https://dx.doi.org/10.4314/dujopas.v10i2b.2
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 10 No. 2b June 2024*

Embedded Communication System for Monitoring and Authenticating Transactions via Proxy on Automatic Teller Machine (ATM)

[1]Ibilade Abdurrasaq Ibiyemi, [2] Haruna Musa, [3] Jelilat Olusola Yusuf

[1]Department of Computer Science,
Faculty of Computing,
Federal University Dutse

[2]Department of Mechatronics Engineering,
Faculty of Engineering,
Bayero University,
Kano.

[3]Teaching and Learning Technologies Unit,
ICT Directorates,
Federal University Dutse

Email: ibiladeai@fud.edu.ng

Abstract

This paper reports the development of a secured system which allows the registered customer of a bank to monitor and authorize transaction via proxy on ATM. The system utilizes Atmel AVR microcontroller and communication modem as its controlling device. Microsoft Windows 8 was used as an operating system platform in the host PC for the implementation phase, with Object oriented C programming language in Microsoft Visual Studio 2013 being the front end development and MSSQL server 2012 as back end. A Bank customer's cell phone is used as a token for withdrawal transaction to be made in the account. Transaction could be made without disclosing personal identification number (PIN) to the nominee because the account owner authorizes the machine by sending the PIN and the amount to be withdrawn through his phone even in a remote area as far as there is a communication network. The application evaluation of the system was based on security of user PIN for transaction via proxy, ability of account or debit card owner to validate transaction on the ATM in absentia and average authentication time in comparison to the maximum authentication time allowed on the system. The ability to recognize user's phone number shows the security and reliability of the proposed system for ATM users' authentication. Results also showed that for a successful transaction, the proposed system allowed an average transaction time of 47.58 seconds through SMS.

Keywords: Proxy, Cell Phone, PIN, Authorization, Authentication Time.

INTRODUCTION

The existing self-banking system has got very high popularity with 24 hours service. Since the introduction and adoption of ATM, customers have enjoyed easy access to cash even outside conventional banking hours. But this system is sometimes not safe to use because anybody

Author for Correspondence

can access the system if they have the card and PIN, people share card and PIN to friends and relatives in order to help them make transaction when they are busy or could not access the machine. Furthermore, once a card and password (PIN) are stolen by a culprit, money can be withdrawn from the account in shortest period, which may bring huge financial losses to the users (Century Savings Bank, 2014). However, the transaction by proxy being carried out on the existing machine is at bank account owner's risk because the financial institutions has advised that card owners should protect their smart cards and PIN from third party. The ATM fraud is not a sole problem of banks alone; it is a big threat that requires coordinated and cooperative action on the part of the bank, customers and the law enforcement agencies (Adelowo and Mohammed, 2010). Smartcard theft, skimming devices and PIN fraud such as shoulder surfing, utilizing of fake PIN pad overlay, PIN interception are outlined as the major techniques used for perpetrating frauds on ATMs (Diebold Corporation, 2012).
The objectives of this research are as follows:

1. To develop a bank database (backend) to accommodate and match the main client's account records with its cellular phone number.
2. To design and implement an embedded system to fetch information from the backend and provide communication to the modeled ATM GUI (frontend).
3. To design an embedded system for generating and transmitting of SMS through communication channel to client's phone number and receiving feedback (reply) via the same channel from the client's phone.
4. To validate and evaluate the system reliability for user's authentication.

A lot of notable works done to ameliorate the security level on ATM are reviewed and discussed as follows;

Conventional ATM Transactions Security
In this category of transactions security, research methods proposed through various technologies for preventing major frauds mentioned in Diebold Corporation (2012) are discussed as follows. To prevent the major techniques used for perpetrating frauds on ATMs, fingerprint module, one time password (OTP) and personal identification number(PIN) were developed and incorporated in the proposed ATM system (Frimpong and Asante, 2016; Okafor, 2015; Khatmode et al., 2014).

Frimpong and Asante (2016) argued that in the absence of robust personal recognition schemes, ATMs are vulnerable to the deceits of an imposter. The system has suffered a lot over the years against PIN theft and other associated ATM frauds due to its traditional authentication mode (PIN). Okafor (2015) presented the design of ATM software using object oriented analysis and design (OOAD) with unified modelling language (UML) as its methodology. A system that employs a two factor authentication method was developed utilizing PIN and OTP which will be sent to the client's mobile phone through SMS. It was claimed that if the technique is deployed, a fraudster who has access to someone's ATM card and PIN will still not gain access to their bank account if there is no access to the SMS containing the OTP. In another approach by Jayasudha (2014) RFID chip and microcontroller were employed. RFID tag/reader is embedded along with user's mobile phone and ATM respectively. In the proposed system, services are read by sensing emitted signal from RFID tag enclosed in user mobile phone. PIC microcontroller was used for the application. The amount to be withdrawn is sent as message from mobile phone, it must match the amount entered in ATM or else transaction will not proceed. The research technique provides RFID

as alternative to ATM smartcard and abolished the use of PIN for authorization on ATM. It implies that all the phones to be used for transactions on the machine must have RFID tag.

Security of Transactions via Proxy

Transaction by proxy in this paper refers to the situation whereby the owner of an account is unable to process transactions on ATM in person and another person is being designated to carry out the process, the designated person(s) is addressed as the nominee. Majority of the work that have been done on nominee transactions security on ATM are fingerprint recognition based (Madhuri et al., 2018; Kaur and Malhotra, 2014; Aneesh et al, 2017; Padmapriya and Prakasam, 2013; Ravikumar et al., 2013).

