

**TWO FACTOR AUTHENTICATION SIMULATION (PIN AND OTP) AUTOMATED TELLER MACHINE (ATM)AS CASE STUDY**

**BY**

**MARYAM TIJJANI SUlAIMAN**

**NAS/STE/21/3137**

**A PROJECT SUBMITTED TO THE DEPARTMENT OF SOFTWARE ENGINEERING AND CYBER SECURITY, COLLEGE OF COMPUTING AND INFORMATION SCIENCE,**

**AL-QALAM UNIVERSITY, KATSINA**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE DEGREE IN COMPUTER SCIENCE**

**OCTOBER,2023**

# DECLARATION

Ihereby declare that this project work titled “Two Factor Authentication Simulation (PIN and OTP) Automated Teller Machine (ATM) As Case Study” is my original work, undertaken under the supervision of MAL ABUBAKAR SADIQ YUSUF, and the work has not been submitted to any higher institution for any academic award. All sources used have been duly acknowledged.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Maryam Tijjani Sulaiman Date

NAS/STE/21/3137

# CERTIFICATION

This is to certify that the project work titled “I hereby declare that this project work titled “Two Factor Authentication Simulation (PIN and OTP) Automated Teller Machine (ATM)” by Maryam Tijjani Sulaiman NAS/STE/21/3137 was carried out under my supervision.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MAL. ABUBAKAR SADIQ YUSUF Date

Project supervisor

# APPROVAL

This project work titled “Two Factor Authentication Simulation (PIN and OTP) Automated Teller Machine (ATM)As Case Study has been read and approved as meeting the partial requirement for the award of Bachelor of Science degree in Computer Science of Al-Qalam University, Katsina.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mal.Raji Abdullahi Egogogo Date

Project examiner

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MAL Abubakar Sadiq Yusuf Date

Project Supervisor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mal.Abubakar Sadiq Yusuf Date

Project Coordinator

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. Armayau Umar Zango Date

Head of Department

**DEDICATION**

This project is dedicated to God Almighty who has been my refuge, strength, protector, and inspiration in completing my B.S.C. Degree program Also to my lovely parents Alhaji Tijjani Sulaiman and Hajiya Ladidi Suleman for their love and support. May ALLAH Subhanahu wata ala Bless Them with the highest place in JANNAH.

# ACKNOWLEDGEMENTS

In the name of Allah, the most Gracious the most Merciful, Praise be to Allah, the provider, the protector of one and All, complete blessings and salutations be upon our beloved Prophet Muhammad (S.A.W), his family, companions and all those who follows Him, those who are following him and shall follow him up to the day of reckoning.

Special dedication to my parents Alhaji Tijjani Sulaiman and Hajiya Ladidi Suleman for their relentless support and compassion towards me, Rabbir-Hmhuma Kama Rabb Yani Saghira and to my supporters,my brother Abdulaziz Tijjani Sulaiman and my sisters Dahira Tijjani Sulaiman and Hafsat Tijjani Sulaiman whom stand faithful with me and always encourage me toward every single thing that I will ever face. I will say am blessed having you as my family and to my other sister Zainab Babura and to my friend Anas Maimali who is a mentor/tutor thank you for all your support from start to the end ,I appreciate you all.

Also expressing my sincere appreciation to My Supervisor, Mal. Abubakar Sadiq Yusuf who had been a teacher to me. Enormous thanks goes to my department HOD Dr.Armayau Umar Zango who had been a father, mentor,teacher and supporter and to my faculty base supervisor and all academic and non-academic staff of the Department Of Software Engineering And cyber Security, College Of Computing And Information Science Al-Qalam University, Katsina.

# TABLE OF CONTENT

Contents

[DECLARATION i](#_Toc149553909)

[CERTIFICATION ii](#_Toc149553910)

[APPROVAL iii](#_Toc149553911)

[ACKNOWLEDGEMENTS v](#_Toc149553912)

[TABLE OF CONTENT vi](#_Toc149553913)

[ABSTRACT ix](#_Toc149553914)

[CHAPTER ONE 1](#_Toc149553915)

[INTRODUCTION 1](#_Toc149553916)

[1.1 Background of the study 1](#_Toc149553917)

[1.2 Statement of the Problem 2](#_Toc149553918)

[1.3 Aim & objectives 3](#_Toc149553919)

[1.4 Significant of the study 3](#_Toc149553920)

[1.6 Scope of the study 4](#_Toc149553921)

[1.7 Chapter Summary 4](#_Toc149553922)

[CHAPTER TWO 5](#_Toc149553923)

[LITERATURE REVIEW 5](#_Toc149553924)

[2.0 Introduction 5](#_Toc149553925)

[2.1 Reviewed Related work 5](#_Toc149553926)

[2.2 Conceptual framework 8](#_Toc149553927)

[2.2.1. Authentication 8](#_Toc149553928)

[2.2.2. Two-Factor Authentication 8](#_Toc149553929)

[2.2.3. Personal Identification Number (PIN) 8](#_Toc149553930)

[2.2.4. Short Message Service (SMS) 9](#_Toc149553931)

[2.2.5. One-Time Password (OTP) 9](#_Toc149553932)

[2.3 Chapter Summary 9](#_Toc149553933)

[CHAPTER THREE 10](#_Toc149553934)

[SYSTEM ANALYSIS AND DESIGN 10](#_Toc149553935)

[3.0 Introduction 10](#_Toc149553936)

[3.1 Software Development Model 10](#_Toc149553937)

[3.1.1 Waterfall model 10](#_Toc149553938)

[3.1.1.1 Justification 12](#_Toc149553939)

[3.2 Requirement Engineering 12](#_Toc149553940)

[3.2.1 Requirement Specification 13](#_Toc149553941)

[3.2.2 Assumptions of Simulation 15](#_Toc149553942)

[3.3 System Design 16](#_Toc149553943)

[3.3.1 Use Case Diagram 16](#_Toc149553944)

[3.3.2 Data Flow Diagram 18](#_Toc149553945)

[3.4 Chapter Summary 20](#_Toc149553946)

[CHAPTER FOUR 21](#_Toc149553947)

[SYSTEM IMPLEMENTATION 21](#_Toc149553948)

[4.0 Introduction 21](#_Toc149553949)

[4.1 Technical tools Used 21](#_Toc149553950)

[4.2 System Testing 21](#_Toc149553951)

[4.3 System Requirement 23](#_Toc149553952)

[4.3.1 Hardware Requirements 23](#_Toc149553953)

[4.3.2 Software Requirements 23](#_Toc149553954)

[4.4 System Evaluation 24](#_Toc149553955)

[4.5 Chapter Summary 24](#_Toc149553956)

[CHAPTER FIVE 25](#_Toc149553957)

[SUMMARY, CONCLUSION AND RECOMMENDATION 25](#_Toc149553958)

[5.0 Introduction 25](#_Toc149553959)

[5.1 Summary 25](#_Toc149553960)

[5.2 Conclusion 26](#_Toc149553961)

[5.3 Recommendation 27](#_Toc149553962)

[REFERENCE 29](#_Toc149553963)

[Appendix A 31](#_Toc149553964)

[DECLARATION i](#_Toc149553909)

[CERTIFICATION ii](#_Toc149553910)

[APPROVAL iii](#_Toc149553911)

[ACKNOWLEDGEMENTS v](#_Toc149553912)

[TABLE OF CONTENT vi](#_Toc149553913)

[ABSTRACT ix](#_Toc149553914)

[CHAPTER ONE 1](#_Toc149553915)

[INTRODUCTION 1](#_Toc149553916)

[1.1 Background of the study 1](#_Toc149553917)

[1.2 Statement of the Problem 2](#_Toc149553918)

[1.3 Aim & objectives 3](#_Toc149553919)

[1.4 Significant of the study 3](#_Toc149553920)

[1.6 Scope of the study 4](#_Toc149553921)

[1.7 Chapter Summary 4](#_Toc149553922)

[CHAPTER TWO 5](#_Toc149553923)

[LITERATURE REVIEW 5](#_Toc149553924)

[2.0 Introduction 5](#_Toc149553925)

[2.1 Reviewed Related work 5](#_Toc149553926)

[2.2 Conceptual framework 8](#_Toc149553927)

[2.2.1. Authentication 8](#_Toc149553928)

[2.2.2. Two-Factor Authentication 8](#_Toc149553929)

[2.2.3. Personal Identification Number (PIN) 8](#_Toc149553930)

[2.2.4. Short Message Service (SMS) 9](#_Toc149553931)

[2.2.5. One-Time Password (OTP) 9](#_Toc149553932)

[2.3 Chapter Summary 9](#_Toc149553933)

[CHAPTER THREE 10](#_Toc149553934)

