transaction ");
       lcd.setCursor(0,1);
       lcd.print (" 2- Deposit");
        lcd.setCursor(0,2);
       lcd.print( " 3- Balance ");
       lcd.setCursor(0,3);
       lcd.print(" 4- Transfer");
        delay(500);
```

```
        lcd.clear();
lcd.setCursor(0,0);
lcd.print(" 5- Exit");
int take= 0;
while (take<=1 ){
 char key = keypad.getKey();
if (key){
if(key !=NO_KEY ){
if (key=='1'){
op1:
Serial1.println("");
Serial1.print("OTP is 1235");
Serial.println("");

lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Enter OTP");
count1=0;

while(new1<=1){
char key1 = keypad.getKey();
if (key1){
OTP[count1]=key1;
Serial.print(OTP[count1]);
count1++ ;
if (count1 ==4){
if ( OTP[0] == '1' && OTP[1] == '2'&& OTP[2] == '3' && OTP[3] == '5' )
{
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Enter Amount  ") ;
int j =0;
int k =0;
while (j<=1){
```

```
char key = keypad.getKey();
if (key) {
lcd.setCursor ( k ,1);
lcd.print(key);
k ++ ;
if (k==6){
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction in  ") ;
lcd.setCursor(0,1);
lcd.print( " Process.. ") ;
delay(700);
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction Done  ") ;
delay(1000);
goto code1;
}
}
}
}
else {
  lcd.clear();
  lcd.print("OTP is wrong");
  delay(1000);
  goto op1;
}

}
}
}
}
}
if (key!=NO_KEY){
```

```
if (key=='2'){
int allow=0;
lcd.clear();
lcd.setCursor(0,0);
lcd.print ( "Enter the amount" );
lcd.setCursor(0,1);
int b=0;
int a =0;
while (a<=1){
char key = keypad.getKey();
if (key){
lcd.setCursor ( b ,1);
lcd.print(key);
b ++ ;
if (b ==6){
lcd.clear();
lcd.print ("Done Deposit ");
delay(1000);
goto code1;
}
}
}
}
}
if (key!=NO_KEY){
if (key=='3'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..");
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Your Balance is");
delay (200);
```

```
lcd.setCursor(0,1);
lcd.print(balance);
delay(1000);
goto code1;
}
}
if (key!=NO_KEY){
if (key=='4'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..") ;
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Transfer done.");
delay (1000);
goto code1;
}
}
if (key != NO_KEY){
if (key=='5'){
lcd.clear();
lcd.setCursor(0,0);
delay (100);
lcd.print("Take your card");
delay (1000);
lcd.clear();
goto back1;
}
}



}
}
```

```
}
else{
    lcd.print(" Incorrect pin");
    delay(1000);
    lcd.clear();
    lcd.setCursor(0,0);
    count=0;
    count1=0;
    goto back1;
    }
}
}
}
}
back2:
count=0;
if ( randn == 3 && s1 == 1 && s2 == 1 && s3 == 0 && s4 == 1 && s5 == 1 && s6
== 1){
lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Welcome ID 3");
  delay(180);
  lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Enter your pin");
    delay(100);
while(ask<=1){
    char key = keypad.getKey();
    if (key) {
            lcd.setCursor ( PIN[count],1);
            PIN[count]=key;
            lcd.print(PIN[count]);
            Serial.print(PIN[count]);
            count++ ;
```

```
                    if (count ==4){
                     lcd.clear();


    if ( PIN[0] == '1' && PIN[1] == '9'&& PIN[2] == '9' && PIN[3] == '1' )
         {
        lcd.print("Welcome");
        delay (100);
        lcd.clear();
          lcd.setCursor(1,0);
         lcd.print("ID 3");
         delay(500);

         code2:
        lcd.clear();
        lcd.setCursor(0,0);
        lcd.print( " 1- Transaction ");
        lcd.setCursor(0,1);
        lcd.print (" 2- Deposit");
         lcd.setCursor(0,2);
        lcd.print( " 3- Balance ");
        lcd.setCursor(0,3);
        lcd.print(" 4- Transfer");
         delay(500);
         lcd.clear();
lcd.setCursor(0,0);
lcd.print(" 5- Exit");
int take= 0;
while (take<=1 ){
 char key = keypad.getKey();
if (key){
if(key !=NO_KEY ){
if (key=='1'){
op2:
```