The work presented by Kaur and Malhotra (2014) combines the biometric recognition technology with PIN to identify bank customers. The nominee fingerprints and family member fingerprints are also used to access the ATM machine in case of emergency when actual card holder is unable to do the transactions. The recognition of fingerprints is restricted to three people on the proposed system. Also presented by Aneesh et al. (2017) is a combination of finger print and voice.

To summarize and make clear the research gap, some of the reviewed works allow only the registered debit card owner or a nominee who has the card PIN to transact on ATM while others restricted the number of nominees to prevent PIN sharing, However, the proposed system presented in this paper is an enhancement of the existing system and it is built upon the account owner serial number (SN) on database (representing smartcard). It was developed to provide account owners the benefit of monitoring, authenticating and authorizing transactions in their accounts without disclosing PIN when transacting via proxy.

Technology involved in the Proposed System

The proposed system involves various technologies such as tools, techniques and algorithms that serve unique purposes in the operation of the system, such as the following;

Application for Graphical User Interface

Software application programming involves the concept of human-computer interaction and in this area of the program, a graphical user interface (GUI) is very important. Visual widgets such as checkboxes and buttons are used to manipulate information to simulate interactions with the program. Different programs such as Microsoft Visual Studio (MSVS) make it very simple to get a GUI with high application functionalities that are very attractive to users (Folks, 2015). Each one of these different types of applications can be used for a common interface.

Microcontroller

Microcontroller is a small computer on a single integrated circuit (IC) containing a processor core, memory, and programmable input/output peripherals. Kapoor et al. (2014) stated that microcontrollers are designed for embedded applications, in contrast to the microprocessors used in personal computers or other general purpose applications. The choice of Atmega128 microcontroller for this work is based on the design criteria such as Architecture, Program Memory, Development Tools, cost and ability to communicate with Modem.

MATERIALS AND METHOD

The design and realization of this proposed system was achieved in four phases which include the development of database (backend), modeling and designing of GUI (frontend), designing

of the selected microcontroller chip to implement the hardware and finally interfacing of the hardware with a communication modem to the host computer.

Architecture of the Proposed System

For the hardware consideration, host PC is the platform on which other components depend for this work. Microsoft Windows 8 was used as an operational platform, running on a 32 bit, 2.0 GHz processor, 3GB RAM, 320GB hard disk and 1024 by 768 resolutions. The microcontroller and communication modem derived their power through USB port from the PC. The input is the PC keyboard for entering required information on the system. The PC monitor serves as the output and provides user interface for bank client to interact with the system. Central to the input and output is Microsoft Visual studio 2013 IDE on PC which contains the developed bank database (ATM Web) and the modeled ATM GUI. Moreover, data transfer between the microcontroller hardware and the host PC is achieved through USB to serial converter. It is a hardware which allows other hardware to communicate with PC through USB interface via a standard computer prolific USB-to-serial port. Also, providing connectivity between the host PC and communication modem is the modem USB link (Future Technology Devices International Ltd, 2010). The architecture of the whole system is as presented in block diagram of Figure 1.

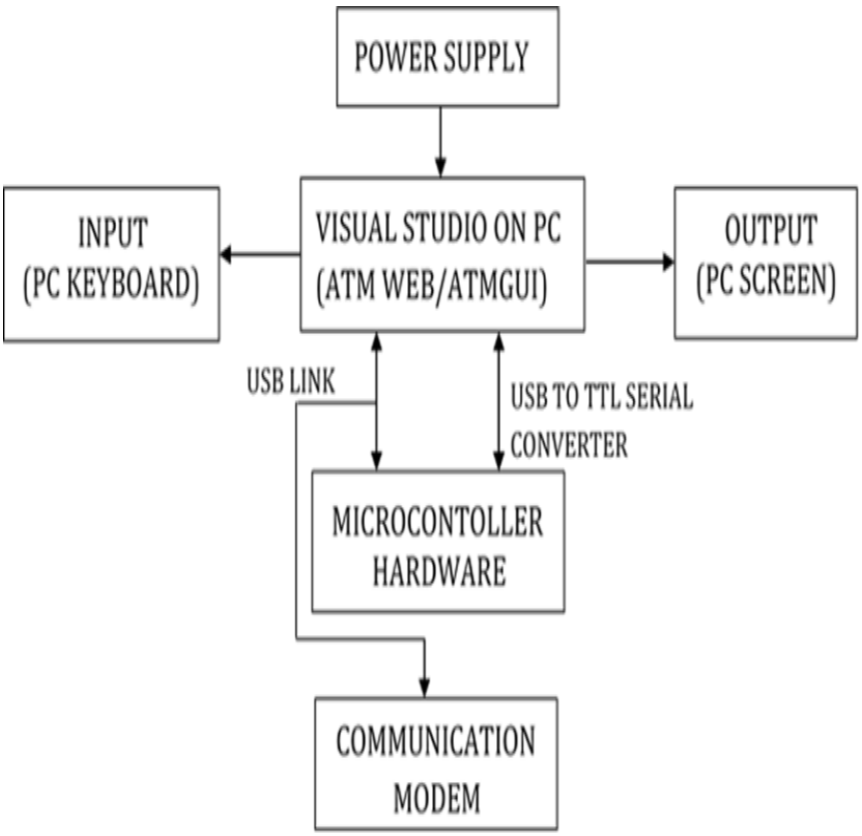


Figure 1: Architecture (Block Diagram) of the Proposed System

For this proposed ATM system, the primary actors are bank administrator, registered account owner and account owner nominee while the secondary actor is the ATM system. Both the primary and secondary trigger the use-case as presented in the diagram of Figure 2.