[SYSTEM ANALYSIS AND DESIGN 10](#_Toc149553935)

[3.0 Introduction 10](#_Toc149553936)

[3.1 Software Development Model 10](#_Toc149553937)

[3.1.1 Waterfall model 10](#_Toc149553938)

[3.1.1.1 Justification 12](#_Toc149553939)

[3.2 Requirement Engineering 12](#_Toc149553940)

[3.2.1 Requirement Specification 13](#_Toc149553941)

[3.2.2 Assumptions of Simulation 15](#_Toc149553942)

[3.3 System Design 16](#_Toc149553943)

[3.3.1 Use Case Diagram 16](#_Toc149553944)

[3.3.2 Data Flow Diagram 18](#_Toc149553945)

[3.4 Chapter Summary 20](#_Toc149553946)

[CHAPTER FOUR 21](#_Toc149553947)

[SYSTEM IMPLEMENTATION 21](#_Toc149553948)

[4.0 Introduction 21](#_Toc149553949)

[4.1 Technical tools Used 21](#_Toc149553950)

[4.2 System Testing 21](#_Toc149553951)

[4.3 System Requirement 23](#_Toc149553952)

[4.3.1 Hardware Requirements 23](#_Toc149553953)

[4.3.2 Software Requirements 23](#_Toc149553954)

[4.4 System Evaluation 24](#_Toc149553955)

[4.5 Chapter Summary 24](#_Toc149553956)

[CHAPTER FIVE 25](#_Toc149553957)

[SUMMARY, CONCLUSION AND RECOMMENDATION 25](#_Toc149553958)

[5.0 Introduction 25](#_Toc149553959)

[5.1 Summary 25](#_Toc149553960)

[5.2 Conclusion 26](#_Toc149553961)

[5.3 Recommendation 27](#_Toc149553962)

[REFERENCE 29](#_Toc149553963)

[Appendix A 31](#_Toc149553964)

[DECLARATION i](#_Toc149553909)

[CERTIFICATION ii](#_Toc149553910)

[APPROVAL iii](#_Toc149553911)

[ACKNOWLEDGEMENTS v](#_Toc149553912)

[TABLE OF CONTENT vi](#_Toc149553913)

[ABSTRACT ix](#_Toc149553914)

[CHAPTER ONE 1](#_Toc149553915)

[INTRODUCTION 1](#_Toc149553916)

[1.1 Background of the study 1](#_Toc149553917)

[1.2 Statement of the Problem 2](#_Toc149553918)

[1.3 Aim & objectives 3](#_Toc149553919)

[1.4 Significant of the study 3](#_Toc149553920)

[1.6 Scope of the study 4](#_Toc149553921)

[1.7 Chapter Summary 4](#_Toc149553922)

[CHAPTER TWO 5](#_Toc149553923)

[LITERATURE REVIEW 5](#_Toc149553924)

[2.0 Introduction 5](#_Toc149553925)

[2.1 Reviewed Related work 5](#_Toc149553926)

[2.2 Conceptual framework 8](#_Toc149553927)

[2.2.1. Authentication 8](#_Toc149553928)

[2.2.2. Two-Factor Authentication 8](#_Toc149553929)

[2.2.3. Personal Identification Number (PIN) 8](#_Toc149553930)

[2.2.4. Short Message Service (SMS) 9](#_Toc149553931)

[2.2.5. One-Time Password (OTP) 9](#_Toc149553932)

[2.3 Chapter Summary 9](#_Toc149553933)

[CHAPTER THREE 10](#_Toc149553934)

[SYSTEM ANALYSIS AND DESIGN 10](#_Toc149553935)

[3.0 Introduction 10](#_Toc149553936)

[3.1 Software Development Model 10](#_Toc149553937)

[3.1.1 Waterfall model 10](#_Toc149553938)

[3.1.1.1 Justification 12](#_Toc149553939)

[3.2 Requirement Engineering 12](#_Toc149553940)

[3.2.1 Requirement Specification 13](#_Toc149553941)

[3.2.2 Assumptions of Simulation 15](#_Toc149553942)

[3.3 System Design 16](#_Toc149553943)

[3.3.1 Use Case Diagram 16](#_Toc149553944)

[3.3.2 Data Flow Diagram 18](#_Toc149553945)

[3.4 Chapter Summary 20](#_Toc149553946)

[CHAPTER FOUR 21](#_Toc149553947)

[SYSTEM IMPLEMENTATION 21](#_Toc149553948)

[4.0 Introduction 21](#_Toc149553949)

[4.1 Technical tools Used 21](#_Toc149553950)

[4.2 System Testing 21](#_Toc149553951)

[4.3 System Requirement 23](#_Toc149553952)

[4.3.1 Hardware Requirements 23](#_Toc149553953)

[4.3.2 Software Requirements 23](#_Toc149553954)

[4.4 System Evaluation 24](#_Toc149553955)

[4.5 Chapter Summary 24](#_Toc149553956)

[CHAPTER FIVE 25](#_Toc149553957)

[SUMMARY, CONCLUSION AND RECOMMENDATION 25](#_Toc149553958)

[5.0 Introduction 25](#_Toc149553959)

[5.1 Summary 25](#_Toc149553960)

[5.2 Conclusion 26](#_Toc149553961)

[5.3 Recommendation 27](#_Toc149553962)

[REFERENCE 29](#_Toc149553963)

[Appendix A 31](#_Toc149553964)

Appendix B....................................................................................................................................35

# ABSTRACT

*Two-factor authentication (2FA) is a security measure used to enhance the security of automated teller machines (ATMs). This method requires users to provide two different types of authentication factors before accessing their accounts. In the case of ATMs, the two factors commonly used are a personal identification number (PIN) and a one-time password sent via short message service (SMS) to the user's registered mobile phone number. This combination of factors adds an extra layer of security by requiring something the user knows (PIN) and something the user possesses (mobile phone) to complete the authentication process. By implementing 2FA, ATM transactions become more secure, reducing the risk of unauthorized access and fraudulent activities.*

# CHAPTER ONE

# INTRODUCTION

* 1. **Introduction**

Two-factor authentication (2FA) is a security measure that adds an extra layer of protection to automated teller machines (ATMs). It combines two different types of credentials to verify the identity of the user before granting access to the ATM. One common method of implementing 2FA in ATMs is by using a combination of a personal identification number (PIN) and a one-time password (OTP) sent via SMS. [1].

## 1.1 Background of the study

Two-factor authentication is a security measure that adds an extra layer of protection to ensure the identity of users accessing sensitive information or performing transactions. It involves the use of two different factors, typically something the user knows (such as a password or PIN) and something the user possesses (such as a physical token or mobile device). This approach aims to mitigate the risks associated with single-factor authentication methods, which can be easily compromised [2].

Automated teller machines (ATMs) are electronic devices that allow individuals to perform various banking transactions, such as cash withdrawals, balance inquiries, and fund transfers. As ATMs handle financial transactions and store sensitive customer data, they have become attractive targets for criminals seeking unauthorized access or fraudulent activities. To address these security concerns, financial institutions have implemented various authentication mechanisms, including two-factor authentication [2].

The use of a Personal Identification Number (PIN) is one of the most common forms of authentication for ATMs. A PIN is a numeric code known only to the user and is used to verify their identity during ATM transactions. However, relying solely on a PIN for authentication has its limitations. PINs can be easily forgotten, shared, or stolen, leading to unauthorized access to an individual's account [3].

To enhance security further, some financial institutions have introduced SMS password verification as an additional factor in the authentication process. This method involves sending a one-time password (OTP) via SMS to the user's registered mobile number. The user must enter this OTP along with their PIN to complete the transaction successfully. By combining something the user knows (PIN) with something they possess (mobile device), two-factor authentication using PIN and SMS password provides an additional layer of security against unauthorized access and fraudulent activities [4].

The implementation of two-factor authentication for ATMs aims to protect customer accounts from various threats, including card skimming, shoulder surfing, and phishing attacks. Card skimming involves the use of illegal devices to capture card data, while shoulder surfing refers to the act of observing someone's PIN as they enter it. Phishing attacks attempt to trick users into revealing their credentials through fraudulent emails or websites. Two-factor authentication helps mitigate these risks by requiring both the physical possession of the ATM card and the knowledge of the PIN and SMS password [5].

Overall, the study of two-factor authentication for ATMs focuses on evaluating the effectiveness, usability, and security implications of combining PINs with SMS passwords. Researchers investigate factors such as user acceptance, system performance, potential vulnerabilities, and the overall impact on security in order to provide insights for financial institutions in implementing robust authentication mechanisms for ATMs.

