cisdiJournal

Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 13 No. 2, June, 2022 - www.cisdijournal.net

Towards Developing a 4-Level Authentication Method for Securing ATM Cards

[1]Onamade, Akintoye Abraham, [2] Bambi Bunmi Janet & [3]Jenyo, Ifeoluwa
Department of Computer Science
Adeleke University
Ede, Osun State, Nigeria.
E-mails: [1]onamadeakintoye@adelekeuniversity.edu.ng, [2]bambibunmijanet@gmail.com
[3]ifejenyo@adelekeuniversity.edu.ng
Contacts: +234 703 066 7893[1], +234 806 718 3857[2], +234 806 005 0863[3]

ABSTRACT

In recent years, the rapid development of information and communication engineering has affected every aspect of human life. As a result, the manner in which banking activities are conducted has also changed. ATM cards have made banking easier worldwide; funds are easily accessed, transferred, and withdrawn without hindrances. The advancement in modern technology paved the way for the rapid increase in ATM card usage, which is directly proportional to the rate of fraud attached to it. Presently, ATM cards are seriously having security challenges, in the sense that it is only being secured by four digits ATM pin, which can be easily guessed by fraudsters. This paper discusses the current security issues faced by the users of ATM cards. It also proposes a 4-level authentication method that is solely on the use of ATM cards on POS terminals and Automated Teller Machines. In contrast, the online usage of ATM cards is being excluded. It is believed that if these levels of authentication are strictly adhered to, there will be a significant reduction in ATM cards fraud.

Keywords: Automated Teller Machine, Fraud, ATM Cards, Security

CISDI Journal Reference Format
Onamade, A.A., Bambi, B.J. & Jenyo, I. (2022): Towards Developing a 4-Level Authentication Method for Securing ATM Cards. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 13 No 2, Pp 11-.14.
Available online at www.computing-infosystemsjournal.info
CrossREF DOI No - dx.doi.org/10.22624/AIMS/CISDI/V13N2P2.

1. INTRODUCTION

The long waiting hours in the banking hall were drastically reduced with the introduction of Automated Teller Machines (ATM). ATM has made banking transactions more accessible and effective compared to the traditional banking system. To access an ATM, an ATM card is needed; without the ATM card, nothing can be done on the ATM. Because of the extensive database of transactions on the ATM, high-security protection measures are being implemented periodically to guarantee the operations of the ATM. At present, the ATM card is only secured by the unique four digits, which are only known to the owner of the ATM card. Once this personal identification number (PIN) is disclosed, anyone can use the ATM card and perform transactions with it. Transactions on the ATM cards could be carried on any ATM, Point of Sale (POS) Terminals or over the Internet.

A typical ATM card contains the following entities:

- The Expiration dates (it shows the expiry date of the card)
- Name of the cardholder (cardholder name is optional)
- The issuance date (the card issued date is optional)
- Manufactured company Logo
- Magnetic stripe
- The Debit card numbers (16 digits) (First 6 digits are the Bank Identification Number, and the rest ten digits are a Unique Account Number of the cardholder.)

* Bank Name
* Signature panel
* Network logo
* Smart Chip (contains owner's details)
* Cad Verification Value (CVV)

2. LITERATURE REVIEW

With ATM and ATM cards, you can withdraw cash, check your fund balance, transfer money to another user, recharge airtime and change the pin to a new one. Once a user inserts the ATM card into the ATM, the magnetic reader will scan the magnetic stripe to obtain the owner's information. 4 digits authentication pin is easier to remember when talking of memorability (De Luca, 2010). Sruthi (2019) did a study on ssecuring ATM with One Time Password, by providing a second level security to the use of ATM card; they proposed the addition of OTP to personal identification number (PIN). Jayandhi (2018) implemented an additional security features to the use of ATM pin code by using face recognition and QR code based OTP system. Validation of the face recognition pattern will send OTP to the user's phone number. This is good when there is network availability. Asoke (2019) designed a new technique to prevent skimming with the use of OTP only and eradicating ATM card PIN. Mithun (2018) implemented a bio-metric feature which is mainly fingerprint and OTP for ATM card security. Bhuvaneshwari (2019) also proposed the usage of ATM card with only OTP as a means of authentication. Sangeetha (2021) proposed the use of fingerprint only as a means of authentication for ATM cards. Joy (2021) did a systematic review by comparing different security measures that has been adopted and proposes face recognition or fingerprint identification and sensors to detects physical attacks along with PIN in various literatures. It was concluded that the traditional PIN verification along with either biometrics or IoT. But fingerprint is the most commonly used biometric technology.

