IBBUL
Lapai Journal of Applied and Natural Sciences
LAJANS Vol 6(1): 231 - 235
SHORT COMMUNICATIONS

An OTP Model for Securing of Automatic Teller Machine (ATM) Transactions

***Oladipupo, E.T., Siyaka, O.H., Nzeako, C.B., Ataneh, C., Salihu, H.D. and Ekeh, O.J.**
Department of Computer Science, Federal Polytechnic, Bida, Nigeria,

ABSTRACT

The present use of pin and password provide only single security layer to the use of Automatic teller machine (ATM). However, if password/pin is compromised by the hacker, the ATM can be use for legitimate transactions by an imposter. In this research work, a model which introduces one more layer of security for securing ATM transactions in case password/pin is compromised is proposed. With this new layer, the hacker will not be able to carry out any transaction unless the OTP is provided. The working of the model is such that once a user inserts ATM card into the machine and type in the correct password and PIN, an OTP code is sent to the registered phone number during the collection of the ATM card. It is believed that if PIN/password is compromised, this second authentication measure will be very difficult to break.

Keywords: ATM, OTP, Password/Pin, Single, Double, Layer, Security, Mobile number

INTRODUCTION

An automated teller machine (ATM) is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller.

A one-time password (OTP), also known as a one-time PIN, one-time authorization code or dynamic password is a pin that is valid for only one login session or transaction, on a computer system or other digital device.

In present days, the ATM holds only one way to secure the money saved in the bank (pin), the pin is the only identity for someone to access the account when they have the card and correct password. Once the card is stolen by the culprit and if he/she comes to know the pin by any means then the culprit can take more money from the account in the shortest period, it may bring vast financial losses to the users. In the recent times, there have been many such ATM fraud cases. Due to some of the flaws in our present ATM system, we introduce the concept of one time password (OTP) in ATM banking. Our system will provide the second level of security using different factors to generate OTP. This will send over customer's mobile number stored in records. To secure ATM, user will have to register mobile and its IMEI number in bank system. When user puts/swipes card into machine, user get request to insert PIN (which is current way of ATM banking). In the proposed system user will get OTP on their mobile which will be send by the bank. When user enters OTP to the system, he/she will be having access to the machine else no transaction can be made. The bank database will hold information about a user's account details, mobile number which will improve security in ATM.

The current system does not have any other means of ATM security except for the use of pin or password, this leads to necessity of a new technique or instrument to deal with any possible attack that can lead to ATM fraud.

The need to ensure the security of money while carrying out the automation of banking services cannot be over-emphasized, which lead to the development of OTP as a way of enhancing security in ATM that will serve as the second layer of ATM security.

The basic aim of this research is to solve the single layer of the ATM and add an OTP as a double layer in ATM.

Received 02 November, 2021
Accepted 13 December, 2021
Address Correspondence to:
christypinmiloye@gmail.com

A proposed conceptual model that addresses concerns that face recognizability evaluation for ATM applications with exceptional occlusion handling which was proposed by (Eum, Suhr & Kim, 2000), the methodology used here was face recognition. In order to handle these problems, the proposed method facilitated the exceptional occlusion handling (EOH) process to handle both types of falsely evaluated cases. The EOH can be divided into two different approaches: 1) accepting the falsely rejected cases, 2) rejecting the falsely accepted cases. Humans have a diverse set of facial expressions which can reduce the accuracy of facial recognition software.

Furthermore, (Nagendrarajah, 2010) proposed a model to overcome this dilemma, where Principal Component Analysis (PCA) is used to extract a set of Eigen-images known as Eigen faces and weights of this representation are used for, recognition. This system stores only one image of the individual during enrolment phase since it is inconvenient to store more than one image of an individual from a commercial point of view (e.g. Immigration office). During this phase, the individuals are required to maintain a neutral expression and the hair is tied away from their face. The model is tested using a database of images of diverse nations like images of Chinese faces and English faces. This security system was accurate in recognizing enrolled individuals when they had spectacles on. However, this project is yet to recognize real occluded images.

