Journal of
Information Security and Technologies

Research Article Open Access

Design of a Multifactor Authentication System for Automated Teller Machines

Peter Kibaya[1] and Charles S Lubobya[2*]

[1]Electrical Engineering, The University of Zambia Lusaka, Zambia

[2]Department of Electrical and Electronic Engineering, University of Zambia, Great East Road Campus, Lusaka, Zambia

[*]**Corresponding Author:** Charles S Lubobya, Department of Electrical and Electronic Engineering, University of Zambia, Great East Road Campus, Lusaka, Zambia, Tel: +260 95 5883480 / +26097 2823238, E-mail: cslubobya@unza.zm

Received Date: February 25, 2023 **Accepted Date:** March 25, 2023 **Published Date:** March 28, 2023

Citation: Peter Kibaya, Charles S Lubobya (2023) Design of a Multifactor Authentication System for Automated Teller Machines. 1: 1-17

Abstract

This paper proposes the use of fingerprint authentication and One Time Password (OTPs) as the second and third factor of the Multifactor authentication (MFA) process. By requiring the use if the user to provide any one of the 10 fingerprints, OTP and 4-digit PIN, the risk of fraudulent transactions is greatly reduced. Banking transactions conducted through automated teller machines (ATMs) are vulnerable to fraud and identity theft. Implementing 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. 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.

Keywords: Multifactor Authentication (MFA); One Time Password (OTP); Automated teller Machine (ATM); 4-digit PIN; Fingerprint authentication

Introduction

The banking sector in Zambia has seen a considerable shift over the past three decades, moving from manual processes to investments in automated processes with significant ICT investments in order to have a competitive edge over competitors. Due to the continually rising demand from clients to access their money, almost all commercial banks in Zambia have ATMs. Despite requests for the country to rely less on cash, it is clear that there is a demand for real money.

With the ever-increasing demand for access to cash via ATMs in the Zambian financial sector there has been a rise to fraud through card skimming, card theft and identity theft through acts like social engineering. [1-3]

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 [4]. However even with this in place, ATM/POS transactions are not completely 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 [5] (Verified by Visa) are not mandatory for all online vendors to implement on their e-commerce sites for legitimate users to authorise transactions as some transactions may bypass this safeguard.

This paper proposes a design of a Multi factor authentication of automated teller machines using Fingerprints, PIN and OTPs in order to avert ATM card frauds.

Limitations and Cost Implications of the Proposed System

The cost implication of integrating fingerprint scanner and OTP verification in ATM infrastructure can vary depending on several factors such as the number of ATMs to be upgraded, the type of fingerprint scanner and OTP verification technology used, and the level of security required.

Generally, adding fingerprint scanners and OTP verification to ATM infrastructure can increase the cost of each ATM unit by several hundred to several thousand dollars. This is because the hardware and software required for biometric authentication and OTP verification must be integrated into the ATM machine, and the necessary infrastructure must be established to support these features.

However, it is worth noting that the cost of not implementing these security features could be much higher. ATM fraud is a significant problem, and adding biometric authentication and OTP verification can help reduce the risk of fraud and protect customers' sensitive information. Additionally, the cost of fraudulent activity can be significant, and implementing stronger security measures can help prevent financial losses. Overall, the cost implication of integrating fingerprint scanner and OTP verification in ATM infrastructure will depend on several factors and may vary from one location to another. Still, the benefits of increased security and fraud prevention could outweigh the initial investment in the long run.

Some of the limitations that the system is subject to areas follows;

1. This system could prove to be challenging for users with damaged or missing fingers, loss through accidents 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. Time delays in delivering OTPs by the system could affect its efficiency because OTPs are time bound and do expire after a stipulated amount of time. This could also apply to latency in the ATM network that could affect user input during transactions.

6. The system is also limited to only ATM and POS transactions and does not include online card payments.

The simulation is merely simulation and hence it does not include critical aspects of the transaction flow such as the Transaction switch, CBS and HSM.

Related Works

When conducting this research, 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 this research aims to bridge. After the knowledge gap the justification for the research shall be birthed from the reviewed projects.

Below are research projects conducted by other researches in the area of ATM security using MFA authentication with the use of biometrics.

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 [16].

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 4-digit PIN in addition to an alphanumeric PIN and biometric finger data to authenticate users. The system supports two different kinds of activities: A transaction, such cash withdrawals and fund transfers, and B transactions, including balance inquiries and fund transfers for accounts that aren't linked to the ATMs account [17].

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 [18].

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 [19].

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. biometric data is stored in binary form in the database for cross referencing during the verification process.

The researchers found that this approach worked excellent, 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 [20].

Comparative Analysis

It is important to note that the cost of implementing biometric verification can vary depending on factors such as the number of devices needed, the level of security required, and the specific implementation details. Additionally, ongoing costs such as maintenance and upgrades should also be considered when evaluating the cost of different biometric technologies.

The proposed system and its random request of the fingerprint from the user for authentication and the use of OTPs for transaction authentication make it unique and safe for users. Additionally, the cost of fingerprint scanners relative to other biometric systems is cheaper to implement.

The current security measures are not adequate to curb the many dangers present. Many cards still have the black magnetic stripe that make it very easy for fraudsters to skim such cards and later perform transactions on the customer’s account without their consent. ATM card readers and POS terminals may be compromised by malicious actors by placing a card skimmer one the carder of the ATM or POS terminal, which reads all the card data for cloning.