3. EXISTING SYSTEM

An ATM is an automated system that enables customers to conduct financial transactions such as quick cash withdrawals, fund transfers, balance inquiries, and savings withdrawals from anywhere and at any time without the assistance of a branch representative or teller. Customers with this bank account are required to have a debit or credit card in order to use an ATM. The majority of people today prefer debit or credit cards to pay for their phone, electricity, and gas bills, among other expenses, because these cards provide immediate and easy access to their accounts. For this type of transaction, a swipe machine, also known as Electronic Data Capture (EDC), is used. Users need only to swipe their debit or credit card through the machine in order to pay for items or complete a transaction. Before completing a transaction, the magnetic strip on the card will encode all customer information. The machine reads the magnetic strip to verify the customer's card number, expiration date, and other information. Personal Identification Number (PIN) is an integral part of both ATM and EDC security schemes, as it is typically used to protect a user's financial information from unauthorized access. However, PIN alone has not been sufficient to ensure the security of the transactions. Biometric characteristics can be used to solve this type of issue. Fingerprints, which are located on the surface of the fingertips, are recognized as the most secure and reliable biometric characteristic (Mithun 2018). Since fingerprints are unique to each individual, they can be used as a reliable method of identification.

To increase security, the proposed model is based on biometric characteristics, security questions and message authentication technology. During an ATM transaction, a user's fingerprint is compared to their PIN in order to authenticate the user's identity. Due to the impossibility of duplicating biometric characteristics, such as fingerprints, this proposal can be a viable solution to the authentication issue. When making payment via swipe machine, the client will receive a confirmation message via GSM technology on the mobile number registered with the bank to authorize the transaction.

4. METHODOLOGY

A comprehensive review of the past literature that focuses on resolving ATM card fraud globally was done. While there are still loopholes, several suggestions have been made; then this study proposes a 4-level authentication method for securing ATM cards. As shown in figure 1, the user enters the ATM card into the machine, and the machine scans it and asks for the four-digit PIN; if the PIN is correct, the device will direct the user to the next stage, where the fingerprint will be scanned and verified. The system automatically sends an OTP to the user's mobile number; if the OTP did not arrive on time due to network, the user could generate this on the phone by dialing a USSD code. The last stage of verification is a security question to guarantee the card owner's carrying out transactions on the ATM card. This system will be a secure mechanism if followed.