Another researchers like (Coventry, Angeli & Johnson,2003) analysis and review the summary of the user centered aspect of the research they carried out over the last five years to understand attitudes towards the behavior with biometrics verification at the Automated Teller Machine (ATM) interface. They used the iris verification, for application at ATMs; a wide angle camera finds the head of the person to be identified. A zoom lens then targets in on the user's iris and takes a digital photo. A template of concentric lines is laid on the iris image and a number of specific points are recorded and the information converted into a digital template. This can then be compared with others for verification and identification purposes

Issues and Challenges in Two Factor Authentication Algorithms review by (Nath & Mondal ,2014) which lead (Shally1 & Aujla, 2014) to proposed the review of one time password (OTP) mobile verification , they make used of the hash form, Mobile Token process of authentication on the server which password that is sent to the client is identically equivalent passwords stored on the server. With security reasons infrequently server stores utilize passwords in plaintext form. Commonly, server stores utilize passwords in hash form so it cannot be returned in plaintext form and Mobile Token process of authentication on the server has a very critical time distinction.

Existing Model

There is no security that exists in the ATM card except PIN number, ATM card falling into wrong hands, and the PIN number being cracked by a stranger or imposter. Then stranger can easily use the ATM card in a legal way without being caught. The flowchart in Figure 1 illustrates the current model being used in a typical ATM transaction.

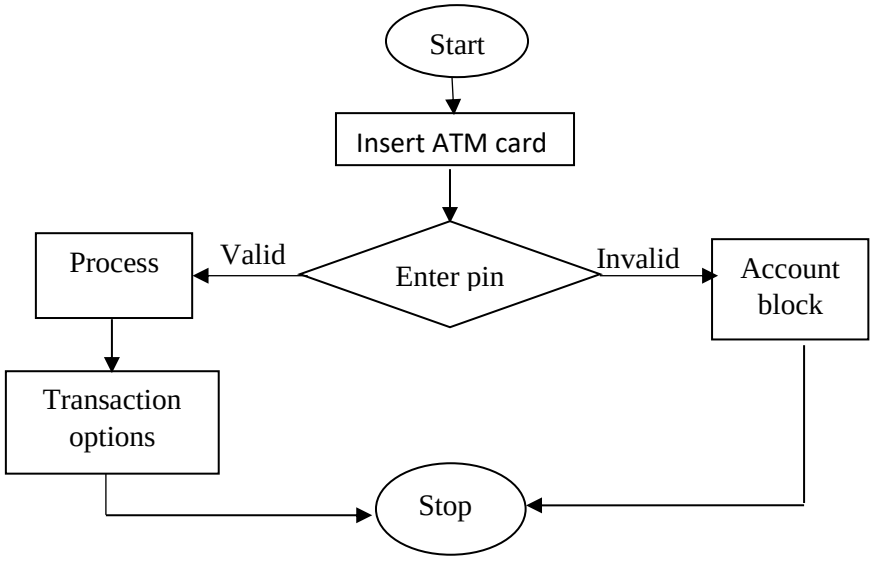

Figure 1: Flowchart of the exiting model

PROPOSED MODEL

This research introduce a double layer of security in ATM which is the OTP after the input of the single layer (pin/password)

A one-time password, also known as a one-time PIN, one-time authorization code or dynamic password is a password that is valid for a computer system or other digital device.OTP is a temporary data and does not belong to a database. In the SMS OTP authentication method, a onetime password (OTP) is sent with the SMS text to the user's phone. The user receives the OTP an8d enters it on the device where the authentication is happening. The OTP must be used within a specific time frame. Each customer's OTP is unique to that customer over series of transactions with an ATM.

OTP Format

The number of digits in the OTP: The default value is 6 codes.

Body: The text in the SMS that is sent to the user. The following structure describes the text in the

1. Bank name
2. Location of operation
3. OTP: One-Time Password
4. Operation: Name of the operation the user is trying to perform.

For example:

1. Bank Name: First bank Plc
2. Minna branch
3. OTP: 276450
4. User is trying to withdraw. Please approve it by using the OTP Security or call the bank for more information.

A flowchart in figure 2 illustrate the process involve in the proposed model.