The registration phase includes capturing the customer’s

Fingerprint, One Time Password and Multi-factor Authentication

One Time Password (OTP)

personal information such as their full names, date of birth and their respective Iris biometric data using a digital camera. This 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.

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 [6-9].

Fingerprint

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 [10-12].

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. 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 such as enhanced security because 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.

This paper reports the results of simulations conducted on a user attempting to transact at an ATM. The MFA is designed to have three tiers in its authentication process. The first being biometric authentication via a randomized approach where the ATM requests a user to provide any one of their 10 fingerprint samples which only user knows and has. One authenticated with the right fingerprint, the user provides their 4-digit PIN, the user was then requested to provide the OTP sent to a mobile device whose phone number is linked to the bank account.

The research showed that the three tier MFA averted the aspect of authenticating the legitimate user of the account and ensuring that malicious persons find it impossible to have access to a user's account [13-15].

Methodology

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.

This phase will constitute capturing the customer fingerprint data in two stages and we adopted a methodology similar to [21].

User Registration stage

At this stage, user data is captured including fingerprint data in line with KYC (Know Your Customers) norms. KYC is a process carried out by banks and other financial institutions which includes verifying a customer's or client's identification, determining their potential risks, and assuring compliance with anti-money laundering (AML) rules and regulations are all included in the process.

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.

The Transaction Switch in question differs from the conventional networking device, it is a service that normally sits between the bank's hardware security modules and the core banking system, its sole purpose is to acquire and issue the bank's transitions via various payment gateways such as VISA, MASTERCARD, UNION PAY, American Express, Mobile Service Operators and many others.

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.

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.