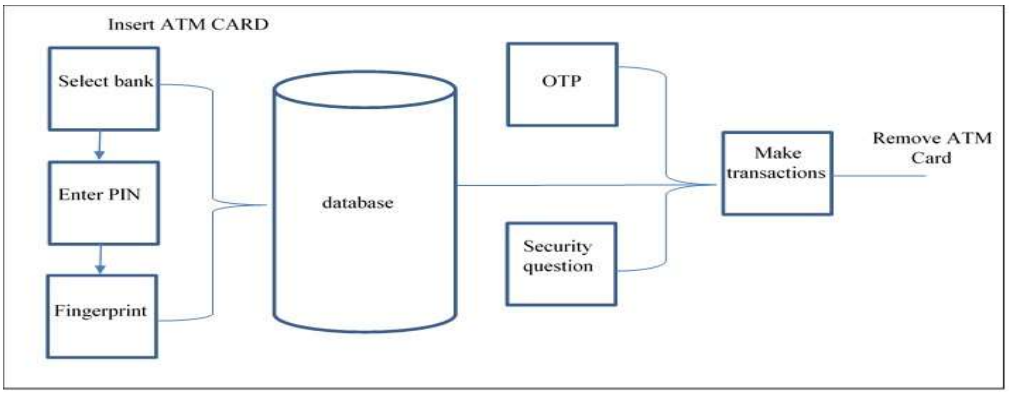

Figure 1: 4-level Authentication Model

4.1 Algorithm:

- User enters ATM card pin into the ATM
- If correct, proceed to validation
- Else send an error message
- Validate Fingerprint
- If a match, proceed to OTP
- Else alert the security
- Send OTP (user-generated with at least eight digits).
- If matched, proceed to Security Question
- Else send an error message
- Ask Security Questions
- If correct, proceed to transaction details
- Else, throw an error and quit

4.2 Recommendation

From the work reviewed so far, it is evident that several researchers have tried to secure the use of ATM cards in our society. Still, as they are working, the hackers, too, are working to bridge the security provided. Hence the need for more research work in this area. This paper is proposing that the security level for protecting ATM cards should be increased; below are the proposed 4-level authentication methods for securing ATM cards:

1. ATM card pin: the traditional method, the 4digit pin, should not be removed. Users will be prompt to enter their PINs before making transactions.
2. Fingerprint: the fingerprint will be verified before proceeding
3. OTP (user-generated with at least eight digits) either through the User's Phone or email address. Then the OTP will be User-generated to avoid network glitches.
4. Security Question: the fourth phase adds security questions for authentication.

The system will improve the security of ATM cards with the above authentication processes and is cost-effective.

5. CONCLUSION

ATM card security is critical because it involves funds. A principal key serves as an umbrella for others with all the protection above measures. This is the User's Mobile number. With different dialed codes, either NIN, BVN, OTP or ALERT SMS can be gotten on a personal mobile number. Nowadays, fraudsters are after mobile numbers that have been linked with Bank Verification Number (BVN) because this is the source to get any other information needed in carrying out fraudulent activities. Therefore, special attention should be drawn to securing the mobile numbers attached to banking details; if stolen, all valuables are gone except its blocked by the network provider immediately.

REFERENCES

1. Asoke, N. (2019): Enhancing Security Of ATM Transactions Via Debit Cards. *International Journal of Computer Science and Engineering*, Vol. 7, Issue 9.
2. Bhuvaneshwari, N. (2019): Enhancing Security Of ATM Transactions Via Debit Cards, *International Journal of Computer Science and Engineering(IJCSE*), Volume 7, Issue 9.
3. De Luca, A., Langheinrich, M., & Hussmann, H. (2010): Towards understanding ATM security: a field study of real-world ATM use. *Proceedings of the sixth symposium on usable privacy and security* (pp. 1-10).
4. Jayandhi, G. (2018): Secure Pin Authentication as a Service for ATM, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 7, Issue 3.
5. Joy, A. (2021): A Systematic Review Comparing Different Security Measures Adopted in Automated Teller Machine. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(13), 388-393.
6. Mithun, D. (2018): ATM Card Security Using Bio-Metric And Message Authentication Technology, *IEEE International Conference on Computer and Communication Engineering Technology*, pg 280-285.
7. Sudharsan, K., Kumar, V. A., Venkatesan, R., Sathyapreiya, V., & Saranya, G. (2019): Two Three Step Authentication in ATM Machine to Transfer Money and Voting Application. *Procedia Computer Science*, *165*, 300-306.
8. Sangeetha T, Kumaraguru M, Akshay S., & Kanishka M. "Biometric based Fingerprint Verification System for ATM machines", *Journal of Physics: Conference Series* 1916 (2021) 012033
9. Sruthi, M. (2019): Secure And Smart Future ATM with One Time Password, *International Journal of Engineering Science and Computing*, Vol. 9, Issue 4.