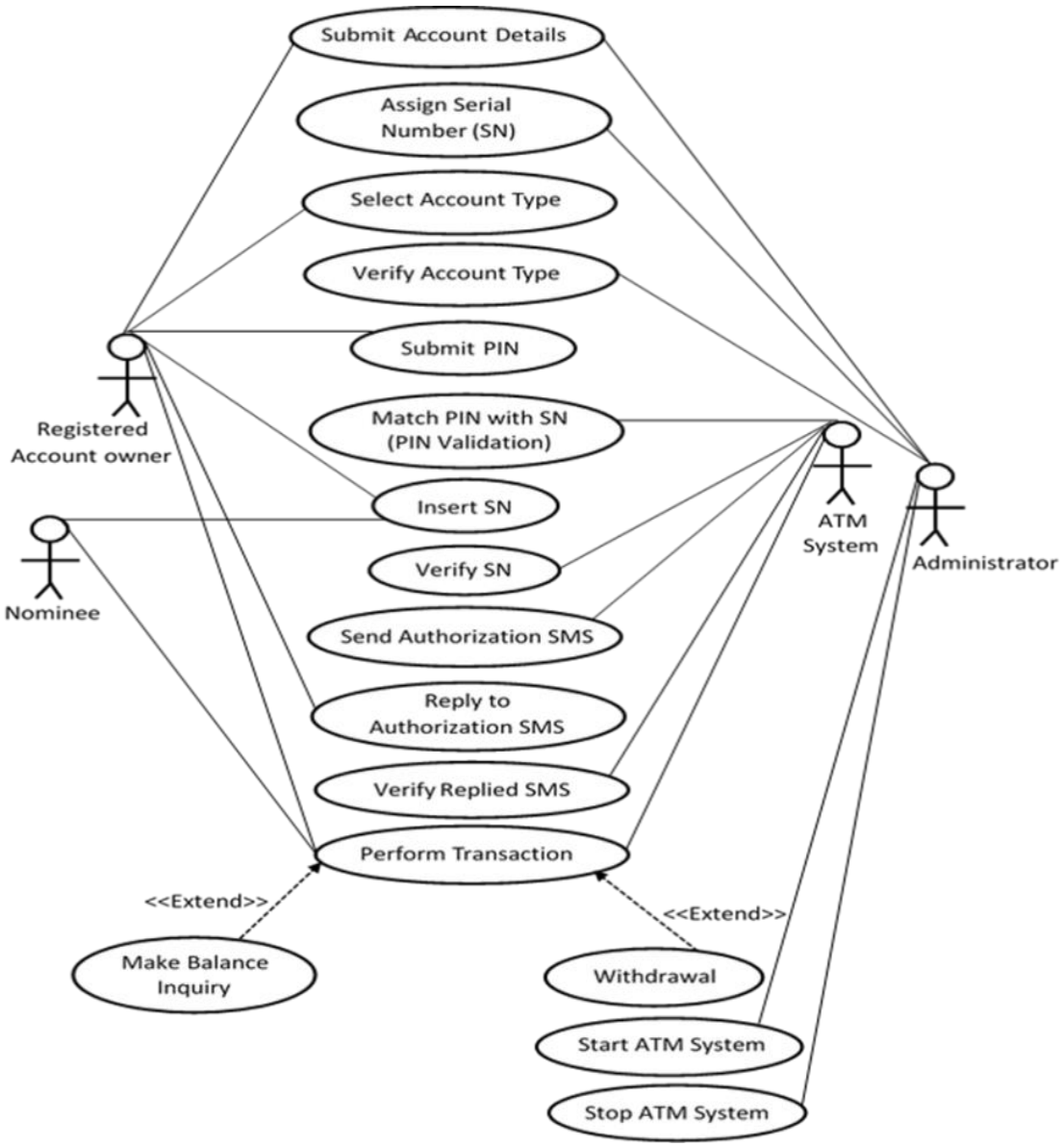


Figure 2: Use Case Diagram for the Proposed ATM System

Flowchart is used to represent the working process of the system components and development of program for the hardware. The system graphical user interface (ATM GUI) will be utilized in two main loops; namely PIN validation and authorization to transact. The validation process will entail the main account owner to create and register PIN in the machine after which it will be matched with the serial number (SN) as updated in the database. The SN is used to imitate and replace the existing ATM smartcard in this system because provision was not made for card reader. Figure 3 shows the flowchart for PIN validation loop (matching of PIN with SN).