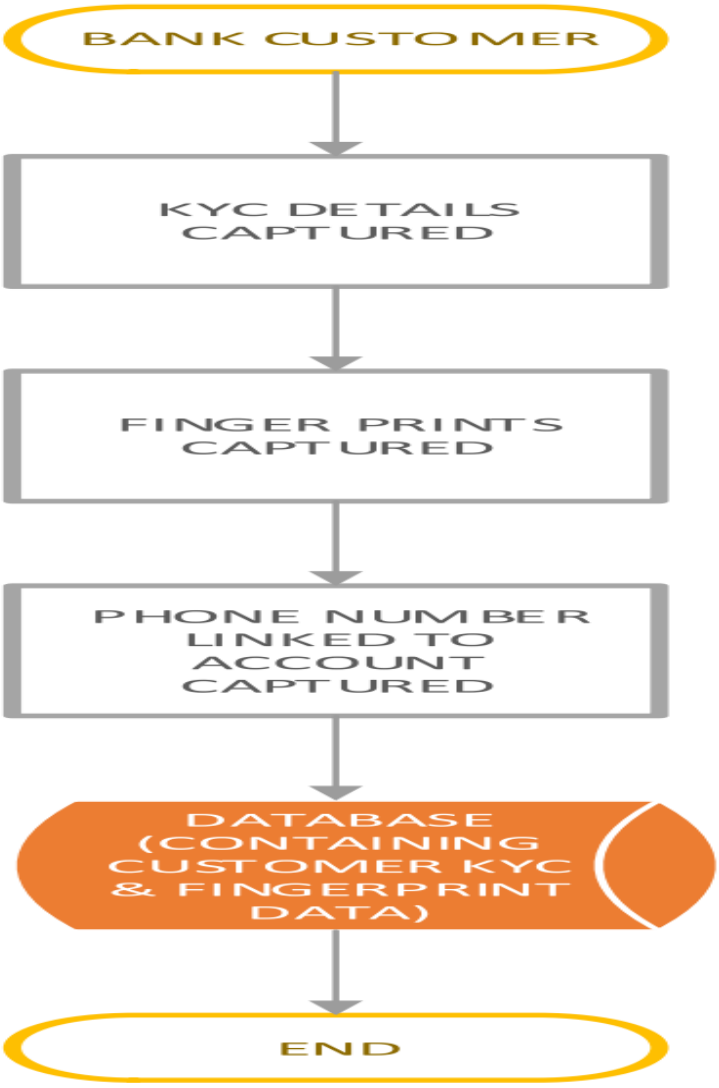

Figure 1: User Registration phase

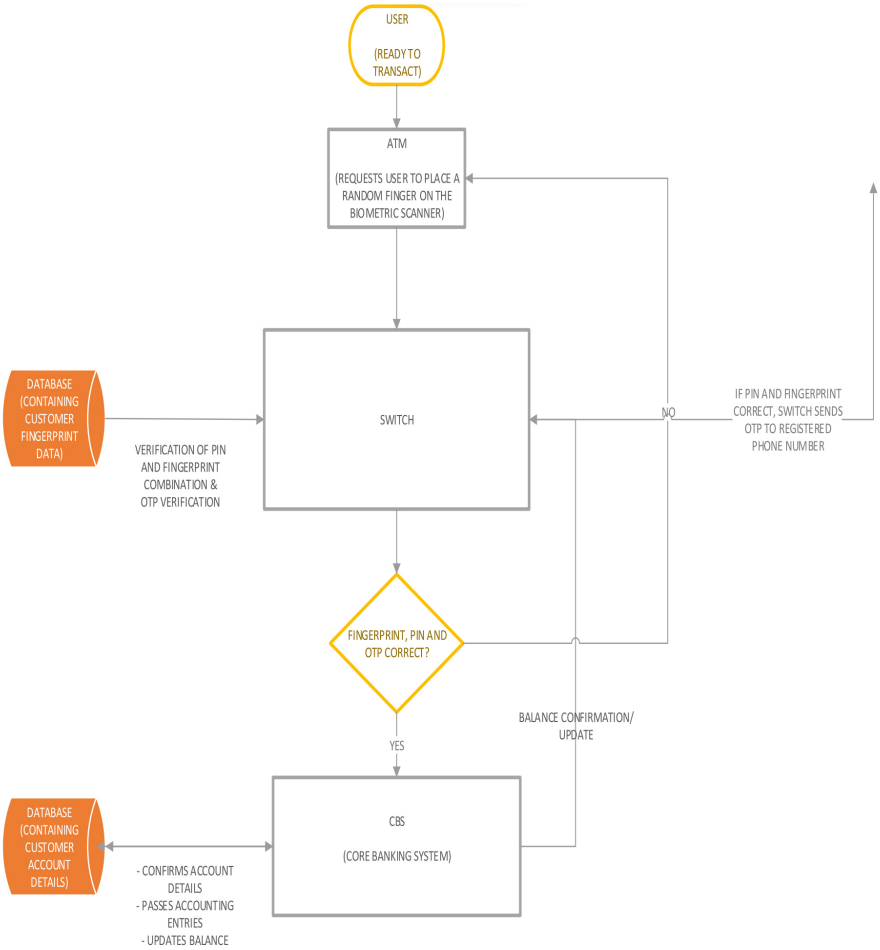

Figure 2: Proposed system Flow chart

Results and Discussion

this section presents result from the simulation of the multifactor authentication system for automated teller machines. The results