```
Serial1.println("");
Serial1.print("OTP is 1236");
Serial.println("");

lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Enter OTP");
count1=0;

while(new1<=1){
char key1 = keypad.getKey();
if (key1){
OTP[count1]=key1;
Serial.print(OTP[count1]);
count1++ ;
if (count1 ==4){
if ( OTP[0] == '1' && OTP[1] == '2'&& OTP[2] == '3' && OTP[3] == '6' )
{
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Enter Amount  ") ;
int j =0;
int k =0;
while (j<=1){
char key = keypad.getKey();
if (key) {
lcd.setCursor ( k ,1);
lcd.print(key);
k ++ ;
if (k==6){
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction in  ") ;
lcd.setCursor(0,1);
```

```
lcd.print( " Process.. ") ;
delay(700);
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction Done  ") ;
delay(1000);
goto code2;
}
}
}
}
else {
  lcd.clear();
  lcd.print("OTP is wrong");
  delay(1000);
  goto op2;
}

}
}
}
}
}
if (key!=NO_KEY){
if (key=='2'){
int allow=0;
lcd.clear();
lcd.setCursor(0,0);
lcd.print ( "Enter the amount" );
lcd.setCursor(0,1);
int b=0;
int a =0;
while (a<=1){
char key = keypad.getKey();
```

```
if (key){
lcd.setCursor ( b ,1);
lcd.print(key);
b ++ ;
if (b ==6){
lcd.clear();
lcd.print ("Done Deposit ");
delay(1000);
goto code2;
}
}
}
}
}
if (key!=NO_KEY){
if (key=='3'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..");
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Your Balance is");
delay (200);
lcd.setCursor(0,1);
lcd.print(balance);
delay(1000);
goto code2;
}
}
if (key!=NO_KEY){
if (key=='4'){
lcd.clear();
lcd.setCursor(0,0);
```

```
lcd.print ("Please wait..") ;
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Transfer done.");
delay (1000);
goto code2;
}
}
if (key != NO_KEY){
if (key=='5'){
lcd.clear();
lcd.setCursor(0,0);
delay (100);
lcd.print("Take your card");
delay (1000);
lcd.clear();
goto back2;
}
}



}
}
}
else{
    lcd.print(" Incorrect pin");
    delay(1000);
    lcd.clear();
    lcd.setCursor(0,0);
    count=0;
    count1=0;
    goto back2;
    }
```

```
}
}
}
}
back3:
count=0;
if ( randn == 4 && s1 == 1 && s2 == 1 && s3 == 1 && s4 == 0 && s5 == 1 && s6
== 1){
lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Welcome ID 4");
  delay(180);
  lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Enter your pin");
    delay(100);
while(ask<=1){
    char key = keypad.getKey();
    if (key) {
            lcd.setCursor ( PIN[count],1);
            PIN[count]=key;
            lcd.print(PIN[count]);
            Serial.print(PIN[count]);
            count++ ;
                  if (count ==4){
                   lcd.clear();


    if ( PIN[0] == '1' && PIN[1] == '9'&& PIN[2] == '9' && PIN[3] == '1' )
        {
       lcd.print("Welcome");
       delay (100);
       lcd.clear();
         lcd.setCursor(1,0);
```

```
          lcd.print("ID 4");
          delay(500);

          code3:
         lcd.clear();
         lcd.setCursor(0,0);
         lcd.print( " 1- Transaction ");
         lcd.setCursor(0,1);
         lcd.print (" 2- Deposit");
          lcd.setCursor(0,2);
         lcd.print( " 3- Balance ");
         lcd.setCursor(0,3);
         lcd.print(" 4- Transfer");
          delay(500);
          lcd.clear();
lcd.setCursor(0,0);
lcd.print(" 5- Exit");
int take= 0;
while (take<=1 ){
 char key = keypad.getKey();
if (key){
if(key !=NO_KEY ){
if (key=='1'){
op3:
Serial1.println("");
Serial1.print("OTP is 1237");
Serial.println("");

lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Enter OTP");
count1=0;

while(new1<=1){
```

```
char key1 = keypad.getKey();
if (key1){
OTP[count1]=key1;
Serial.print(OTP[count1]);
count1++ ;
if (count1 ==4){
if ( OTP[0] == '1' && OTP[1] == '2'&& OTP[2] == '3' && OTP[3] == '7' )
{
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Enter Amount  ") ;
int j =0;
int k =0;
while (j<=1){
char key = keypad.getKey();
if (key) {
lcd.setCursor ( k ,1);
lcd.print(key);
k ++ ;
if (k==6){
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction in  ") ;
lcd.setCursor(0,1);
lcd.print( " Process.. ") ;
delay(700);
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction Done  ") ;
delay(1000);
goto code3;
}
}
}
```

```
}
else {
  lcd.clear();
  lcd.print("OTP is wrong");
  delay(1000);
  goto op3;
}