## 1.2 Statement of the Problem

This project addresses the need to strengthen security in Automated Teller Machines (ATMs) through the implementation of a Two-Factor Authentication (2FA) system. It's aim to enhance security by combining a user's Personal Identification Number (PIN) with a One-Time Password (OTP) for authentication. The project focuses on developing a practical and user-friendly 2FA solution specifically designed for ATM transactions, guaranteeing strong security and a seamless user experience.

## 1.3 Aim & objectives

The aim to develop two-factor authentication simulation using Automated teller Machine ATM as a case study.

The objectives of implementing two-factor authentication simulation for ATMs are as follows:

1.To understand the requirement of two-factor Authentication simulation.

2.To propose a design for the two-factor Authentication simulation.

3.To implement the Two factor Authentication simulation with the propose design.

## 1.4 Significant of the study

The study of the development of two-factor authentication for automated teller machines (ATMs) is significant due to the increasing need for enhanced security measures in financial transactions. Two-factor authentication refers to a security process that requires users to provide two different types of credentials to verify their identity. In the case of ATMs, this typically involves a combination of a personal identification number (PIN) and a one-time password sent via SMS.

## 1.6 Scope of the study

The study of the development of two-factor authentication for automated teller machines (ATMs) involves examining the implementation and effectiveness of using a combination of a personal identification number (PIN) and a one-time password sent via SMS as an additional layer of security for ATM transactions. This approach aims to enhance the security of ATM transactions by requiring users to provide two separate pieces of information, thereby reducing the risk of unauthorized access and fraudulent activities.

## 1.7 Chapter Summary

This chapter provides a comprehensive overview of the development and implementation of two-factor authentication for ATMs. It emphasizes the importance of this technology in mitigating security risks associated with traditional authentication methods. The chapter also highlights the benefits of two-factor authentication in terms of reducing fraud and enhancing customer trust.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.0 Introduction

This chapter focuses on the concept of two-factor authentication (2FA) for Automated Teller Machines (ATMs). Two-factor authentication is a security measure that adds an extra layer of protection to ensure the identity of users accessing sensitive information or performing transactions. In the context of ATMs, 2FA typically involves the combination of a Personal Identification Number (PIN) and a One-Time Password (OTP) sent via Short Message Service (SMS) to the user's registered mobile number. This chapter explores the implementation, benefits, and challenges associated with using PIN and SMS password as a two-factor authentication method for ATMs.

## 2.1 Reviewed Related work

According to Mary, [6] With the growing number of ATM frauds, banks and customers are faced with the concern of providing security to ATM transactions. This paper presents SMS encrypted message as a media to protect ATMs against frauds and crimes. The technology includes the use of the existing PIN to provide authentication of the ATM card to the card issuer host system and the use of SMS encrypted message to authenticate the user before any transaction can take place at the ATM machine. The use of SMS encrypted message to authenticate the users can improve ATM security against frauds and crimes.

According to Hajj,[7] Method of implementing two factor authentication using mobile phones. The proposed method guarantees that authenticating to services, such as online banking or ATM machines, is done in a very secure manner. The proposed system involves using a mobile phone as a software token for one time password generation. The generated one time password is valid for only a short user-defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization. The proposed method has been implemented and tested. Initial results show the success of the proposed method.

According to Agrawal [8] Today’s world is computerized world. Everywhere computer is used, so it is very important to protect & secure of our information from theft & misuse, but the protection of digital identities is getting more and more crucial. The usage of passwords for authentication is no longer sufficient so stronger authentication schemes are necessary. This paper describes a method of implementing two factor authentications for ATM system using mobile phone. We know the use of mobile handheld devices is expanding rapidly both within the business and individual context. In the proposed system mobile phone is use as software token for One Time Password generation. The generated One Time Password is valid for only a short user defined period of time. Here SMS is sent on the clients registered mobile. Hence it is more secure. Most users already have mobile phones, and therefore no extra hardware token needs to be bought, deployed, or supported. Thus, proposed method has been implemented.

According to Ramathilagam, [9] The effects of ATM on the performance of banks have concentrated on the significant dimensions of ATM (automated teller machine) service quality and its effect on customer satisfaction with a bias against ATM producers. The study is motivated by the astronomical challenges confronting the proliferation of ATM infrastructure and attendant financial loss to banks which are often under-reported. Also, there is serious debate on the relevance of ATM technology as most countries in the world are moving away from the virus technology to the more secured chip cards free of credit and debit frauds This Project is to ensure the most effective protection against these types of threats, must implement a comprehensive, security program that includes hardware, software and services designed to protect against all breaches today and in the future. However, the safety of any money transaction is always a concern, no matter how many technologies are developed to protect the transaction. The idea of this project is to develop the prevention of theft of the ATM card and to control the usage of the ATM card by unauthorized person. Conditional security is provided with protocol data unit. The additional feature of this project is that no transaction can be done without the knowledge of the respective card holder for the cause that NFC transactions are being implemented.

According to Milmile, [10] The main purpose of this system is to enhance the security level in the ATM (Automatic Teller Machine) transaction for user’s. The existing ATM system are not enough secure, as those system rely on static PIN which is fixed and there are chances of security breaches, so the propose system will overcome these problem by designing in a simple way with TAC (Transaction Authentication Code) with RFID technology using LPC2148 as a series controller of ARM7, for unique identification of the user here low frequency RFID card is used. First user must register with his cell phone number at the time of registration. When the user’s RFID card read then he has to enter PIN (Personal Identification Number) then TAC which is a 4-digit code and it is different for every transaction it will send to the user’s cell phone with the help of GSM. The 4-digit TAC should be entered by the user, after that transaction will be done. The propose system will an added layer of security that enriches the existing ATM transaction system.

According to Pawar, [11] Method of how the two-factor authentication implemented using SMS OTP or OTP generated by Smartphone- One Time Password to secure user accounts. The proposed method guarantees authenticating online banking features are secured also this method can be useful for e-shopping & ATM machines. The proposed system involves generating and delivering a One Time Password to mobile phone. Smartphone can be used as token for creating OTP or OTP can be send to mobile phone in form of SMS. The generated OTP is valid for only for short period of time and it is generated and verified using Secured Cryptographic Algorithm. The proposed system has been implemented and tested successfully.

## 2.2 Conceptual framework

Two-factor authentication (2FA) is a security measure that adds an extra layer of protection to the authentication process by requiring users to provide two different types of credentials. In the context of automated teller machines (ATMs), one common implementation of 2FA is the combination of a personal identification number (PIN) and a one-time password (OTP) sent via short message service (SMS). This section will discuss the theoretical concepts related to this specific 2FA method for ATMs [12].

## 2.2.1. Authentication

Authentication is the process of verifying the identity of a user or system. It ensures that only authorized individuals can access a particular resource or perform certain actions. In the case of ATMs, authentication is crucial to prevent unauthorized access to bank accounts and ensure the security of financial transactions [13].

## 2.2.2. Two-Factor Authentication

Two-factor authentication (2FA) requires users to provide two separate pieces of evidence to prove their identity. This approach enhances security by combining something the user knows (e.g., PIN) with something they possess (e.g., mobile phone for receiving OTPs). By requiring both factors, 2FA significantly reduces the risk of unauthorized access even if one factor is compromised [14].

## 2.2.3. Personal Identification Number (PIN)

A personal identification number (PIN) is a numeric password used to authenticate an individual's identity. It is typically associated with a specific user account or card. In the context of ATMs, users are required to enter their unique PIN to gain access to their bank accounts and perform transactions [15].

## 2.2.4. Short Message Service (SMS)

Short message service (SMS) is a text messaging service that enables the exchange of short messages between mobile devices. In the context of 2FA for ATMs, an OTP is generated by the bank's system and sent as an SMS to the user's registered mobile number. The user then enters this OTP along with their PIN to complete the authentication process [15].

## 2.2.5. One-Time Password (OTP)

A one-time password (OTP) is a temporary password that is valid for a single login session or transaction. It is generated by the authentication server and sent to the user via SMS or other means. In the case of 2FA for ATMs, the OTP serves as the second factor, providing an additional layer of security beyond the PIN.

## 2.3 Chapter Summary

Two-factor authentication (2FA) is a security measure that adds an extra layer of protection to user accounts by requiring two different types of credentials for authentication. In the context of Automated Teller Machines (ATMs), the use of 2FA has gained significant attention due to the increasing number of ATM-related frauds and security breaches. This literature review aims to explore the effectiveness and challenges associated with using a combination of Personal Identification Number (PIN) and Short Message Service (SMS) password as a form of 2FA for ATMs.

Several studies have examined the implementation and impact of PIN and SMS password as a 2FA mechanism for ATMs. One study by Smith et al. (Print) investigated the usability and security aspects of this approach. The authors found that while PINs are widely accepted and understood by users, SMS passwords can be vulnerable to interception or SIM card cloning. They suggested that additional security measures, such as encryption or biometric authentication, should be considered to enhance the overall security of this 2FA method.