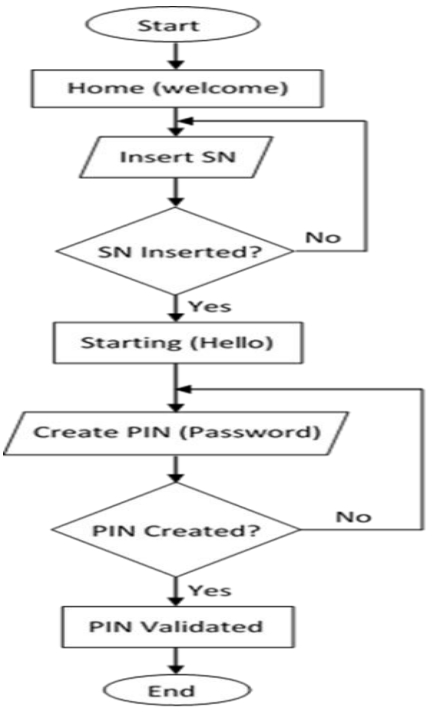
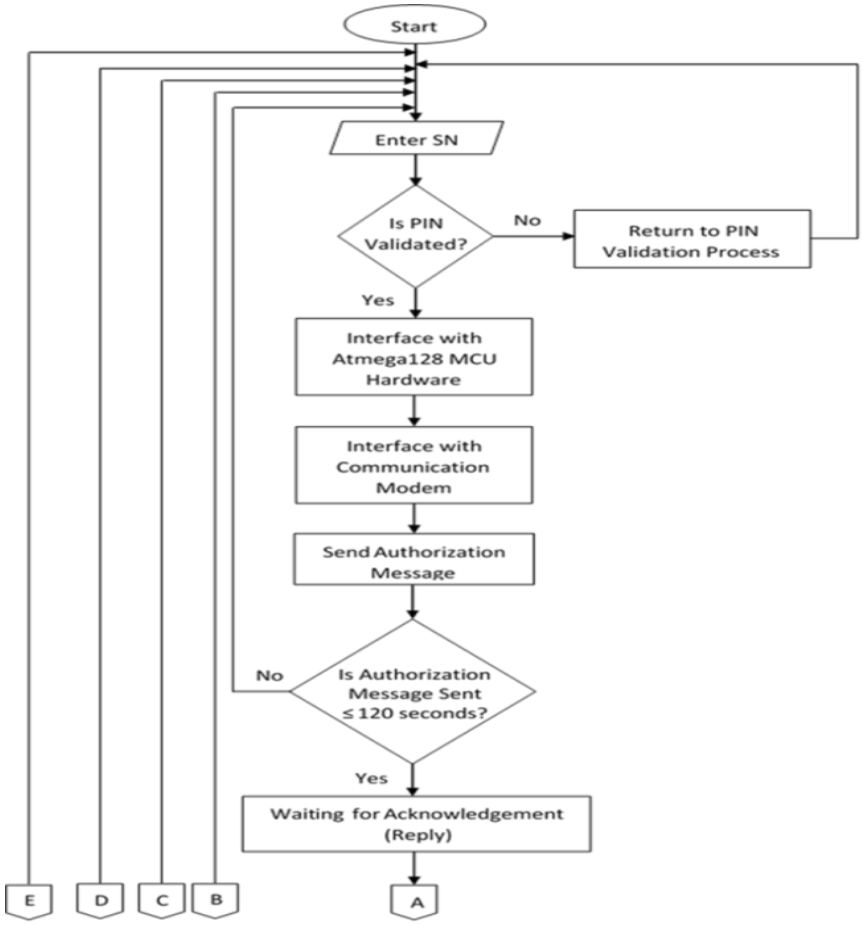


Figure 3: Flowchart for PIN validation

On the other loop, the authorization process allows further transactions on the machine if all the required protocols are fulfilled. Figure 4 presents the flowchart for authorization loop.



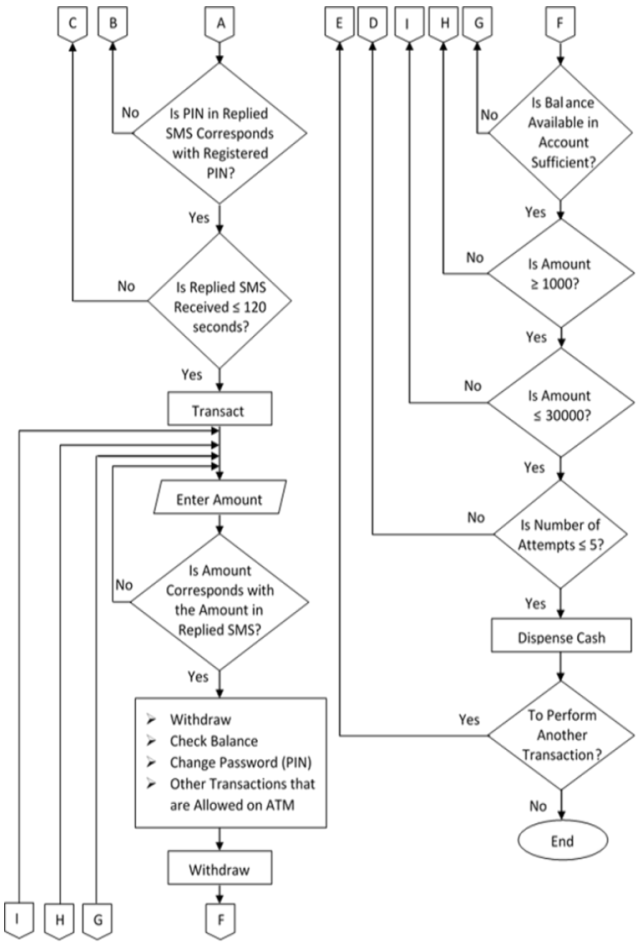


Figure 4: Flowchart for Authorization to Transact Loop

Database (ATM WEB) Design

The backend is developed with Microsoft Structured Query Language (MSSQL) server 2012. MSSQL is integrated in Microsoft Visual Studio (MSVS) 2013 IDE containing entity framework (EF) tools and Microsoft .NET framework 4.5 packages imported in it. The IDE is used to model a logical database schema as the blueprint for conceptual design of the database. Being an object-oriented database, C++ programming language is used to instantiate class diagrams that are used to model the schema as shown in Figure 5. Entity framework code first approach was adopted for the programming part of the database.

