Enforcement of Highly Secured Dynamic ATM Pin Entry

K Ranjith Kumar¹*, R Reegha Shreyaa², K M Thiyaneswaran², R Santhosh², S Gururajan²

¹Assistant professor, Department of Electrical and Electronics Engineering, Kongu Engineering College, Perundurai, India
²UG Scholar, Department of Electrical and Electronics Engineering, Kongu Engineering College, Perundurai, India

*Email id: ranjithkkr7@kongu.ac.in

Abstract. The proposed system carries implementing some real-time modifications to the existing systems. It implies with providing an additional special character along with the 4-digit pin rather than the conventional ATM pin. The special character ensures the implementation of a special mathematical algorithm which creates a dynamic security pin during each transaction, making each transaction highly secure. While the transaction is initiated, a set of special characters is displayed in the ATM screen. The display carries our special character (provided with our security pin) along with the number of special characters. The count of the special character is to be noted and added along with the provided 4-digit security pin and entered. The importance of this algorithm is the count of the special character varies dynamically during every transaction. It creates a new security pin during each transaction. The security pin entered during a transaction is stored in the bank server safely. It adds up a safety feature that, if somebody illicitly captures our security pin and illicitly tries to enter it, it blocks the ATM and intimates the user. To help the blind person to access the ATM centres, a technique implemented for facial recognition and the transactions carry out securely. The facial recognition helps to initiate the transaction, following it the ATM provides voice command to help them to carry out the transactions with the braille keyboard.

Keyword: ATM, ATM PIN, Special Character, Blind People, Raspberry PI

1. Introduction

Automated Teller Machines (ATM’s) are introduced for the betterment and sophistication of the account holders to carry out transactions without any human disturbances and interventions. ATM’s can be accessed with the help of unique Plastic cards called as ATM cards in which magnetic strips are mounted which carries the account details of the customer. Each ATM card has a unique 4-digit pin to ensure safe transaction of the user[1], [2]. Although the ATM card carries numerous advantages, there existed a several flaws like stolen ATM cards, broken ATM cards, lost ATM cards, stolen ATM cards, stolen ATM pins and so on. Another serious problem existed with the old ATM cards, that the magnetic strips stores the user data in the static form, which is very much insecure. Hence, to overcome this, EMV chips are introduced. EMV chips supports dynamic data authentication, which makes it difficult to copy[3]. Although all the transactions are well monitored, and are carried out under safer circumstances, there...
are some issues regarding the ATM centres. Hackers and programmers use skimmers and other copy gadgets to steal card details and carrying out transactions illicitly[4] and [5]. A serious drawback in the ATM centres is that, even there are numerous technologies have been implemented in the ATM’s like dynamic PIN entry[6] and more than one security tools[7]. it is still difficult to prevent the hacking using shoulder suffering technique and the methodology of process for the blind persons to access ATM. Hence, to make ATM centres user-friendly for blind persons and to ensure the safety of the ATM users in safe handling of transactions, a new technology introduced in this paper to overcome above difficulties.

2. Block Diagram

Figure 1. Block diagram of this setup

As shown in Figure 1, setup consists of a Raspberry PI 3B+ Soc powered by using a 5V, 1 Amps DC power supply. The RFID tag and reader are used to initiate the transaction, while the RFID tag acts as the ATM card and the reader acts as the ATM card scanner [8]. The laptop acts as the visual output and the Wi-Fi network is used to update the transaction data to the bank server[9].

3. Algorithm and Process Flow

Step 1: Start the process
Step 2: Swipe the RFID card
Step 3: If the RFID matches go to step 4 else step 2
Step 4: Random special characters are displayed
Step 5: Count your special character and add with your password
Step 6: Enter the added password
Step 7: If the password is correct the process proceeds to step 8 else stops at step 10
Step 8: Enter the amount
Step 9: Cash arrives and the transaction is successful
Step 10: Stop the process.
Figure 2. Algorithm of the system

A new pin is generated by adding the old pin number with the number of special character as shown in figure 2. The proposed algorithm design is enhanced to use blind person also [10]. If blind people operate, the face detection process will take place. The entire process flow will follow the steps as shown in figure 3.

Figure 3. Process flow of the System

4. GUI Setup

The proposed system is a both hardware and software oriented setup which contributes the system in a 50-50 proportion [11]. The software setup of the system is designed as a Graphical User Interface (GUI)
manner to implement a user-friendly operation [12]. The GUI setup and the step-by-step operational procedures are shown below.

**Figure 4.** ATM display while initiating the transaction

This will be the first step of the ATM display, once the person enters into the ATM machine room. Figure 4 shows front view of the screen before initiating the process.