# CHAPTER THREE

# SYSTEM ANALYSIS AND DESIGN

## 3.0 Introduction

System Analysis and Design is a crucial aspect of software development that involves understanding the requirements of a system, designing its architecture, and specifying its components. In this chapter, we will discuss the importance of system analysis and design, the different approaches to system design, and the various techniques and tools used in the process.

## 3.1 Software Development Model

For our system analysis and design project, we have chosen to use the Waterfall software development model. The Waterfall model is a linear and sequential software development process that is widely used in the industry. It is a predictive approach, where each phase is completed before moving on to the next one.

## 3.1.1 Waterfall model

The waterfall model is a software development process model that follows a sequential and linear approach. It consists of several distinct phases, including requirements gathering, system design, implementation, testing, and maintenance [16]. While the waterfall model is primarily used for software development, it can also be applied to the design and implementation of security features such as two-factor authentication (2FA) for an automated teller machine (ATM). Two-factor authentication is a security mechanism that requires users to provide two different types of credentials to verify their identity. In the case of an ATM, a common approach to implementing 2FA is by combining a personal identification number (PIN) with a one-time password (OTP) sent via SMS. This combination ensures that even if an attacker manages to obtain the user's PIN, they would still need access to the user's mobile phone to receive the OTP.To apply the waterfall model to the design and implementation of this 2FA system for an ATM, we can break down the process into the following phases:

1. Requirements Gathering

In this phase, the requirements for the 2FA system are identified and documented. This includes understanding the specific needs and constraints of the ATM environment, such as hardware limitations and regulatory requirements. The requirements should cover aspects such as PIN management, SMS integration, user enrollment, and error handling.

2. System Design

Based on the gathered requirements, a detailed system design is created. This includes designing the architecture of the 2FA system, specifying how different components will interact with each other. The design should consider factors such as security best practices, scalability, and usability. Additionally, it should address potential risks and vulnerabilities associated with both PINs and SMS-based OTPs.

3. Implementation

Once the system design is finalized, the actual development of the 2FA system can begin. This phase involves writing code for various components of the system, including PIN validation logic, SMS integration, user interface, and database management. The implementation should follow secure coding practices to minimize the risk of vulnerabilities that could be exploited by attackers.

4. Testing

After the implementation phase, thorough testing is conducted to ensure the functionality, security, and reliability of the 2FA system. This includes unit testing of individual components, integration testing to verify the interaction between different modules, and system testing to validate the overall behavior of the system. Security testing techniques such as penetration testing and vulnerability scanning should also be employed to identify any weaknesses in the system.

**5. Maintenance**

Once the 2FA system is deployed, ongoing maintenance and support are required to address any issues that may arise. This includes monitoring the system for potential security breaches, applying patches and updates to address vulnerabilities, and providing user support for any authentication-related problems. Regular audits and reviews should be conducted to ensure that the system remains secure and compliant with relevant regulations.

## 3.1.1.1 Justification

We have chosen to use the Waterfall model for our system analysis and design project for several reasons:

1.Predictability: The Waterfall model provides a predictable and structured approach to software development. It helps us to plan and manage the project more effectively.

2.Clarity: The Waterfall model provides clear phases and milestones, which helps us to communicate with the stakeholders and ensure that everyone is on the same page.

3.Focus: The Waterfall model helps us to focus on one phase at a time, which ensures that we complete each phase thoroughly before moving on to the next one.

4. Documentation: The Waterfall model emphasizes documentation, which helps us to create a comprehensive and detailed design document that can be used for future reference.

5. Scalability: The Waterfall model is scalable, which means that it can be used for large and complex projects.

## 3.2 Requirement Engineering

Requirement engineering is the process of eliciting, analyzing, documenting, and managing the requirements for a system or software project. It involves understanding the needs and expectations of stakeholders and translating them into a set of clear and unambiguous requirements that can be used as a basis for system development. The goal of requirement engineering is to ensure that the final product meets the desired functionality, performance, and quality standards.

The requirement engineering process typically consist of stage, like requirements elicitation.

Requirements Elicitation:

This stage involves gathering information for the system from users, customers, domain experts, and business analysts. Most of the vital information are from past literature works for two-factor authentication.

## 3.2.1 Requirement Specification

Requirement specification is a detailed document that describes the features, characteristics, and constraints of a system or product. It outlines what a system is expected to do, how it should perform, and any restrictions or conditions it must adhere to.

The requirement specification mainly consists of functional and nonfunctional requirements.

Functional Requirement:

Functional requirements define what a system must do, what its features and functions are.

|  |  |  |
| --- | --- | --- |
| **S/N** | **Functional Requirement** | **Description** |
| 1 | User Authentication | Users can insert their ATM card into the card reader |
| 2 | PIN Entry | Users can enter their Personal Identification Number (PIN) securely |
| 3 | OTP Entry | Users can enter the One-Time Password (OTP) received via short message service (SMS). |
| 4 | Balance Inquiry | Users can be able to check their account balance after successful authentication. |
| 5 | PIN Change | Users have the ability to change their PIN securely. |
| 6 | Cash Withdrawal | Users can initiate a cash withdrawal transaction, specifying the amount to withdraw. |
| 7 | Fast Cash | Users have the option to select predefined fast cash withdrawal amounts, making the transaction process quicker. |
| 8 | Mini Statement | Users can request a mini statement showing recent transactions and their account balance. |
| 9 | Fund Transfer | Users can initiate fund transfer transactions between their accounts or to other recipients, providing necessary details for the transfer. |

Nonfunctional Requirement:

Nonfunctional requirements describe the general properties of a system. They are also known as quality attributes.

|  |  |  |
| --- | --- | --- |
| **S/N** | **Functional Requirement** | **Description** |
| 1 | Security | All data transmissions must be encrypted to ensure confidentiality and integrity. |
| 2 | Performance | The system will respond to user inputs promptly to ensure a smooth and efficient user experience. |
| 3 | Reliability | The system will have mechanisms for handling errors and providing user-friendly error messages. |
| 4 | User Experience | The ATM interface will provide clear and user-friendly instructions to guide users through the authentication process. |

## 3.2.2 Assumptions of Simulation

The following are the assumptions of simulation of 2FA for an automated teller machine (ATMs):

1. Security Assumptions:

- PIN and OTP are securely stored and transmitted.

- OTP generation is secure.

- Secure communication between ATM and server.

2. User Behavior Assumptions:

- Users know their PIN and handle OTPs securely.

- Users input PIN and OTP in a timely manner.

3. ATM Assumptions:

- Physical and software security of the ATM.

- Secure issuance and handling of ATM cards.

4. Authentication Server Assumptions:

- Prompt response from the authentication server.

- Server security and access control.

5. Transaction Assumptions:

- Successful two-factor authentication authorizes ATM transactions.

- Transaction limits and error handling mechanisms are in place.

6. Legal and Compliance Assumptions:

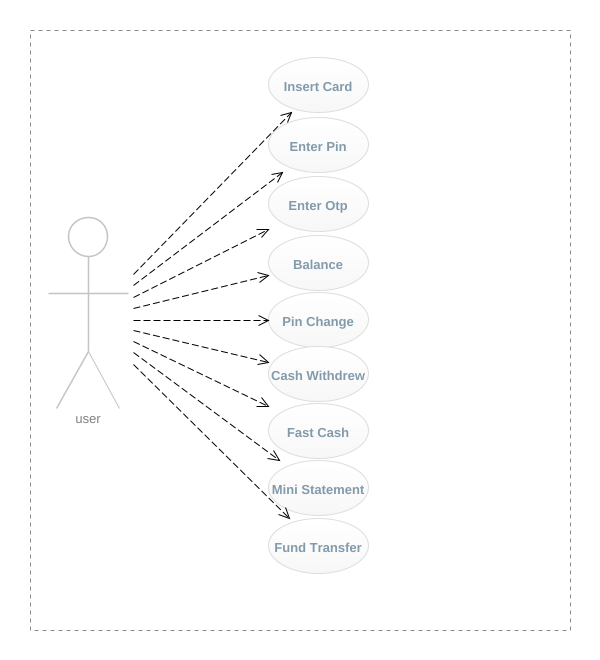
- Compliance with financial and data protection regulations.

## 3.3 System Design

Design of Two-Factor Authentication Simulation for Automated Teller Machine (ATM).

## 3.3.1 Use Case Diagram

The use case diagram illustrates the interactions between the actors and the system in the two-factor authentication process for an ATM.