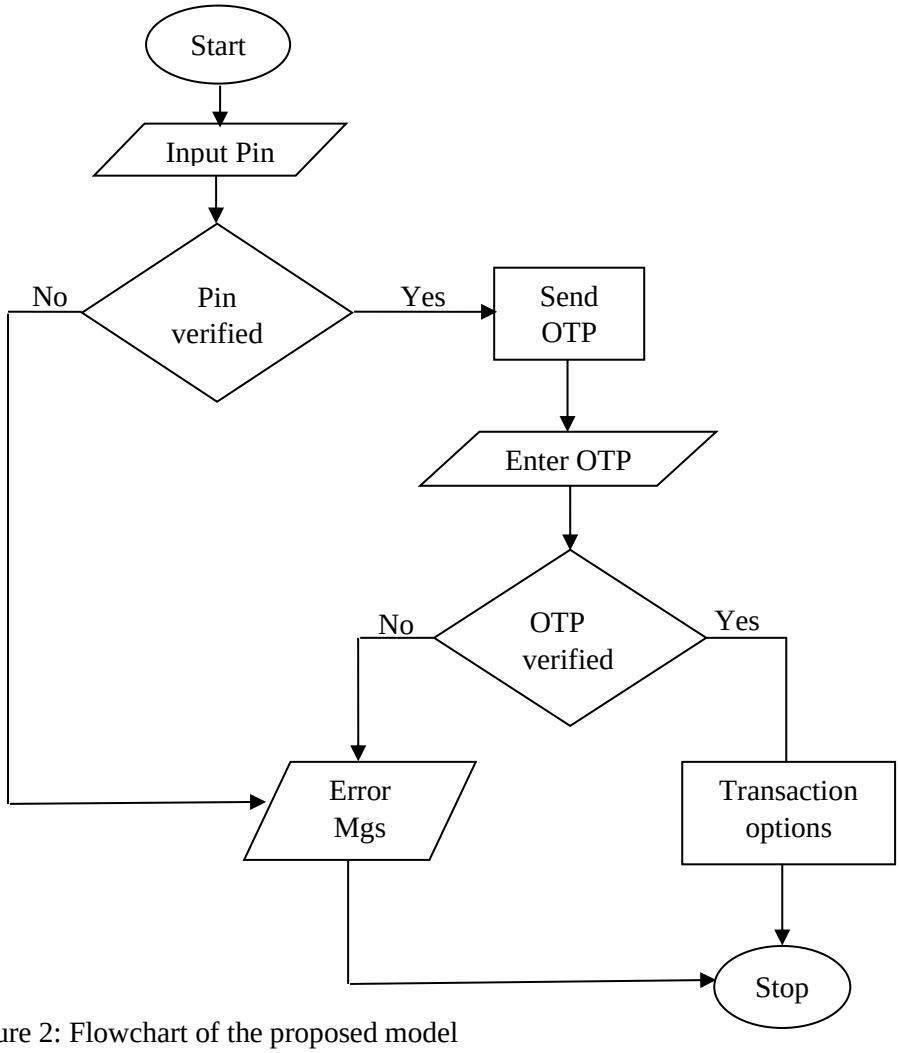

Figure 2: Flowchart of the proposed model

The Figure 2 shows the processes involved in the OTP

1. Start: indicate the first step the user will perform by inserting he/her ATM card into the ATM machine.
2. Input pin: indicate the step in which the user input he/her corresponding pin
3. Pin verified: indicate that the pin the user enter if it is valid or invalid
4. Send OTP: indicate the step which the bank will send the OTP to the user mobile number.
5. Error mgs: indicate that the pin and OTP is invalid.
6. OTP verified: indicate that the OTP code is valid before any transaction will be made.
7. Transaction option: indicate the withdrawal cash, transfer cash, account balance, change of pin.
8. Stop: indicate the last step the user perform be removing he/her ATM card.

Conclusion

This research topic is on the basis of more need of security in ATM banking system. Presently ATM is having less security with the single layer in the machine. In this research, we introduce a second security layer for accessing the ATM in an effective manner. If some unauthorized person uses the ATM card without the authorized owner permission, the hacker will not be able to make any transaction. One time password is send to the user's phone number after the pin is correct or verified, without the valid OTP code, there will no transaction. This model will give more security against ATM attack.

Suggestion For Future Work

In the future, this project can use a well enhance and more accurate equipments with better and more efficient ways to generate OTP and this model can be modified by providing space for invalid OTP codes.