of this simulation were obtained from Proteus Isis Pr0fessional 8. 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.

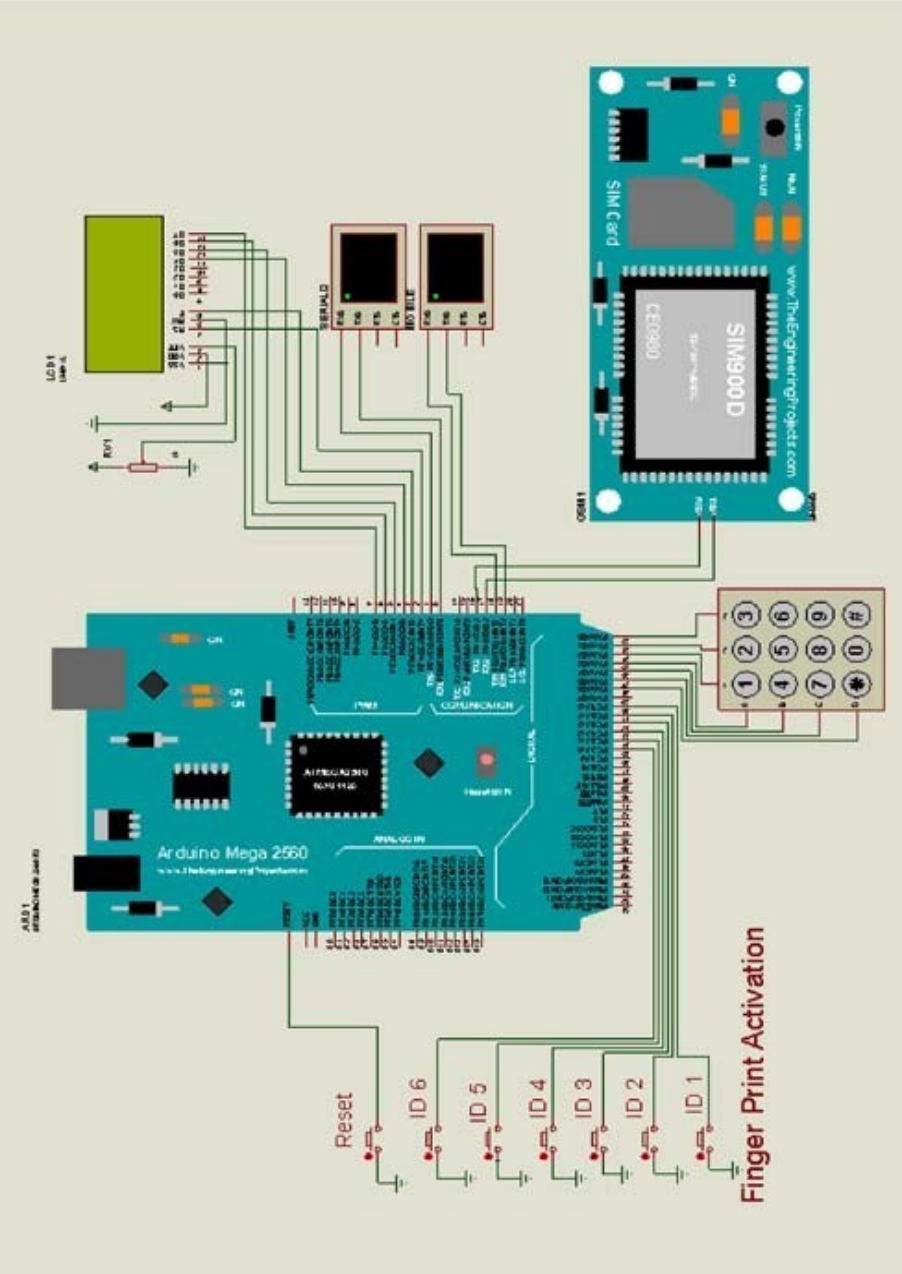

Figure 3: Schematic view of Proteus design

Figure 3 above provides a general layout of the design. The design comprises of the following components.