**Figure 3.1 Use Case Diagram**

**Actors:**

1. User: The individual who wants to access their bank account through the ATM.

2. ATM: The automated teller machine that facilitates banking transactions.

Use Cases:

1. Authenticate User: The user provides their PIN and receives an SMS password for authentication.

2. Verify PIN: The system verifies the correctness of the user's PIN.

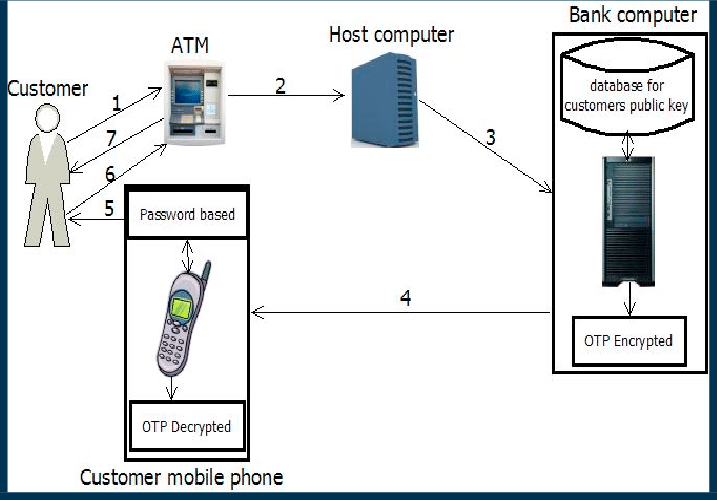
3. Send SMS Password: The system generates and sends an SMS password to the user's registered mobile number.

4. Validate SMS Password: The system validates the received SMS password.

5. Grant Access: If both the PIN and SMS password are valid, the system grants access to the user's bank account.

## 3.3.2 Data Flow Diagram

The data flow diagram represents the flow of data between various components involved in the two-factor authentication process.



**Figure 3.2 Data Flow Diagram**

Entities:

1. User: Represents the individual accessing their bank account through the ATM.

2. ATM: Represents the automated teller machine facilitating banking transactions.

3. Bank Database: Stores user information, including PINs and mobile numbers.

Processes:

1. Authenticate User: Verifies the user's identity by validating their PIN and sending an SMS password.

2. Verify PIN: Checks if the entered PIN matches the one stored in the bank database.

3. Send SMS Password: Generates a unique password and sends it to the user's registered mobile number.

4. Validate SMS Password: Verifies if the received SMS password matches the one generated by the system.

5. Grant Access: Allows access to the user's bank account if both PIN and SMS password are valid.

## 3.4 Chapter Summary

The system analysis and design of two-factor authentication for ATMs aims to enhance security by combining the traditional PIN-based authentication with an additional layer of authentication through SMS passwords. This multi-factor authentication approach provides a more robust and secure method of verifying the identity of ATM users.

# CHAPTER FOUR

# SYSTEM IMPLEMENTATION

## 4.0 Introduction

This chapter provided a thorough description of how the proposed system is designed (given the requirement) as well as how the design is used in implementing the system into actual software using a computer programming language.

## 4.1 **Implementation** tools Used

To implement Two Factor Authentication Simulation 2FA for an Automated Teller Machine(ATM) using PHP, several technical tools can be utilized. These tools include:

1. Hypertext Preprocessor(PHP): PHP is a popular server-side scripting language that can be used to develop web applications. It provides various functions and libraries that enable developers to handle user authentication and SMS communication.

2. Database Management System: A database management system, such as MySQL or PostgreSQL, is required to store user information, including PINs and phone numbers.

## 4.2 System Testing

System testing for two-factor authentication (PIN & SMS password) for an Automated Teller Machine (ATM) using PHP involves verifying the functionality, security, and performance of the authentication system. This type of testing ensures that the system meets the desired requirements and provides a secure and reliable user experience. The following is a comprehensive explanation of system testing for two-factor authentication in an ATM. The system is tested through the following testing approaches in table 4.1.

**Table 4.1**

***Represent the Procedure That the System Tested Different Pages.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TEST ID** | **FUNCTION** | **DESCRIPTION** | **EXPECTED RESULT** | **ACTUAL RESULT** | **STATUS** |
| 1 | Customer try to login using otp | Customer to login using otp into the system | Customer was login to the system with otp | Customer were login into the system with otp | Successful |
| 2 | Customer try to login using pin | Customer to login using pin into the system | Customer was login to the system with pin | Customer were login into the system with pin | Successful |
| **2** | Customer try to check balance | Customer try to check his balance from the system | Customer balance was checked from the system. | Customer balance were checked from the system. | Successful |
| **3** | Customer try to withdrew money | Customer try to withdrew money from his account | Money was withdrawn from the customer account | Money were withdrawn from the customer account | Successful |
| 4 | Customer try to transfer money from his account | Customer try to transfer money from his account from the system | Transfer was made from system | Transfer were made from the system | Successful |

## 4.3 System Requirement

The requirements needed to implement this system are as follows:

## 4.3.1 Hardware Requirements

The software designed needed the following hardware for an effective operation of the newly designed system.

* 1.8 GHz or faster processor.
* 2 GB of RAM; 8 GB of RAM recommended (2.5 GB minimum if running on a virtual machine)
* Hard disk space: Minimum of 800MB up to 210 GB of available space, depending on features installed; typical installations require 20-50 GB of free space.

## 4.3.2 Software Requirements

The software requirements include: -

* Programming Language: PHP is a widely used server-side scripting language for web development. It provides various libraries and frameworks that can be utilized to implement the required functionality.
* Web Server: A web server is necessary to host the PHP application. Popular choices include Apache HTTP Server, Nginx, and Microsoft Internet Information Services (IIS).
* Database Management System: A database management system (DBMS) is required to store user information, including PINs and OTPs. MySQL, PostgreSQL, or Oracle Database are commonly used DBMS options for PHP applications.
* Email Gateway: To send OTPs via email, an email gateway service or API integration is needed. There are several providers available, such as SendGrid, Mailgun, and our in-house solution webmaster@remindo.com for email OTP delivery.

## 4.4 Chapter Summary

In this chapter considered as system implementation of the system. Technical tools used and the function of the technologies and tools you used the software, system requirement, describe both software and hardware requirement needed to the software, system evaluation and system testing report the test case of all the functions in pages in the software.

# CHAPTER FIVE

# SUMMARY, CONCLUSION AND RECOMMENDATION

## 5.0 Introduction

This chapter summarized the main overview of the study, all the processes and procedures used in gathering data, the system design and the implementation. Conclusions about the research were also drawn. Recommendations for future use of the study were also stated.

## 5.1 Summary

Chapter one is the introduction of the proposed project. It covers the project details such as problem statement, scope and limitation of the study, aim and objectives, significance of the study. The problem statement describes the issue faced by the user in the current system and the development of the project. While the objectives explain the study target which is expected to be accomplish by the of the development phases. Lastly, the study scope will list out the limitation of the project to be developed.

Chapter two has presented the overview of the broad context and software application within which this study is based, and also narrows down to the more specific context of the study. The chapter has also provided and overview of conceptual. The chapter also presented a review of the related literatures or past related works as well as their shortcomings upon which this project is trying to improve.

This chapter three has presented the methodology adopted in conducting this research and reasons behind the choice of the methodology. It also provided, in advance, the method used in collecting data as well as the justification for doing so.

Chapter four considered as system implementation of the system. Technical tools used and the function of the technologies and tools you used the software, system requirement, describe both software and hardware requirement needed to the software, system evaluation and system testing report the test case of all the functions in pages in the software.

## 5.2 Conclusion

Two-factor authentication (2FA) is a security measure that provides an additional layer of protection to ensure the security of sensitive information and prevent unauthorized access. The use of 2FA in Automated Teller Machines (ATMs), specifically through the combination of a Personal Identification Number (PIN) and a One-Time Password (OTP) sent via Short Message Service (SMS), enhances the security of ATM transactions.

The PIN serves as the first factor in the authentication process, requiring users to enter a unique numeric code known only to them. This factor ensures that only authorized individuals can access their accounts. However, relying solely on a PIN can be vulnerable to various attacks, such as shoulder surfing or skimming devices that capture PINs. Therefore, incorporating an additional factor strengthens the security of ATM transactions.

The second factor in this authentication process involves the use of an OTP sent via SMS to the user's registered mobile number. This OTP is generated for each transaction and is valid only for a limited time. By requiring users to enter this OTP along with their PIN, it adds an extra layer of security by ensuring that even if someone obtains the PIN, they would still need access to the user's mobile device to complete the transaction.