}
}
}
}
}
if (key!=NO_KEY){
if (key=='2'){
int allow=0;
lcd.clear();
lcd.setCursor(0,0);
lcd.print ( "Enter the amount" );
lcd.setCursor(0,1);
int b=0;
int a =0;
while (a<=1){
char key = keypad.getKey();
if (key){
lcd.setCursor ( b ,1);
lcd.print(key);
b ++ ;
if (b ==6){
lcd.clear();
lcd.print ("Done Deposit ");
delay(1000);
goto code3;
}
```

```
}
}
}
}
if (key!=NO_KEY){
if (key=='3'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..");
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Your Balance is");
delay (200);
lcd.setCursor(0,1);
lcd.print(balance);
delay(1000);
goto code3;
}
}
if (key!=NO_KEY){
if (key=='4'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..") ;
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Transfer done.");
delay (1000);
goto code3;
}
}
if (key != NO_KEY){
```

```
if (key=='5'){
lcd.clear();
lcd.setCursor(0,0);
delay (100);
lcd.print("Take your card");
delay (1000);
lcd.clear();
goto back3;
}
}



}
}
}
else{
    lcd.print(" Incorrect pin");
    delay(1000);
    lcd.clear();
    lcd.setCursor(0,0);
    count=0;
    count1=0;
    goto back3;
    }
}
}
}
}
back4:
count=0;
if ( randn == 5 && s1 == 1 && s2 == 1 && s3 == 1 && s4 == 1 && s5 == 0 && s6
== 1){
lcd.clear();
    lcd.setCursor(0,0);
```

```
    lcd.print("Welcome ID 5");
  delay(180);
  lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Enter your pin");
    delay(100);
while(ask<=1){
    char key = keypad.getKey();
    if (key) {
            lcd.setCursor ( PIN[count],1);
            PIN[count]=key;
            lcd.print(PIN[count]);
            Serial.print(PIN[count]);
            count++ ;
                  if (count ==4){
                   lcd.clear();


    if ( PIN[0] == '1' && PIN[1] == '9'&& PIN[2] == '9' && PIN[3] == '1' )
        {
       lcd.print("Welcome");
       delay (100);
       lcd.clear();
        lcd.setCursor(1,0);
       lcd.print("ID 5");
       delay(500);

        code4:
       lcd.clear();
       lcd.setCursor(0,0);
       lcd.print( " 1- Transaction ");
       lcd.setCursor(0,1);
       lcd.print (" 2- Deposit");
        lcd.setCursor(0,2);
```

```
        lcd.print( " 3- Balance ");
        lcd.setCursor(0,3);
        lcd.print(" 4- Transfer");
         delay(500);
         lcd.clear();
lcd.setCursor(0,0);
lcd.print(" 5- Exit");
int take= 0;
while (take<=1 ){
 char key = keypad.getKey();
if (key){
if(key !=NO_KEY ){
if (key=='1'){
op4:
Serial1.println("");
Serial1.print("OTP is 1238");
Serial.println("");

lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Enter OTP");
count1=0;

while(new1<=1){
char key1 = keypad.getKey();
if (key1){
OTP[count1]=key1;
Serial.print(OTP[count1]);
count1++ ;
if (count1 ==4){
if ( OTP[0] == '1' && OTP[1] == '2'&& OTP[2] == '3' && OTP[3] == '8' )
{
lcd.clear();
lcd.setCursor(0,0);
```

```
lcd.print( "Enter Amount  ") ;
int j =0;
int k =0;
while (j<=1){
char key = keypad.getKey();
if (key) {
lcd.setCursor ( k ,1);
lcd.print(key);
k ++ ;
if (k==6){
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction in  ") ;
lcd.setCursor(0,1);
lcd.print( " Process.. ") ;
delay(700);
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction Done  ") ;
delay(1000);
goto code4;
}
}
}
}
else {
  lcd.clear();
  lcd.print("OTP is wrong");
  delay(1000);
  goto op4;
}

}
}
```

```
}
}
}
if (key!=NO_KEY){
if (key=='2'){
int allow=0;
lcd.clear();
lcd.setCursor(0,0);
lcd.print ( "Enter the amount" );
lcd.setCursor(0,1);
int b=0;
int a =0;
while (a<=1){
char key = keypad.getKey();
if (key){
lcd.setCursor ( b ,1);
lcd.print(key);
b ++ ;
if (b ==6){
lcd.clear();
lcd.print ("Done Deposit ");
delay(1000);
goto code4;
}
}
}
}
}
if (key!=NO_KEY){
if (key=='3'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..");
delay (100);
```