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 send by the MFA system for transaction authorization by the customer.

5. Arduino: This houses the logic of the Fingerprint randomization mechanism and also simulates the ATM.

6. Keypad: To capture user input

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.

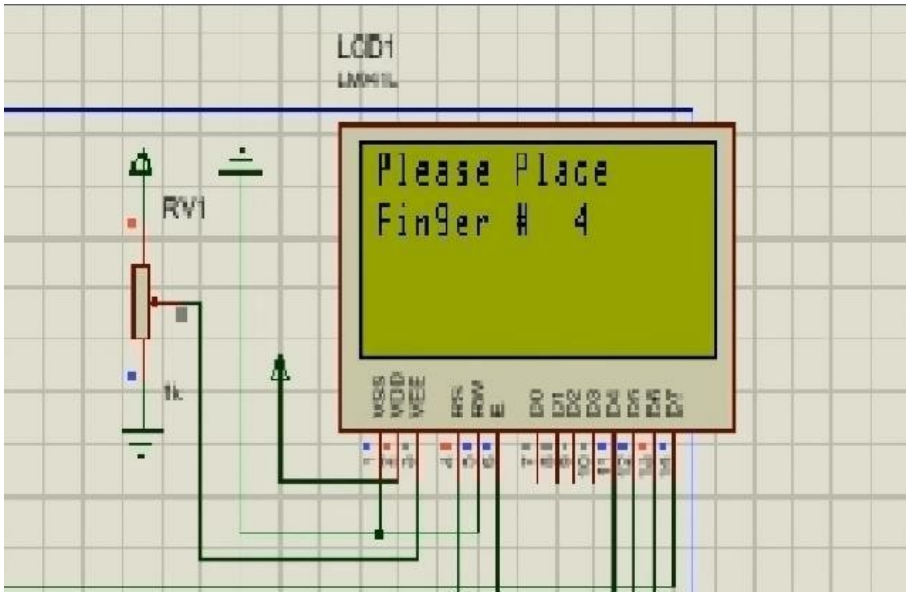

Figure 4: User prompted to place the fourth finger print on fingerprint scanner

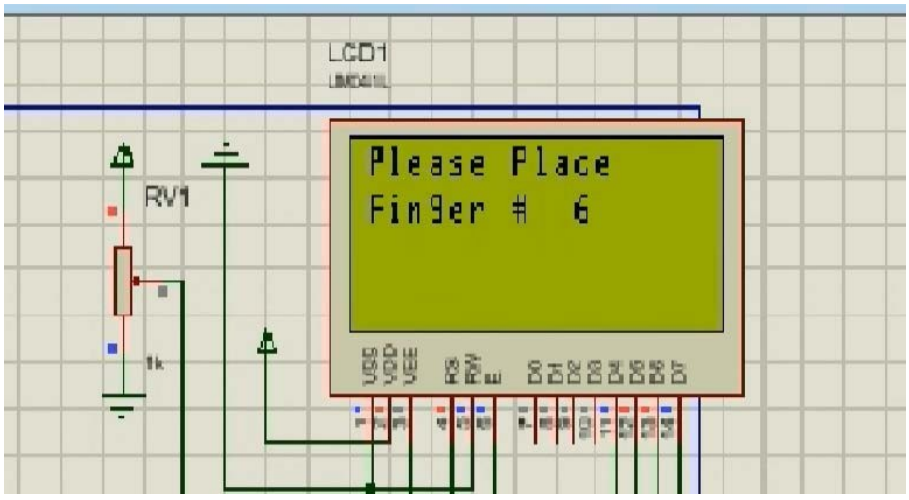

Figure 5: User prompted to place the sixth finger print on fingerprint scanner

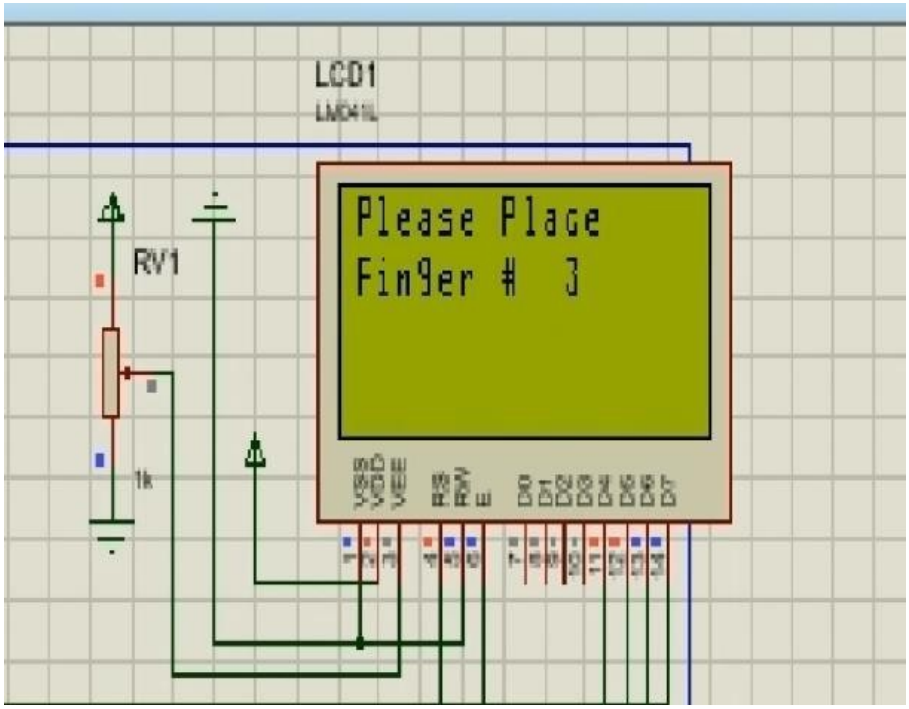

Figure 6: User prompted to place the third finger print on fingerprint scanner

Figures 4, 5 and 6 display the random fingerprint request by the machine. This is the first tier in the authentication stack to ensure that malicious actors have a difficult time authenticating and accessing user accounts.

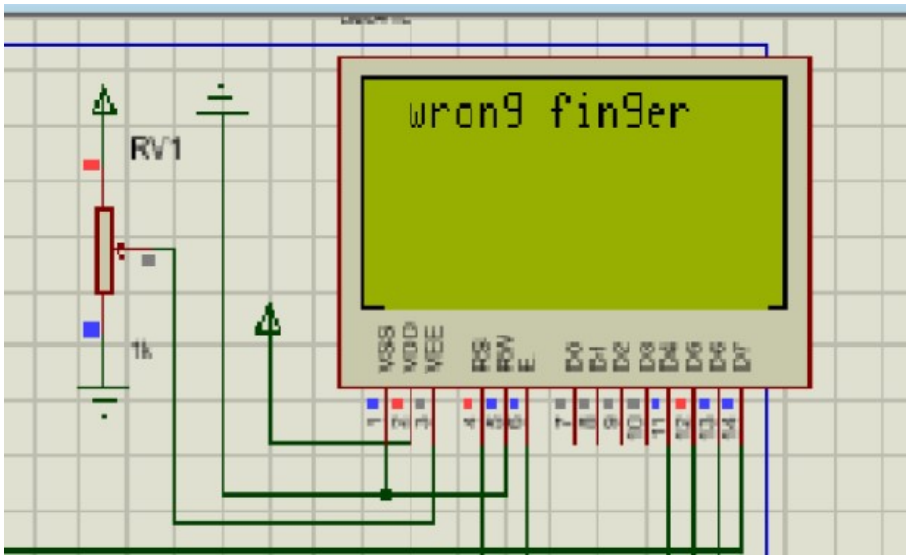

Figure 7: Incorrect Finger error

However, whenever the user provided any finger other than the one requested, even though it is the legitimate owner of the account, the user was not authenticated as can be seen in Figure 7.