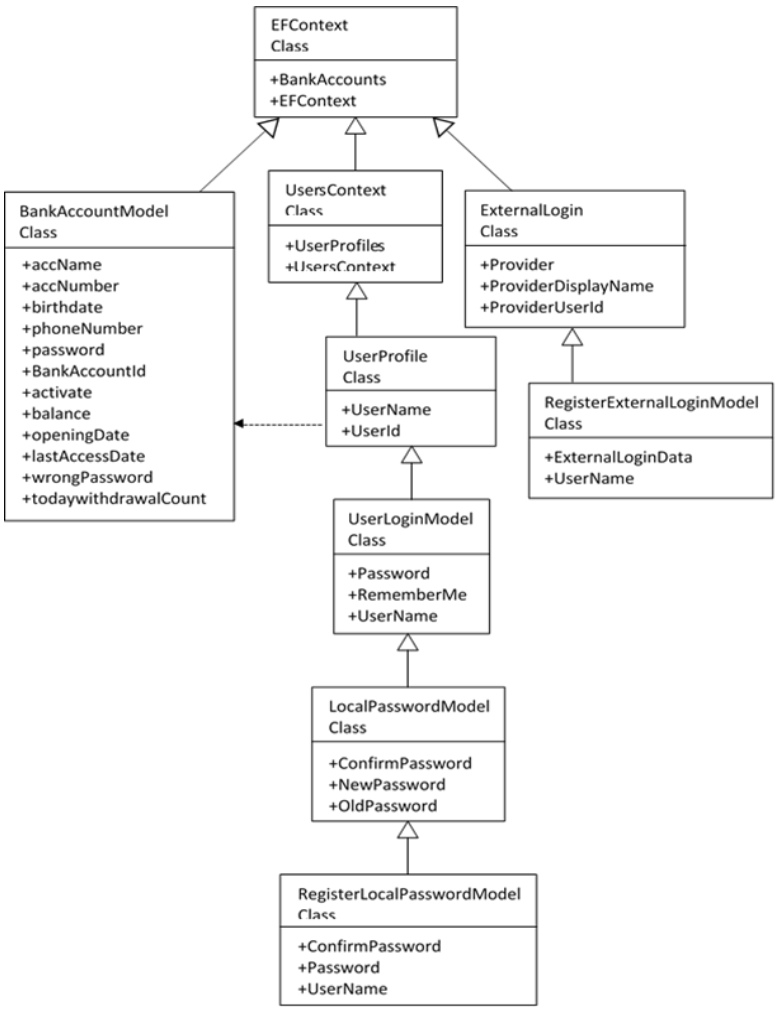


Figure 5: Class Diagram (Database Schema)

Graphical User Interface (ATM GUI) Design

An object-oriented language C# is also employed in Window's form of Microsoft Visual Studio 2013 to design the frontend (ATM GUI) where users can interact with the ATM. Graphical work with programming is combined to yield the design which composed of the following control buttons and select options as represented in Figure 6.

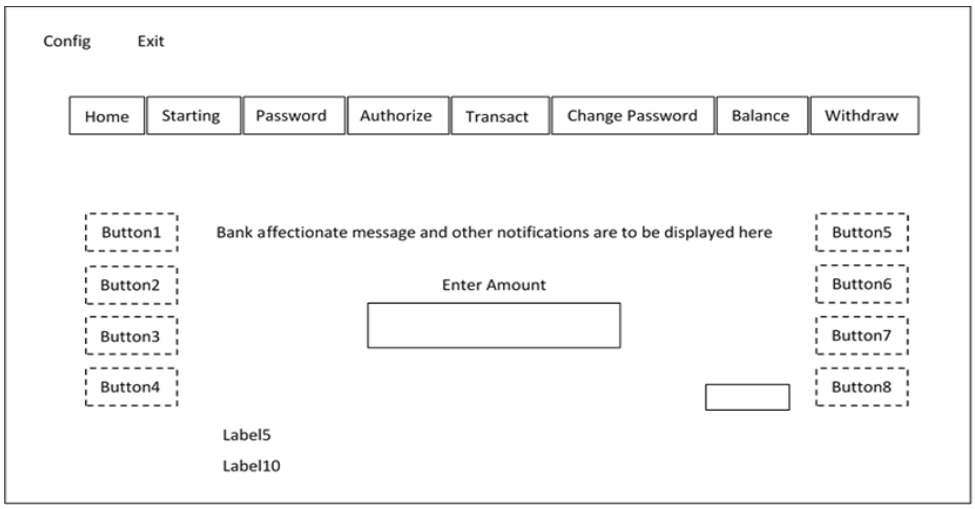


Figure 6: Design Arrangement of ATMGUI

Halvosen (2014) narrated that visual studio has ability to provide a working environment to easily generate a database that can be accessed from the internet, workstation, local area network (LAN) and so on. My ASP.NET model view controller (MVC) within the visual studio is used as the local host for the database so that the controller can provide the required information to the graphical user interface (GUI) designed for the ATM.

Design and Development of Microcontroller Hardware

The software, hardware and other tools requirement for designing and developing the microcontroller hardware includes; Eclipse Neon IDE for C/C++ Developers, WinAVR: AVR-GCC for windows, USBasp-USB programmer for Atmel AVR microcontrollers, Express PCB 7.3.5 software, Iron (III) chloride ($FeCl_3$) or etching solution, Copper clad laminate or plate, Laser Printer and Glossy (photo) paper, PCB drilling machine and soldering iron.

Programming Atmega128 Microcontroller

The first step taken in designing of the hardware was programming using embedded C language in Eclipse Neon integrated development environment (IDE). Moreover, the created source code (C-code) was compiled in GNU compiler (AVR-GCC) to produce executable linkable format (ELF) file which was converted to machine code (Hex-file) within the IDE domain. AVR-GCC is contained within the Eclipse IDE, it uses command line to compile C-code to Hex-file and store the code in a specified location in the host computer. The sequential read/write routine for accessing electrically erasable programmable read-only memory (EEPROM) and USART routine of Atmel AVR microcontroller were considered while preparing the program. Transfer of the program was done with the algorithms of standard in-system programming (ISP) of the Atmel AVR microcontroller family using the serial peripheral interface (SPI) programming. The majority of devices in the Atmel Atmega AVR family conform to the standard SPI pin-out for ISP using the master-out slave-in(MOSI), master-in slave-out (MISO) and serial clock (SCK) pins of the target device (Marriott, 2007). These derivatives are referred to as 'UART SPI Pin-out' devices as presented in Figure 7.