REFERENCES

Answers. (2012). Automated Teller Machine. Available from http://www.answers.com/topic/automatic-teller-machine

Badmus, M. (2011). Nigerian Students and the ATM (Automated Teller Machines). [Online]. Available:http://www.upiu.com/other/2011/06/15/Nigerian-students-and-the-ATMAutomated-Teller-Machines/UPIU-3801308194612/

BBC News, (2012)."ATMs to operate without a card."

Bowen, J. (2010). How ATMs Work. [Online]. Available: http://money.howstuffworks.com/atm3.htm

Coventry, L., Angeli, A. & Johnson, G. (2003). "Usability and Biometric Verification at the ATM Interface." Advanced Technology and Research NCR Financial Solutions Division. Vol. 5, pp 153-160.

Croft, E. W. & Spencer, B. J. (2003). "Fees and surcharging in automatic teller machine networks: non-bank ATM providers versus large banks", 2003.

Eum, S., Suhr, J. & Kim, J. (2011). "Face Recognizability Evaluation for ATM Applications with Exceptional Occlusion Handling." In proceedings of Institute of Electrical and Electronic Engineers Conference on Computer Vision Recognition Workshops, School of Electrical and Electronic Engineering, Yonsei University, Republic of Korea, pp 82-89.

Hossain, R. (nd). et al., Designing an ATM Network Based on Distributed Database Systems".

Janarthany, N. (2010). "Recognition of Expression Variant Faces – A Principle Component Analysis Based Approach for Access Control" 978-1-4244-6943-7/10 ©2010 IEEE.

Khattri, V. Singh, D. K. (2019). "Implementation of an Additional Factor for Secure Authentication in Online Transactions," J. Organ. Comput. Electron. Commer, vol. 29, no. 4, pp. 258–273.

Kumar, K, S., Prasad, S., Semwal, V. B. & Tripathi, R. C. (2011). "Real Time Face Recognition Using AdaBoost Improved Fast PCA Algorithm," Int. J. Artif. Intell. Appl., vol. 2, no. 3, pp. 45–58.

Mohamed, M. A. J. K. & Sidi, F. (2000). "Strengthening User Authentication for Better protection of mobile application system," J. Theor. Appl. Inf. Technol., vol. 85, no. 3.

Mohan, R. & Partheeban, N. (2014). "Secure Multimodal Mobile Authentication Using One Time Password," Int. J. Recent Technol. Eng., vol. 1, no. 1, pp. 131–136.

Nath, A. & Mondal, T. (2014). "Issues and Challenges in two factor Authentication Algorithms" International Journal of latest trends in Engineering and Technology. Published January, 6(3): 318-327.

Obradovic, S., Tesic, D., Milanovic, D., Zoric, A., Perisic, D. (2012) @Protocols and programs in ATM Terminal Network", Telecommunications Forum(TELFOR),2012 20th edition.

Rai, A. R. (2008). "Customer relationship management: Concepts and cases " New Delhi, pp. 97-98

Rajesh, R. & Sivagnanasithi, T. (2009). "Banking theory: LAW & Practice," New Delhi, pp 313-314.

Robat, C. (2006). ATM Automatic Teller Machine. Available: http://www.thocp.net/hardware/atm.htm

Ross, B., Jackson, C., Miyake, N., Boneh, D. & Mitchell, J. C. (2005). "Stronger Password Authentication Using Browser Extensions, Proceedings" of the 14thUsenix Security Symposium.

Shally, G. & Aujla, S. (2014). "A Review of One Time Password Mobile Verification" International Journal of Computer Science Engineering and Information Technology Research. ISSN (P): 2249-6831, ISSN (E): 2249-7943. Vol. 4, Issue 3, 113-118 © TJPRC Pvt. Ltd.

Singh, S. K. (2009). "Bank Regulation". New Delhi, pp 169-170.

Venugopal, H. & Viswanath, N. (2016). "A robust and secure authentication mechanism in online banking," Proc. 2016 Online Int. Conf. Green Eng. Technol. IC-GET 2016, pp. 0–2.

Wikipedia the Free Encyclopedia. (2010). Automated Teller Machine. Available: http//:en.wikipedia.org.