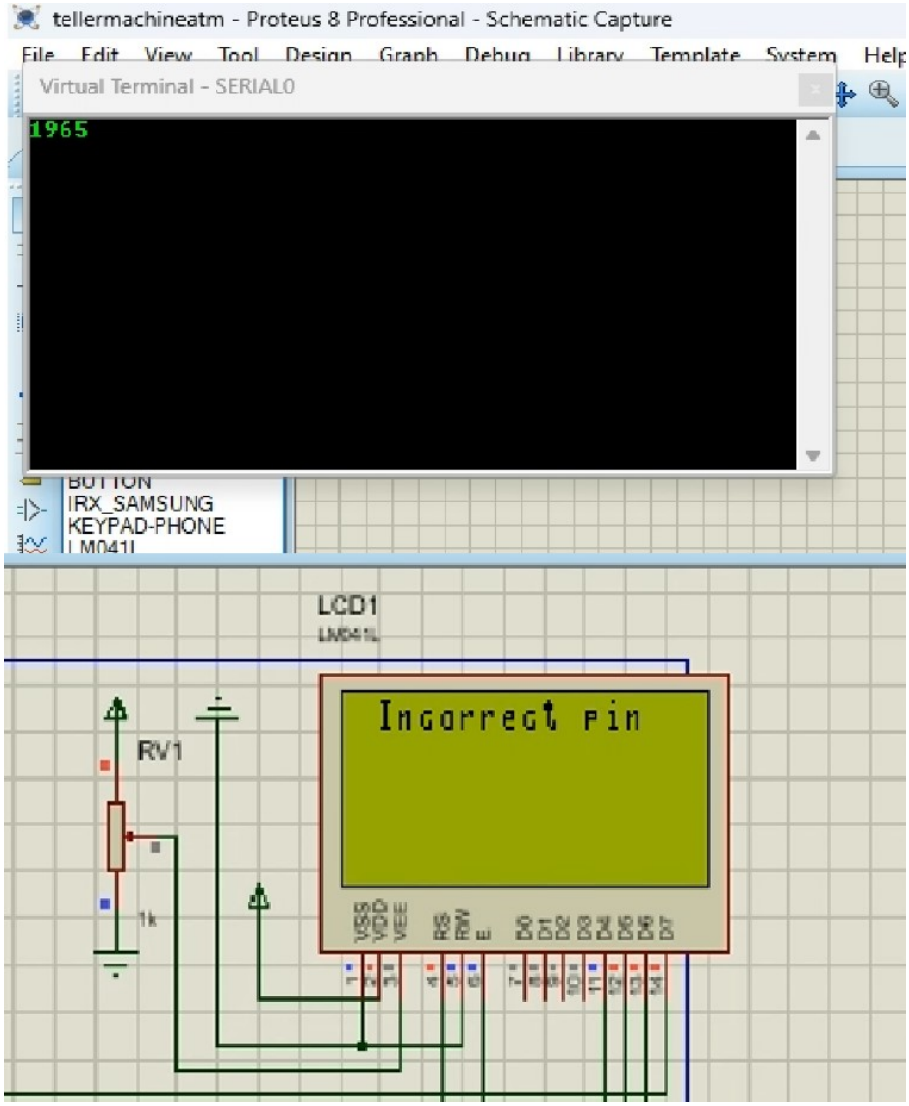

Figure 8: Incorrect PIN error

When the wrong PIN was entered, the error Incorrect PIN was displayed, in the figure above, the user entered the PIN 1965 instead of the correct PIN 1991.

The 4-digit PIN is the second tier in the authentication stack, when the correct PIN is provided, the user is granted access to the transaction options available on the ATM.

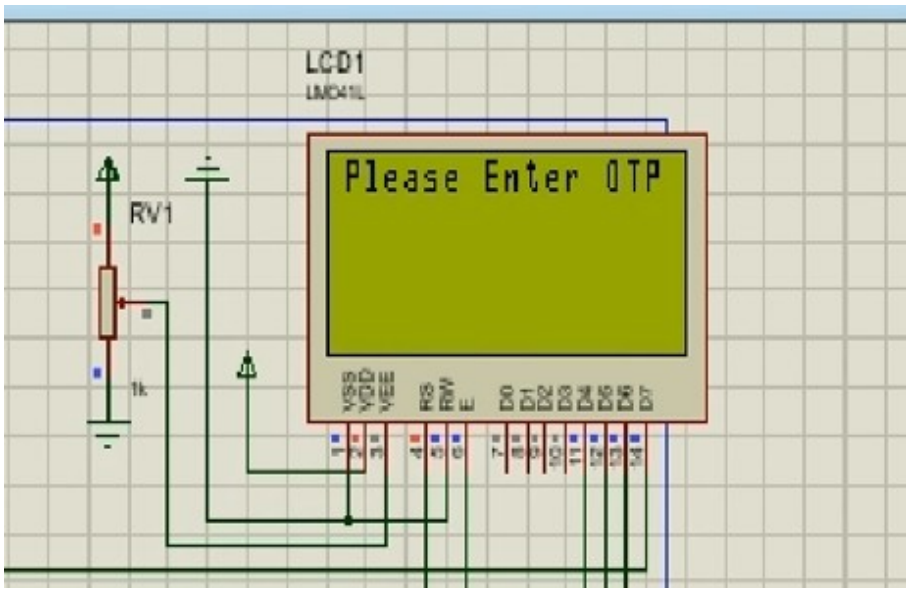

Figure 9: OTP prompt

The figure above shows the OTP prompted displayed to the customer at the ATM, after going passed the first 2 authentication tiers, the third and final authentication stage is via OTP. The OTP is sent to a user's mobile device whose number is linked to the bank account.

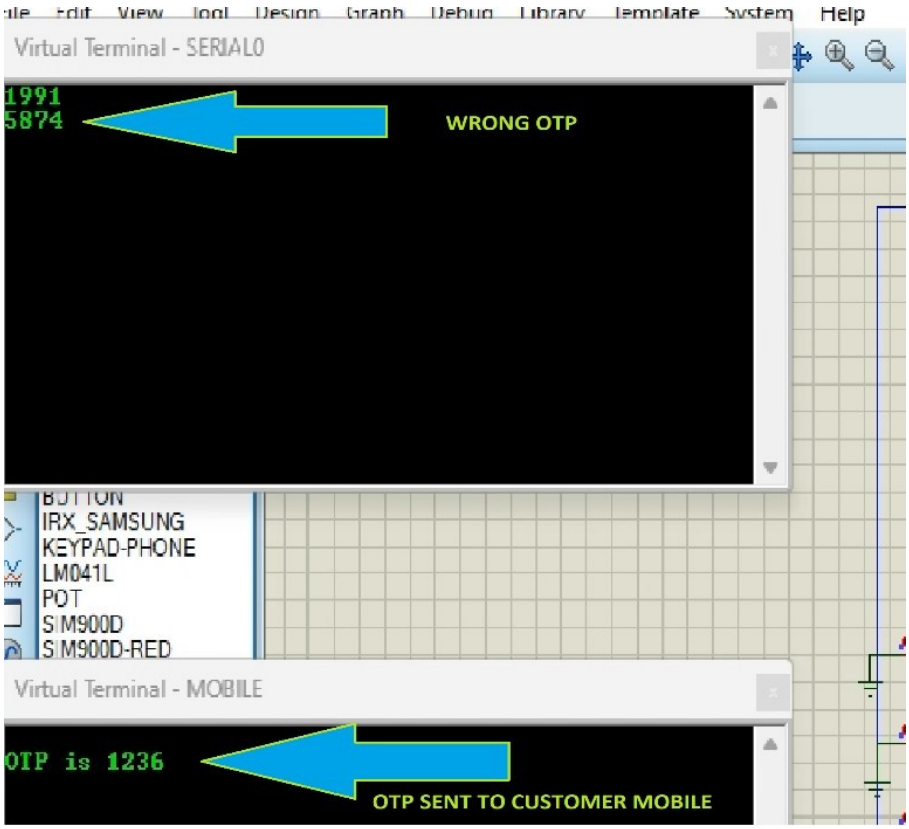

Figure 10: Shows a failed OTP authentication prior to an ATM withdraw. The user entered 5874 as the OTP when the correct OTP was 1236. This showed the that without correctly authenticating at all three tiers, the user can not complete a transaction

Failed authentication – incorrect OTP Figure 10.