**Figure 5.** Special Characters section

As like shown in figure 5, once the ATM card is entered, the ATM screen now shifts to special characters section i.e. it shows a list of special characters along with our dedicated special character.

**Figure 6.** ATM Pin entry section
Followed by the special character screen, ATM pin entry screen is displayed as shown in figure 6. Once after noting the count of dedicated special security special character, it is to be processed by the special mathematical algorithm and new pin is entered in this section.

**Figure 7.** Two factor authentication section

One of the most sensible security features of our system is the two-factor authentication. Once after the ATM pin is entered, our second security feature i.e. the two-factor authentication arises. The OTP will be sent to registered mobile number to clear next level verification as shown in figure 7.

**Figure 8.** Amount withdrawal

After completing all the security measures, the next screen is shown to enter the amount as shown in figure 8. Here withdrawn amount value is to be entered.

**Figure 9.** Completion of Transaction
If sufficient balance is present in account, as shown in figure 9 the transaction proceeds and successful authentication message will be displayed.

Figure 10. Facial recognition methodology for blind people

To help the visually challenged people to access the ATM’s, a special security feature of facial recognition is added to their bank accounts [13]. Once after they entered their ATM card, the ATM identifies visually challenged person and switch ON the camera and starts capturing the person’s visuals as shown in figure 10. The captured visuals are processed and verified with the bank server[14],[15]. After the successful verification, the transaction window is open. The entire hardware assembly of the designed system shown in Figure 11

Figure 11. Hardware setup

5. Conclusion

This algorithm provides positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions. It helps to overcome the main drawbacks of misusing highly authenticated fingerprint security and reduce the use of skimmer. This system also helps the visually challenged persons to access the ATM centres as the normal people. The proposed second level authentication mechanism for ATM will increase customer satisfaction and give customers the peace of mind they need considering the high level of security applied to accounts.

References

[1] Bhosale S.T, Sawant B.S “Security in e-banking via card less biometric ATMs”, International Journal of Advanced Technology and Engineering Research 2012 2 4.
[2] Kwon T, Na S, “Switch PIN: Securing smartphone PIN entry with switchable keypads,” IEEE International Conference Consumer Electron, 2014 27–28.

[3] Biswas S, Bardhan Roy A, Ghosh K, Dey N, “A Biometric Authentication Based Secured ATM Banking System”, International Journal of Advanced Research in Computer Science and Software Engineering, 2012 24.

[4] Ojaswi K. Kasat, Umesh S.Charade, “Revolving Flywheel PIN Entry Method to Prevent Shoulder Surfing Attacks”, 3rd International Conference for Convergence in Technology (I2CT) 2018 1-5.

[5] Priyadharshini S, Kurinjimalar R, “Security enhancement in automated teller machine”, International Conference on Intelligent Computing and Control(I2C2) 2017 1-5.

[6] Jong-Hoon Kim, Gokarna Sharma, Irvin Steve Cardenas, Do Yeon Kim, Nagarajan Prabakar, S.S. Iyengar, “Dynamic PIN: A Novel Approach towards Secure ATM Authentication”, International Conference on Computational Science and Computational Intelligence, 2017 69-73.

[7] Shweta Sankhwar, "A Safeguard Against ATM Fraud", IEEE 6th International Conference on Advanced Computing, 2016 23-27.

[8] Tabitha V, Guarani Srikanth G, “Moving ATM Applications to Smartphones with a Secured Pin-Entry Methods”, IOSR Journal of Computer Engineering (IOSR-JCE), 2015 17 58-65.

[9] Yogesh Kisangani, Arti Mohanpurkar, “Advanced Pin Entry Method by Resisting Shoulder Surfing Attacks”, International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology, 2015 37-42.

[10] Taekyoung Kwon, Jin Hong, “Analysis and Improvement of a PIN Entry Method Resilient to Shoulder-Surfing and Recording Attacks”, IEEE transactions on information forensics and security, 2015 10 278-292.

[11] Mun-Kyu Lee, “Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry”, IEEE transactions on information forensics and security, 2014 9 695 -708.

[12] Kwon T, Shin S, Na S, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2014 44 716–727.

[13] Sunil Lo hiya “Biometric identification and verification techniques -A future of ATM Banking System”, Indian Streams Research Journal 2012 2 7-20.

[14] M. Sabarimuthu, N. Senthilnathan, M. A. Kumar, M. S. Kamalesh, V. Jayaprakash, and R. Srinivasan, "Fast and Integrated Chargers for Lithium Ion Batteries," IOP Conference Series: Materials Science and Engineering, 937 1-8

[15] Nilesh Chakraborty, Sam rat Mondal, “Colour Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack”, Proceeding of the 2014 IEEE Students' Technology Symposium, 2014 13–18.