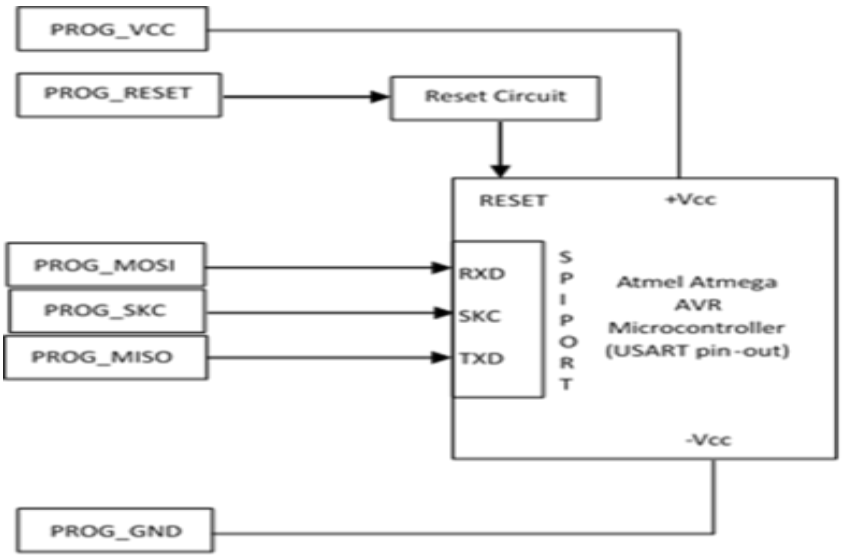


Figure 7: Atmega Standard Pin-out ISP Connection (Marriott, 2007)

It works on computer with USB port and Windows 7 operating system (OS) installed. The SPI serial programming algorithms used for the download is as follows:

Step 1- Start

Step 2- Select EEPROM (data) file
Step 3- AVR is running from internal 1MHz oscillator frequency
Step 4- Programmer uses SLOW SPI speed of 50 KHz
Step 5- Enter programming mode
Step 6- Chip erased (set EEPROM to 0xFF)
Step 7- Reset cycle the chip (AVR starts to run from the internal 8MHz oscillator frequency)
Step 8- Set EEPROM page size (the granularity of the EEPROM memory can be 1, 4 or 8 bytes in SPI mode)
Step 9- Programmer uses FAST SPI speed of 1.8432MHz
Step 10- Program EEPROM area at SPI frequency is equal to 1.8432MHz
Step 11- Program security fuses at SPI frequency is equal to 50 KHz
Step 12- End

Interfacing the Hardware
The hardware is mounted on USB to TTL serial UART converter through the 6 pins connector (CONN-SIL6) for interfacing to personal computer (PC). Prior to the interface, prolific USB to serial converter driver was installed in the PC. The driver configures and allocates prolific USB port on the PC which gives way for serial communication between the PC and the USB to serial converter hardware via the microcontroller hardware. The converter handles all the USB signaling and protocols, it provides a fast, simple way to connect devices with transistor-transistor logic (TTL) level serial interface to USB. Selectable +3.3V, 50mA or +5V, 250mA CMOS drive output and 5V safe TTL inputs make the converter easy to interface to 5V microcontrollers.

The Choice of Communication Modem
A GSM modem with USB interface was chosen for this work in order to exclude need for USB to serial converter and external power supply. The modem was tested in Micro C Pro 6.0 software to confirm that it supports protocol description unit (PDU) and text mode of sending and receiving SMS messages. The baud rate of the modem was also determined to be 9600bps in the software.

MTN communication network SIM card was used as the service provider because of its network wide coverage area in this region. AT-command was used to initiate and generate authorization message (SMS) through the implemented hardware. Huawei E168G USB modem was used to send the SMS to another mobile phone and the reply from the mobile phone was also routed through the modem back to the hardware. The algorithm used in sending SMS and receiving reply is presented as follows:
Step 1- Open Visual Studio on PC
Step 2- Lunch ATM Web
Step 3- Interface Implemented Hardware and Modem
Step 4-Lunch ATMGUI
Step 5- Hardware communicates with Modem
Step 6- Valid identification (SN) is entered in card reader emulator
Step 7- AT-command "AT+CMGF" selects message format
Step 8- AT-command "AT+CSCA" specifies the service center to be used for modem
Step 9- AT-command "AT+CMGS" sends authorization SMS to user's phone number
Step10- Reply SMS is received within the specified authentication time (120 seconds)
Step 11- AT-command "AT+CMGR" reads the reply SMS
Step 12- If the required syntax (PIN_Amount) is sent as reply SMS, transaction is allowed
Step 13 – AT-command "AT+CMGD" delete the reply SMS

Step 14- End

The realization of the interfaces utilized for this work is depicted in the block diagram in Figure 8.