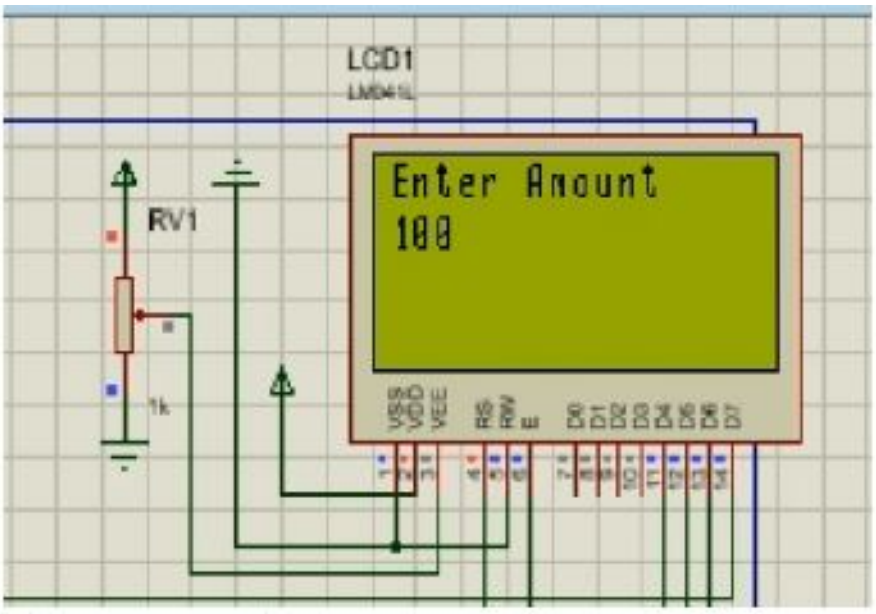

Figure 11: Amount input Screen

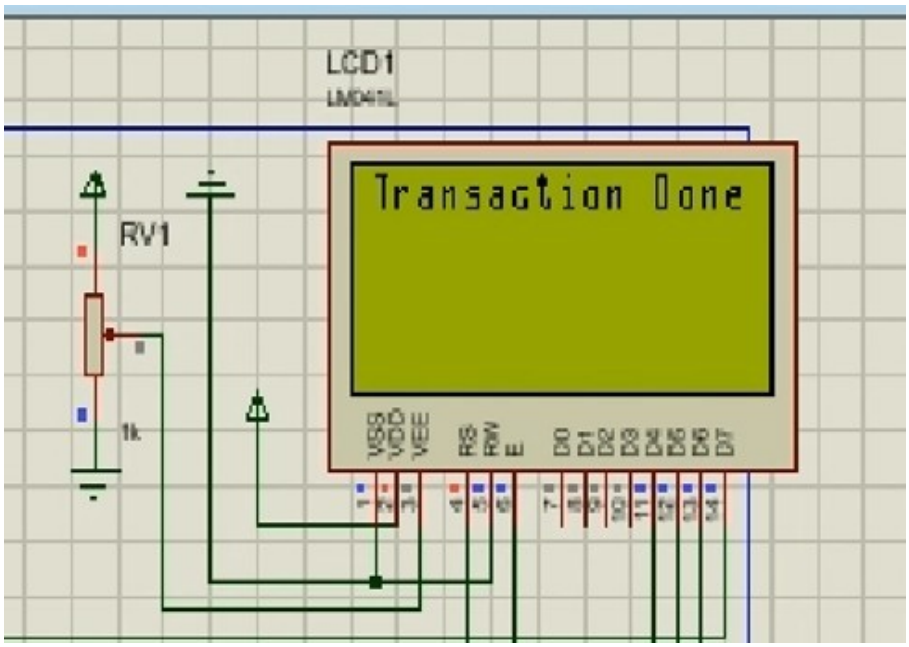

Figure 12: Transaction complete

Once the correct OTP was provided, the user was prompted to enter the amount required for withdraw, after which the transaction was processed and completed.

The tables I, II and III summarise the tests, Table I shows a summary of the Fingerprint authentication use cases where three attempts were made. The system showed the randomization capabilities by requesting a user to place any one of the 10 fingerprints at each given time and being authenticated based on the correct position fingerprint.

The tests show that the user was displayed with a Wrong Finger error whenever another finger other than the one requested was given despite the user being the legitimate owner of the account. In the failed authentication test, the system requested the user to place their Third (3) position finger, however the fingerprint on position 1 was provided hence failing to authenticate.

The other 3 tests where the system requested for the fourth (4), sixth (6) and third (3) fingerprints were re-

quested and the correct fingerprints were provided, the user was successfully authenticated.