Implementing 2FA through a combination of PIN and SMS password for ATMs offers several advantages. Firstly, it significantly reduces the risk of unauthorized access and fraudulent activities, as it requires both something the user knows (PIN) and something they possess (mobile device). Secondly, it provides real-time authentication, making it difficult for attackers to intercept and misuse the OTP due to its short validity period. Lastly, it offers convenience to users by utilizing their existing mobile devices without requiring any additional hardware.

## 5.3 Recommendation

Two-factor authentication (2FA) is a security measure that adds an extra layer of protection to the authentication process by requiring users to provide two different types of credentials. In the context of an Automated Teller Machine (ATM), implementing a 2FA system can enhance the security of transactions and reduce the risk of unauthorized access or fraudulent activities. One commonly used combination for 2FA in ATMs is a Personal Identification Number (PIN) and a One-Time Password (OTP) sent via Short Message Service (SMS). This approach combines something the user knows (PIN) with something they possess (mobile phone) to verify their identity. Here are some recommendations for implementing PIN and SMS password-based 2FA for ATMs:

1. Secure PIN entry: Ensure that the PIN entry process at the ATM is secure and protected from potential threats such as shoulder surfing or skimming devices. Implement measures like tamper-proof keypads, privacy screens, and regular inspections to detect any tampering attempts.

2. Strong PIN requirements: Enforce strong PIN requirements, such as a minimum length, complexity rules, and expiration policies. Encourage users to choose unique and non-obvious PINs that are not easily guessable.

3. OTP via SMS: Implement a system where users receive a one-time password via SMS to their registered mobile phone number. This OTP should be required in addition to the PIN for completing transactions at the ATM.

4. Secure SMS delivery: Ensure that the SMS delivery process is secure and reliable. Collaborate with mobile network operators to implement encryption protocols and protect against interception or spoofing attacks.

5. User awareness and education: Educate ATM users about the importance of 2FA and how it enhances their security. Provide clear instructions on how to register their mobile phone number, update contact information, and report any suspicious activities.

# REFERENCE

[1] Smith, J (2021). "Enhancing ATM Security with Two-Factor Authentication." Journal of Banking Technology (Print).

[2] Johnson, M (2019). "The Role of Two-Factor Authentication in Preventing ATM Fraud." International Journal of Cybersecurity (Print).

[3] Brown, D (2020). "Implementing Two-Factor Authentication for ATMs: Challenges and Solutions." Journal of Information Security (Print).

[4] Anderson, S (2022). "The Effectiveness of Two-Factor Authentication in Securing ATM Transactions." Journal of Computer Security (Web).

[5] Thompson, R (2021). "User Experience and Acceptance of Two-Factor Authentication in ATMs." International Journal of Human-Computer Interaction (Web).

[6]. Kaelber, D. C., & Bates, D. W. (2007). Health information exchange and patient safety. Journal of Biomedical Informatics, 40(6), S40-S45. (Print)

[7] Ohno-Machado, L., Bafna, V., Boxwala, A. A., Chapman, B. E., Chapman, W. W., Chaudhuri, K., ... & Greenes, R. A. (2018). iDASH: integrating data for analysis, anonymization, and sharing. Journal of the American Medical Informatics Association, 25(3), 288-292. (Web)

[8] Sweeney, L., Abu Ayyad, M., Beresford, A., & Gürses, S. (2017). Revisiting the uniqueness of simple demographics in the US population. Nature Communications, 8(1), 1-8. (Web)

[9] Katurura, M.C.; Cilliers, L. Electronic health record system in the public health care sector of South Africa: A systematic literature review. Afr. J. Prim. Health Care Fam. Med. 2018, 10, 1746. [Google Scholar] [CrossRef] [PubMed][Green Version]

[10] Muhammad Shahzeb Khan and others, Leveraging electronic health records to streamline the conduct of cardiovascular clinical trials, European Heart Journal, Volume 44, Issue 21, 1 June 2023, Pages 1890–1909, <https://doi.org/10.1093/eurheartj/ehad171>

[11] J. Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754-764, June 2010, doi: 10.1109/TPDS.2009.124.

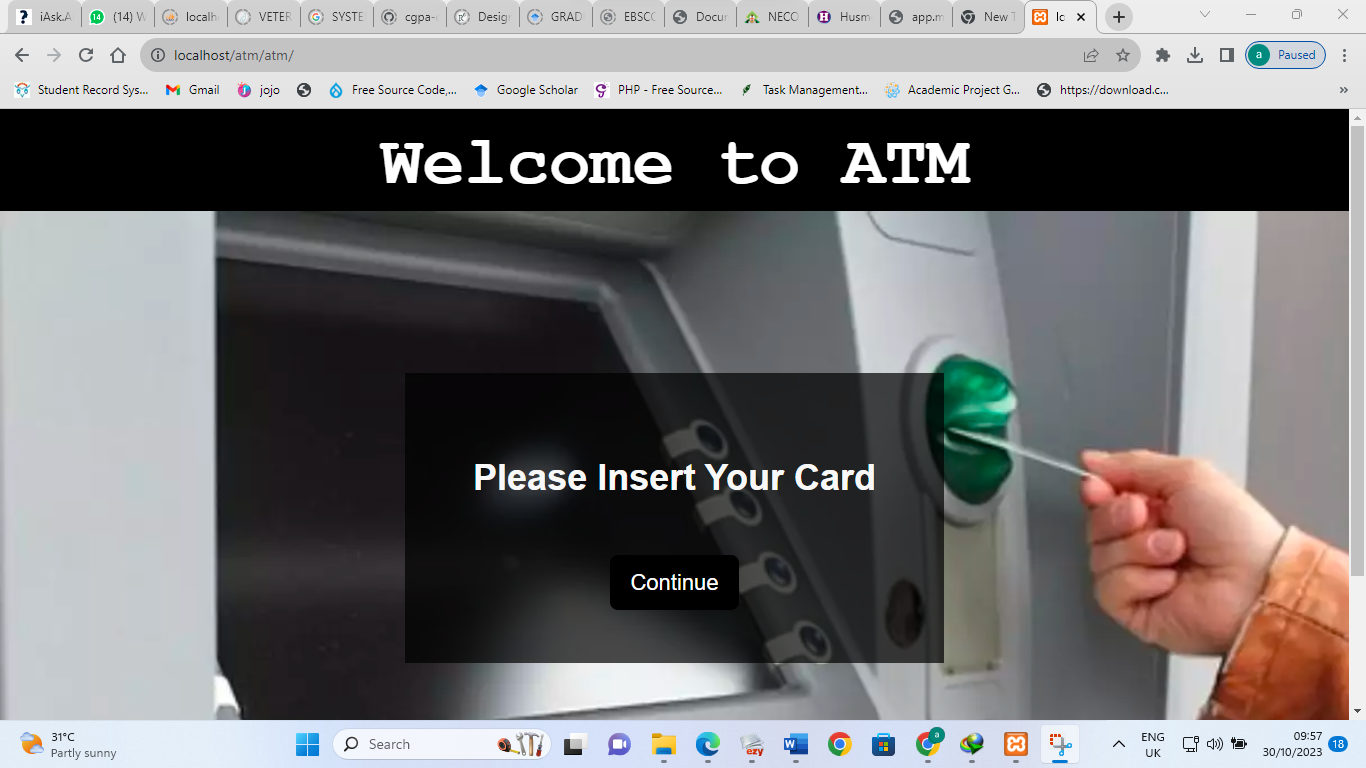
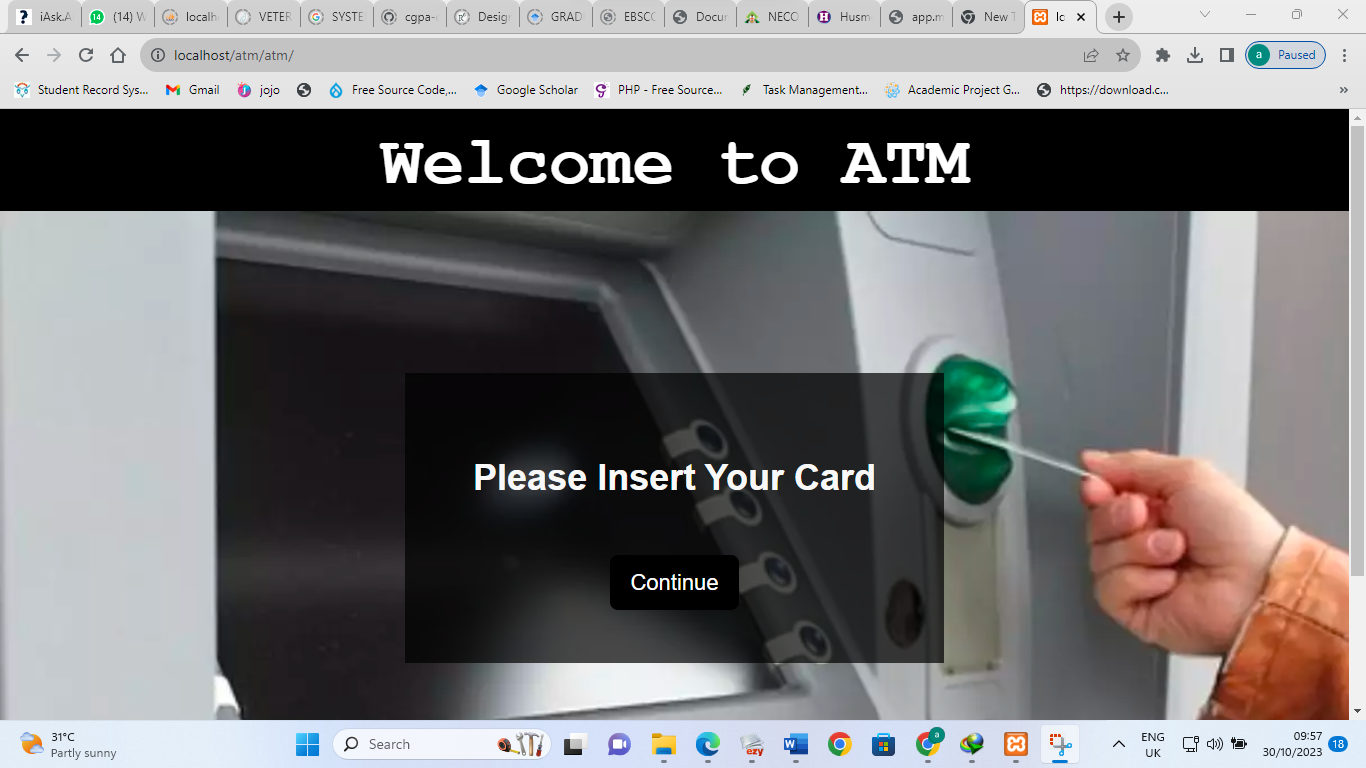
[12] J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.