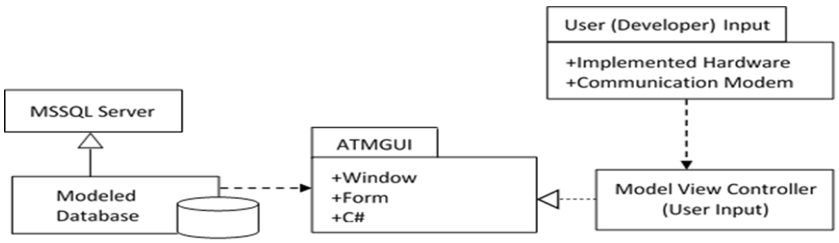


Figure 8: Realization of the Proposed System Interface

RESULTS AND DISCUSSION

The evaluation of the system was carried out with information collected from fifty (50) randomly selected staff of the Federal University Dutse, Jigawa State, Nigeria. The performance of the system was measured using the following evaluation indices:

1. Security of user PIN for transaction via proxy (security)
2. Ability of account owner to command the ATM in absentia (monitor)
3. Average authentication time ($T_{Average/S}$) which is the ratio of sum of the time taken in seconds to authenticate all the individual participant ($T_{Individual/S}$) to the total number of participants as expressed in equations (1) and (2);

$$T_{Individual/S} = T_{Received/S} - T_{Send/S} \quad (1)$$

$$T_{Average/S} = \frac{\sum_1^n T_{Individual/s}}{n} \quad (2)$$

Where ($T_{Send/S}$) time taken by the system to send authorization message, ($T_{Received/s}$) is the time taken to receive the reply message from the same customer and n is the number of participants. At the end of the authentication process, the results of the exercise are computed as shown in the Table 1.

Table 1: Results of the time-taken to authenticate some of the participants on the Proposed System.

No of Participants ($\boldsymbol{n}$)	Individual Participant (SN)	$\boldsymbol{T_{Send/S}}$	$\boldsymbol{T_{Received/S}}$	$\boldsymbol{T_{Individual/S}}$
1	25	8	50	42
2	24	9	54	45
3	23	8	55	47
4	22	10	53	43
5	21	10	51	41
6	20	10	74	64
7	15	10	65	55
8	14	8	64	56
9	13	10	63	53
10	12	9	62	53
11	11	10	60	50
12	10	8	60	52
13	9	9	50	41
14	8	10	64	54
15	7	10	63	53
16	6	10	65	55
17	5	9	52	43

18	4	9	54	45
19	3	10	60	50
20	2	10	61	51
21	1	10	62	52

Analyzing the results using equations (1) and (2), $T_{Average/S}$ was determined to be 47.58 seconds. The percentage decrease between $T_{Allowed/S}$ and $T_{Average/S}$ was also calculated to be 60.35% which shows an improvement in the authentication time on the system.

Major Findings on the Proposed System

Some of the characteristics obtained while operating the ATM system are highlighted in the following section.

Running the ATM WEB (Database) on PC

The ATM Web provides to the system customers' detail, the customer name is restricted to not more than twelve letter words. The restriction was done so that the authorization SMS which contains the name would not exceed the standard one hundred and sixty (160) characters per page of SMS. During the operation of the system, the following stages are examined on the proposed machine.

1. Starting stage: The SN of a customer is entered in the card reader emulator; the customer is welcomed with account name displayed on the GUI.
2. Password stage: The machine mandates new customers to create 4-digit PIN, the PIN is confirmed and virtually linked with customer's account records. This is to enable the machine to validate the PIN and to recognize the SN as a token for transaction.
3. Authorization stage: After PIN validation, the account owner or nominee can transact on the machine by inserting SN in the reader. On detecting the SN, ATM will send SMS to account owner's phone. The system affords the account owner two minutes to acknowledge the message or ignore it. If the request is acknowledged within the time interval, the system will process it and give way for further transaction. But if the message is ignored or communication network is not available, further transaction is denied. The message sent to the client reads 'Accessing your account "Client's name (account number)" on an ATM machine. Reply with PIN and AMOUNT to authorize this access or ignore'. The diagram in Figure 9 presents the authorization stage.

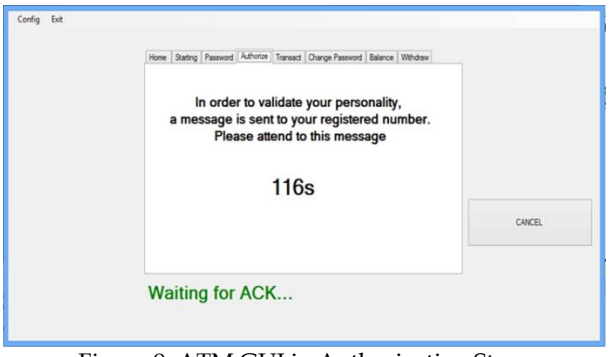


Figure 9: ATM GUI in Authorization Stage

For the machine to grant transaction, the PIN in the replied SMS must correspond with the actual client's PIN. Otherwise, the transaction is blocked due to authorization failure and system returns to home stage.

4. Transaction stage: This stage allows financial transactions such as withdrawal of money, checking of account balance, change of PIN and other related transactions allowable on ATM. Figure 10 shows the transaction page on the ATM.

Figure 10: ATM GUI in transaction Stage

5. Withdraw stage: To make cash withdrawal, the amount
6. To be withdrawn is included in the replied SMS sent from client's mobile phone to ATM as authorized amount. It must be the same amount with the one to be entered in the space provided. If the entered amount does not correspond, withdrawal will not be processed. The machine will remain in withdraw stage and display "Not authorized to dispense this amount" until when the bearer enters the required amount or cancels the process. Figure 11 presents the withdrawal page on the machine.