Table II displays a summary of the PIN and OTP authentication stages. Where the user provided any PIN other than a customer's 4-digit PIN the user was not authenticated and an Incorrect PIN error was displayed. However, when the

user provided the correct PIN, the user was successfully authenticated. The same was the result for the OTP authentication for ATM transactions, the user was required to enter the correct OTP sent to the mobile device, anything other than the correct OTP prompted the user to not proceed with the transaction and display a Wrong OTP error.

The final Table III shows the authentication matrix of the entire system showing that for a transaction to be completed successfully, a user requires to successfully provided the correct parameters at all tiers of the authentication stack.

Table 1: Table Summary of Fingerprint Simulation Tests

No.	Finger ID	User input	Result	TXNStatus
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 2: Otp and Pin Authentication Table Summary

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	Transactioncomplete	Success

Table 3: Authentication Matrix

Tier	Finger	PIN	OTP	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

Table4

Biometric Verification	Advantages	Disadvantages	Cost Considerations
Fingerprint Recognition	Widely available and easy to use Highly accurate Low cost compared to other biometric technologies	May not work for peoplewith certain skin conditions or injuries Fingerprints can be spoofed or copied	Generally low cost, with prices ranging from a few dollars to a few hundred dollars per device.
Face Recognition	-Non-intrusive and easy to use -Widely available, as many devices already have cameras -Can be used for real time authentication	-May not work as well in low light or if the person is wearing a mask or sunglasses -Can be less accurate than other biometric technologies	Generally low to moderate cost, with prices ranging from a few dollars to a few hundred dollars per device. More advanced face recognition technologies may be more expensive.
Iris Recognition	-Highly accurate -Difficult to spoof or copy -Less affected by changes in lighting or facial hair	-Requires more specialized equipment than other biometric technologies -Can be more expensive than other biometric technologies	Generally moderate to high cost, with prices ranging from a few hundred to a few thousand dollars per device.
Voice Recognition	-Non-intrusive and easy to use -Can be used for real-time authentication -Can be integrated with other security measures	- May not work as well in noisy environments -Can be less accurate than other biometric technologies	Generally low to moderate cost, with prices ranging from a few dollars to a few hundred dollars per device.
Hand Geometry Recognition	-Easy to use -Less affected by skin Conditions or injuries than fingerprint recognition -Less invasive than other biometric technologies	-Requires specialized equipment -May not work as well for people with small hands or disabilities	Generally moderate to high cost, with prices ranging from a few hundred to a few thousand dollars per device.

Conclusions

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.

References

1. "ATM (2023) skimming fraud: DEC arrest Chinese gang cloning bank cards in Zambia – Mwebantu."

2. Chinese men in court for theft (2023) 'ATM fraud' - Zambia: News Diggers!"

3. "Barclays Bank Zambia (2023) hit by ATM fraud - PC Tech Magazine."

4. Chip-And-PIN Card Definition (2023) "https://www.investopedia.com/terms/c/chipandpin- card.asp.

5. "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).

6. M K. IJ on R, I. Trends and undefined (2015) "Securing ATM with OTP and Biometric," academia.edu.

7. 7. M al Imran, M Mridha (2023) MNIC on, and undefined 2019, "OTP based cardless transction using ATM."

8. M K-IJ on R. and I Trends and undefined 2015, "Securing ATM with OTP and Biometric," academia.edu.

9. M al Imran, M Mridha, M. N.-I. C. on, and undefined 2019, "OTP based cardless transction using ATM,"

10. A Steven, L Arokiasamy (2023) "Fingerprint Based Automatic Teller Machine,"

11. L Narayan, SG, SM (2020) "Fingerprint Recognition and its Advanced Features," International Journal of Engineering Research 9

12. B Sahar, AR on E. S and undefined 2018 "Fingershield atm–atm security system using fingerprint authentication,"

13. O Ebenezer, MO Genseleke, EN Osuigbo, C Chigozie Okwum (2018) "Implementation of multifactor based authentication scheme for enhanced atm security," researchgate.net vol. 181: 975-8887.

14. F Twum, K Nti, MA. -IJ. of S and undefined 2016 (2016) "Improving security levels in Automatic Teller Machines (ATM) using multifactor authentication," ijsea.-com 5: 2319-7560.

15. K Olatunji, C Afolalu, OA. J Multidiscpl (2016) Eng. Sci. Technol., and undefined 2016, "Design and Implementation of a Multifactor Authentication System In ATM Security," jmest.org 3: 2458-9403.

16. D Ranjitham, S Manoharan, V Murugesan, S Sabaresan Ravi (2023) A Professor "Face Recognition and Fingerprint Based New Generation ATM," ijisrt.com 3: 3.

17. A Iyabode, Y Nureni, AA -IJ of and undefined (2015) "Card-less electronic automated teller machine (EAT-M) with biometric authentication," Citeseer 30: 2.

18. SM Shuhidan et al. "AES cardless automatic teller machine (ATM) biometric security system design using FPGA implementation," iopscience.iop.org

19. S Das, JD. IJ of I and undefined 2011 "Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system," Citeseer,

20. A Omolara, A Jantan, OA J of E and undefined 2019 "Fingereye: improvising security and

21. optimizing ATM transaction time based on iris-scan authentication.," researchgate.net

22. Kangwa M, Lubobya CS, Phiri J (2023) Enhanced Protection of Pseudonymized User Data via the Use of Multi-layered Hardware Security. In: Ao SI. Castillo O, Katagiri H, Chan A, Amouzegar MA (eds) Transactions on Engineering Technologies. IMECS