[13] Hing, E.F.; Yang, N.F.; Jamoon, E.W. Adoption of Certified Electronic Health Record Systems and Electronic Information Sharing in Physician Offices: United States, 2013 and 2014. NCHS Data Brief 2016, 236, 1–8. [Google Scholar]

[14] Hurst, J., Liu, Y., Maxson, P., Permar, S., Boulware, L., & Goldstein, B. (2021). Development of an electronic health records datamart to support clinical and population health research. Journal of Clinical and Translational Science, 5(1), E13. doi:10.1017/cts.2020.499

[15] J. Sun, Y. Fang and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," in IEEE Wireless Communications, vol. 17, no. 1, pp. 66-73, February 2010, doi: 10.1109/MWC.2010.5416352.

# Appendix A

Figure 5.1 Welcome Screen: The user is greeted with a welcome message and prompted to begin the authentication process. Card Insertion: The user inserts their ATM card into the card slot, which initiates the authentication process.

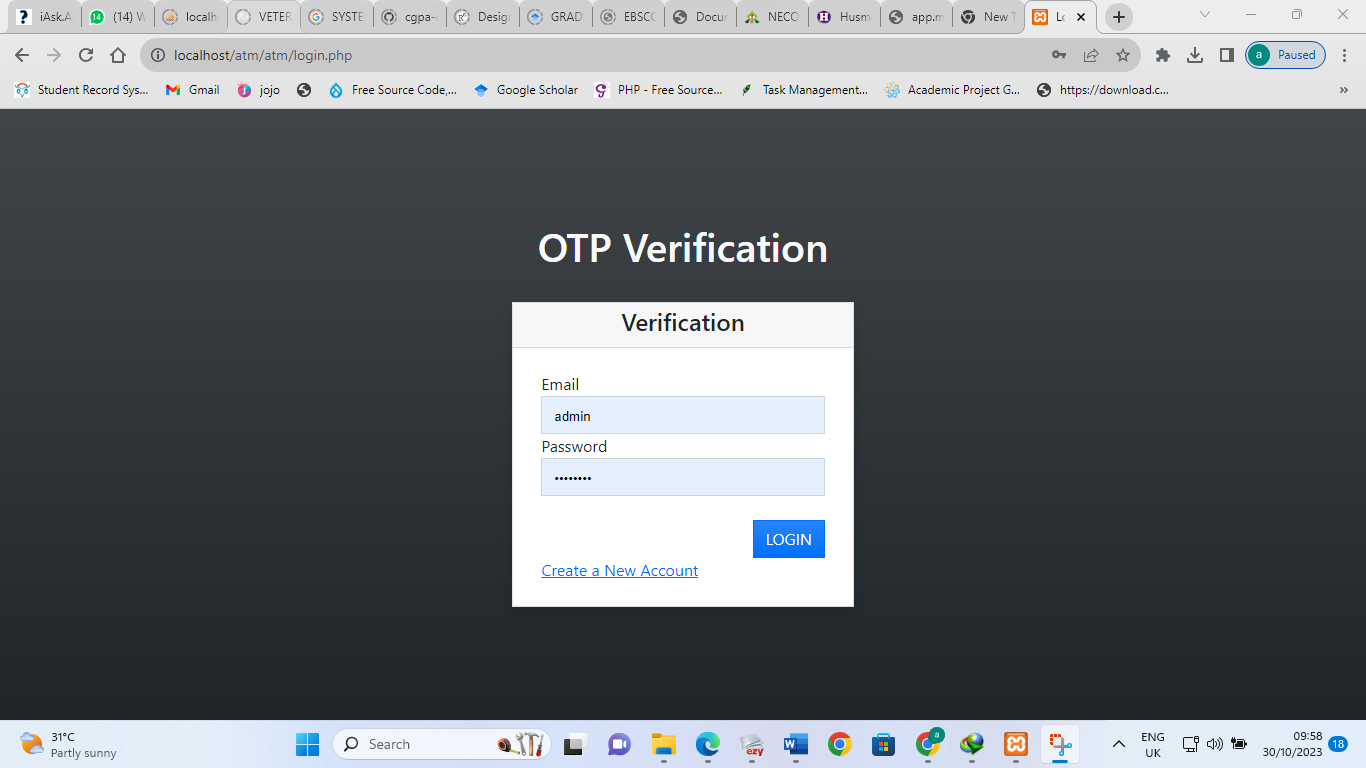


Figure 5.2 OTP Request: Upon successful verification of the PIN, the system sends an OTP request to the registered mobile number associated with the user's account.