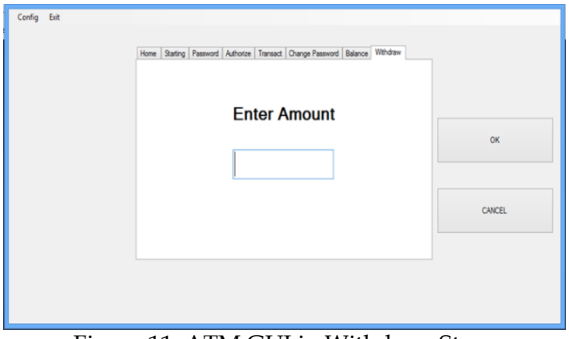


Figure 11: ATM GUI in Withdraw Stage

An authorization SMS can be used for only one withdrawal attempt on the the machine. If another attempt is to be made, another message must precede it. The maximum amount that can be dispensed is fixed at thirty thousand naira (₦30,000) while the minimum is one thousand naira (₦1,000) and withdrawal can be made five (5) times in a day.

6. Balance stage: This stage provides the available balance in the account to the bank customer.
7. Change password stage: It permits customer to change PIN if the old PIN has been compromised or for any other reason. Change of PIN can only be effected with an authorization SMS as applicable in checking balance and making withdrawal of cash. The proposed system cannot be operated without the hardware being interfaced and transactions can never be carried out because the system would be in deactivated mode.

Bridging the Research Gap

It is evident from Figure 9, 10 and 11 and the subsequent discussions that a preferred nominee of the account owner does not need to possess a PIN to debit card before transaction by proxy could be made on the system, this will provide relief on the financial institution worry and

advice that card owners should protect their PIN from third party (Adelowo and Mohammed, 2010). It will also eradicate debit card PIN fraud such as shoulder surfing, utilizing of fake PIN pad overlay and PIN interception being outlined as the major techniques used for perpetrating frauds on ATMs according to Diebold Corporation, (2012).

.

CONCLUSION

The proposed system described in this paper will serve to legalize nominee transactions on ATM. It identifies a high level model for the modification of existing ATM systems to support transaction by proxy without the user's PIN being disclosed. The authorized amount and PIN for the transaction is sent to ATM and the nominee simply takes the cash from the machine. With the integration of the technique in this research into the design of the existing system, security vulnerability of transaction via proxy is reasonably addressed. This is a step towards eradicating the limitations and fears associated with the use of ATMs.

REFERENCES

Adelowo S. A and Mohammed E. A. (2010) "Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria – A Case Study of Selected Banks in Minna Metropolis" Journal of Internet Banking and Commerce, 2(15): 2-2.

Aneesh C., Aiswarya P., Abee Joe V., Deen Shifaz (2017) "ATM for Visually Challenged People "International Research Journal of Engineering and Technology, 4(3): 370-375.

Century Savings Bank (2014) "ATM Debit Card and Security Tips". Published by Financial Education Corporation, Las Vegas, USA, pp. 1-4

Diebold Corporation, (2012) "White Paper on ATM Fraud and Security". North Canton, Ohio, United States, File No. 98-192, pp. 1-8.

Folks Joshua, (2015) "Using Microsoft Visual Studio to Create a Graphical User Interface". User Interface ECE 480 Design Team 11 Application Note, April 3, 2015, pp. 1-10.

Frimpong Twum, Kofi Nti and Michael Asante (2016) "Improving Security Levels in Automatic Teller Machines (ATM) Using Multifactor Authentication". International Journal of Science and Engineering Applications, 3(5): 126-134

Future Technology Devices International Ltd (2010) "TTL to USB Serial Converter PCB Datasheet" Seaward Place, Glasgow, United Kingdom. Version 2.04, pp. 1-29.

Halvosen Hans-Petter (2014) "Introduction to Visual Studio and C#".Telemark University College, Faculty of Technology, Department of Electrical Engineering, Information Technology and Cybernetics, Porsgrunn, Norway. Published Material by Postboks, Porsgrunn, Norway, pp.1-47.

Jayasudha A. C., (2014) "Two Factor Authenticated Cash Withdrawal Using Mobile Phones and Apprehend Insecure Users within the ATM Centre". Contemporary Engineering Sciences, 7(10): 449-455.

Kapoor Sahil, Narendra Singh and Shiv Chauhan, (2014) "Microcontrollers". International Journal of Innovative Research in Technology, 1(6):1275-1278.

Kaur Jaspreet and Malhotra Sheenam, (2014) "An Overview of ATM Security Using Biometric Technology". International Journal of Advanced Research in Computer Science and Software Engineering, 4(3): 761-763.

Khatmode Ranjit P, Kulkarni Ramchandra V, Ghodke Bharat S, P. P. Chitte and Prof. Anap S. D (2014) "ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology" International Journal of Emerging Technology and Advanced Engineering, 2(4): 856-860.

Madhuri More, Sudarshan Kankal, Akshaykumar Kharat, Rupali Adhau (2018) "Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using Human

Fingerprints" International Journal of Advance Engineering and Research Development, 5(5): 392-399.

Marriott (2007) "Serial Peripheral Interface (SPI) and Joint Test Action Group (JTAG) In-System Programming (ISP) Guidelines for the Atmel Atmega AVR Microcontroller Family". Application Note 101, 12th June 2007, Version V1.07, pp. 1-27.

Okafor, Chinedu Martin (2015) "Design of Two-Factor Authentication (Pin and SMS Password) for an Automated Teller Machine (ATM)". M.Eng. Thesis in Electronic Engineering, Department of Electronic Engineering, University of Nigeria, Nsukka, Nigeria. pp. 1-131.

Padmapriya V., and Prakasam S., (2013) "Enhancing ATM Security using Fingerprint and GSM Technology" International Journal of Computer Applications, 80(16): 43-46.

Ravikumar Sowmya, Sandhya Vaidyanathan and Thamotharan Ramakrishnan (2013) "A new Business Model for ATM Transaction Security using Fingerprint Recognition". International Journal of Engineering and Technology, 5(3): 2041-2047.