```
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Your Balance is");
delay (200);
lcd.setCursor(0,1);
lcd.print(balance);
delay(1000);
goto code4;
}
}
if (key!=NO_KEY){
if (key=='4'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..") ;
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Transfer done.");
delay (1000);
goto code4;
}
}
if (key != NO_KEY){
if (key=='5'){
lcd.clear();
lcd.setCursor(0,0);
delay (100);
lcd.print("Take your card");
delay (1000);
lcd.clear();
goto back4;
}
}
```

```
}
}
}
else{
    lcd.print(" Incorrect pin");
    delay(1000);
    lcd.clear();
    lcd.setCursor(0,0);
    count=0;
    count1=0;
    goto back4;
    }
}
}
}
}
back5:
count=0;
if ( randn == 6 && s1 == 1 && s2 == 1 && s3 == 1 && s4 == 1 && s5 == 1 && s6
== 0){
lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Welcome ID 6");
  delay(180);
  lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Enter your pin");
    delay(100);
while(ask<=1){
    char key = keypad.getKey();
    if (key) {
            lcd.setCursor ( PIN[count],1);
```

```
            PIN[count]=key;
            lcd.print(PIN[count]);
            Serial.print(PIN[count]);
            count++ ;
                  if (count ==4){
                   lcd.clear();


    if ( PIN[0] == '1' && PIN[1] == '9'&& PIN[2] == '9' && PIN[3] == '1' )
        {
       lcd.print("Welcome");
       delay (100);
       lcd.clear();
        lcd.setCursor(1,0);
       lcd.print("ID 6");
       delay(500);

       code5:
       lcd.clear();
       lcd.setCursor(0,0);
       lcd.print( " 1- Transaction ");
       lcd.setCursor(0,1);
       lcd.print (" 2- Deposit");
        lcd.setCursor(0,2);
       lcd.print( " 3- Balance ");
       lcd.setCursor(0,3);
       lcd.print(" 4- Transfer");
        delay(500);
        lcd.clear();
lcd.setCursor(0,0);
lcd.print(" 5- Exit");
int take= 0;
while (take<=1 ){
 char key = keypad.getKey();
```

```
if (key){
if(key !=NO_KEY ){
if (key=='1'){
op5:
Serial1.println("");
Serial1.print("OTP is 1239");
Serial.println("");

lcd.clear();
lcd.setCursor(0,0);
lcd.print("Please Enter OTP");
count1=0;

while(new1<=1){
char key1 = keypad.getKey();
if (key1){
OTP[count1]=key1;
Serial.print(OTP[count1]);
count1++ ;
if (count1 ==4){
if ( OTP[0] == '1' && OTP[1] == '2'&& OTP[2] == '3' && OTP[3] == '9' )
{
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Enter Amount  ") ;
int j =0;
int k =0;
while (j<=1){
char key = keypad.getKey();
if (key) {
lcd.setCursor ( k ,1);
lcd.print(key);
k ++ ;
if (k==6){
```

```
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction in  ") ;
lcd.setCursor(0,1);
lcd.print( " Process.. ") ;
delay(700);
lcd.clear();
lcd.setCursor(0,0);
lcd.print( "Transaction Done  ") ;
delay(1000);
goto code5;
}
}
}
}
else {
  lcd.clear();
  lcd.print("OTP is wrong");
  delay(1000);
  goto op5;
}

}
}
}
}
}
if (key!=NO_KEY){
if (key=='2'){
int allow=0;
lcd.clear();
lcd.setCursor(0,0);
lcd.print ( "Enter the amount" );
lcd.setCursor(0,1);
```

```
int b=0;
int a =0;
while (a<=1){
char key = keypad.getKey();
if (key){
lcd.setCursor ( b ,1);
lcd.print(key);
b ++ ;
if (b ==6){
lcd.clear();
lcd.print ("Done Deposit ");
delay(1000);
goto code5;
}
}
}
}
}
if (key!=NO_KEY){
if (key=='3'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..");
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Your Balance is");
delay (200);
lcd.setCursor(0,1);
lcd.print(balance);
delay(1000);
goto code5;
}
}
```

```
if (key!=NO_KEY){
if (key=='4'){
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Please wait..") ;
delay (100);
lcd.clear();
lcd.setCursor(0,0);
lcd.print ("Transfer done.");
delay (1000);
goto code5;
}
}
if (key != NO_KEY){
if (key=='5'){
lcd.clear();
lcd.setCursor(0,0);
delay (100);
lcd.print("Take your card");
delay (1000);
lcd.clear();
goto back5;
}
}



}
}
}
else{
    lcd.print(" Incorrect pin");
    delay(1000);
    lcd.clear();
    lcd.setCursor(0,0);
```

```
    count=0;
    count1=0;
    goto back5;
    }
}
}
}
}
}
```