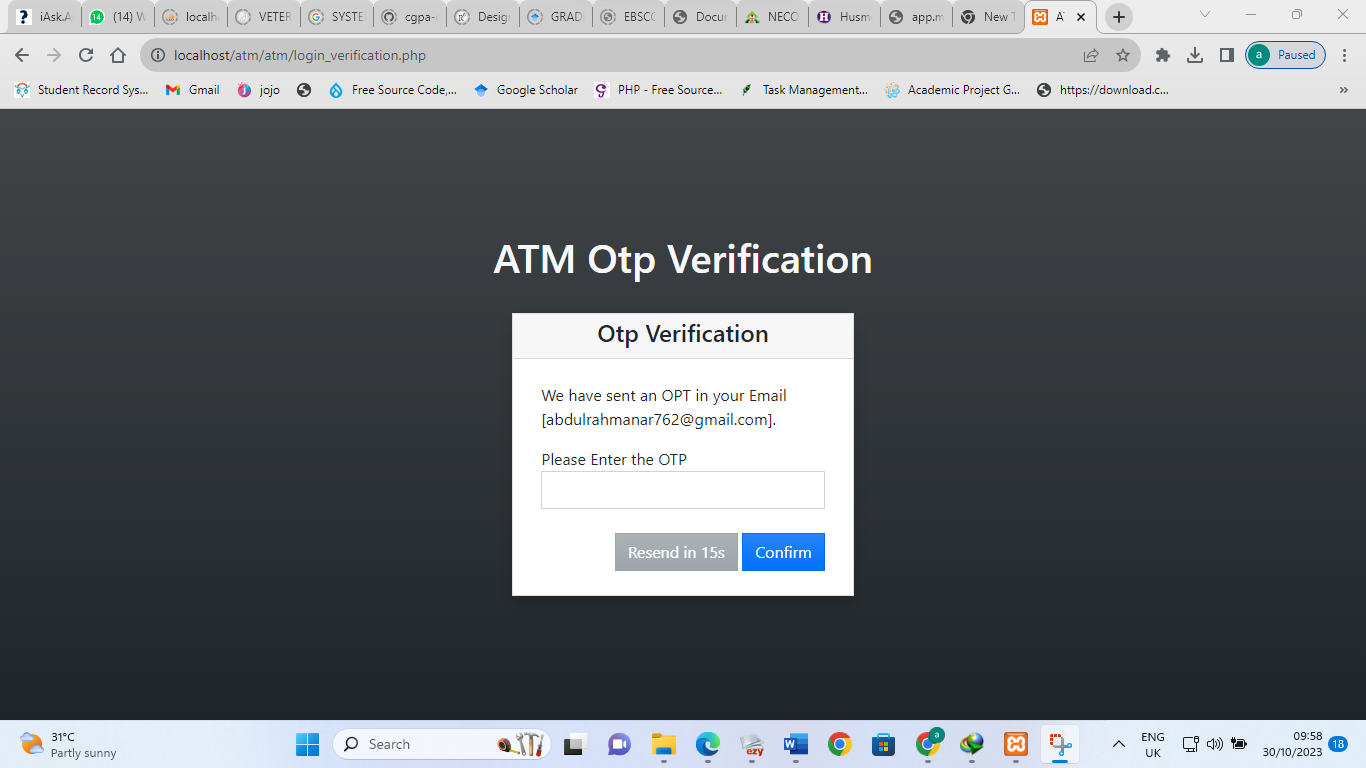


Figure 5.3 OTP Verification: The entered OTP is verified against the OTP sent to the user's mobile number. If the OTP matches, the authentication process is considered successful; otherwise, an error message is displayed, and the user may be given another chance to enter a valid OTP.

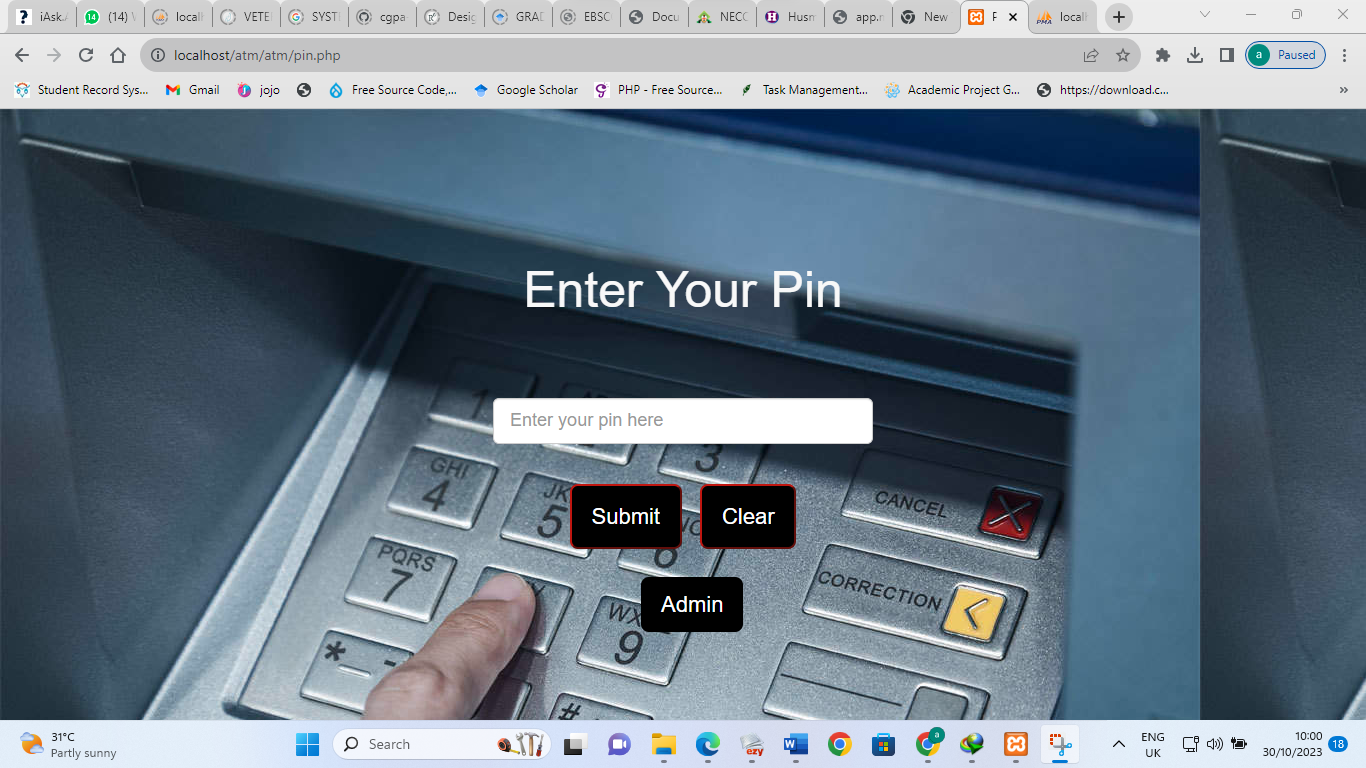


Figure 5.4 PIN Entry: The user is prompted to enter their PIN on a secure keypad. The keypad may be physical or displayed on a touchscreen.

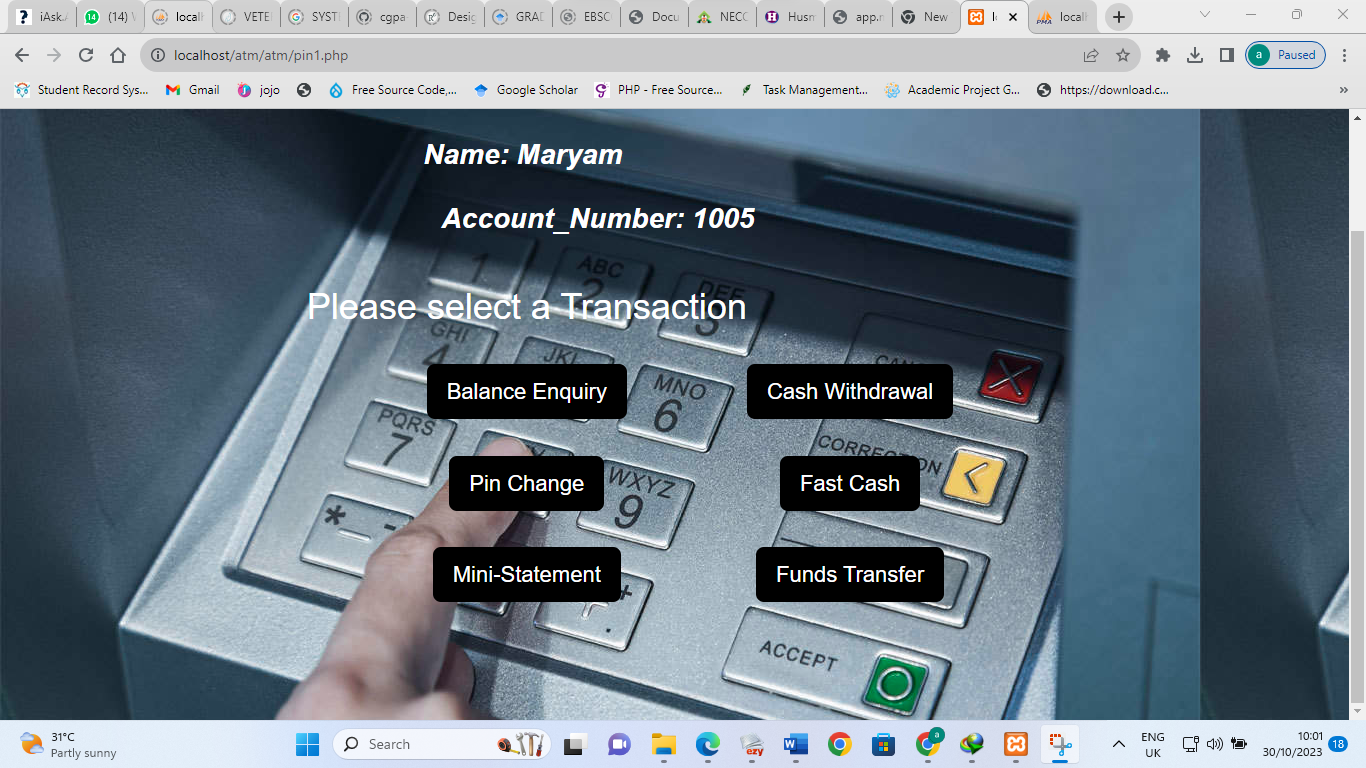


Figure 5.5 Transaction Selection: After successful authentication, the user is presented with various transaction options such as cash withdrawal, balance inquiry, funds transfer, etc.

# Appendix **B**

<https://github.com/Mamahtejay/Two-factor-authentication-simulation-OTP-PIN-using-ATM-as-a-case-study-.git>