A Systematic Review Comparing Different Security Measures Adopted in Automated Teller Machine

Anjalin Joy[a], Caren Babu[b], D Abraham Chandy[c]
[a]Sahrdaya College of Engineering and Technology, Kodakara, Kerala, India
[b]Sahrdaya College of Engineering and Technology, Kodakara, Kerala, India
[c]Karunya Institute of Technology and Sciences, Coimbatore, India
[a]anjalinjoy007@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: The automated teller machines (ATM) uses are increasing day by day. Majority of the population uses ATM cards for shopping and cash withdrawal from ATMs. Along with increasing use of ATM cards the numbers of ATM thefts are also increasing worldwide. Majority of the ATM thefts are by manipulating or cloning the card. The incidences of physical ATM attacks by breaking into the ATM are also increasing worldwide. The securities of the customers are important in ATM transactions. The customers are protected from both physical and fraudulent ATM attacks by enhanced security measures provided by the bank. Majority of the ATMs provide fraud attacks by using a valid ATM card and PIN which could be easily identified and manipulated resulting in thefts. This paper discusses about the enhanced security measures implemented like face recognition, fingerprint identification, sensors to detects physical attacks along with PIN in various literatures. The merits and demerits of each security systems are compared.

Keywords: ATM, card verification, face recognition, password verification, fingerprint verification.

1. Introduction

Automated teller machine (ATM) allows people to do online transactions, shopping, checking bank balance and cash withdrawals without going to the bank. There are now more than one ATM per 3000 persons across the world. It was discovered by John Shepherd-Barron from UK. In India, first ATM was installed by Hongkong and Shanghai banking corporation (HSBC). ATM service is one of the most important facilities provided by the banks worldwide to its customers. Banks provide ATM facilities to provide easy availability of money to customers any time and to reduce their own working cost by reducing staffs to make cash transactions available for customers. In the present busy world people don’t have enough time to wait in banks for banking transactions and so the banks improved customer satisfaction [25] by providing electronic banking [1]. The increase in the number of ATMs made cash transactions easy for common man. But it’s running and maintenance results in difficulties for banks. Banks usually employs third parties to fill cash and provide maintenance and security [3]. Majority of the population uses ATM card for online transactions, shopping, cash withdrawals and checking balances of their account without going to their bank.

In traditional ATM systems transactions are authorized using customers card and personal identification number (PIN). The transaction is authorized only when they entered PIN matches the data in the server. On the other hand, as majority of the population are using ATM cards, the numbers of ATM thefts are also increasing worldwide. The details of the ATM cards like card number, CVV and PIN are saved in majority of the online shopping sites which may also increase chances of theft if the details are known to another person. Nowadays PIN can be scanned or hacked [8] easily by using scanning devices or video cameras. ATM thefts usually occur by putting duplicate cards into the ATM slots and machine is not able to read the original card when it is inserted. So the machine asks to enter the PIN and the other person watches the PIN from behind. The customer will stop the transaction thinking the ATM swallowed the card. The thieves empty your account with the plastic sleeve completely. Since most of the customers are not familiar with ATM transactions they may not remember the PIN. Therefore people are reluctant to use ATM because of the chances of losing their money if their card is lost or PIN is identified. The incidence of physical ATM attacks by digging tunnels beneath the ATM, breaking into ATMs and using explosives are reported worldwide. Since the incidence of ATM robberies, physical attacks and ATM password hacking are increasing day by day, technology has to be developed to overcome this problem.

The ATM security is affected significantly if either the card or PIN is manipulated by frauds. So the ATM security has been increased by the bank to provide secure customer transactions. The main purpose of ATM security is to increase security against ATM frauds. So, to get rid of these security issues the efficient method is to combine the traditional PIN verification with biometric security and Internet of Things (IOT). In this present era by combining technologies like IoT and biometrics, ATM services become much more advanced, safe and user friendly. This paper identifies and compares different ATM security measures and analyzes the merits and demerits of each system and proposes a multilayer enhanced security system for the ATM counter and transactions.

2. Traditional ATM Security Measures

The traditional ATM system works when a customer inserts a valid card and enters the correct PIN which helps to identify the authorized users and avoid fraud transactions. In card verification stage authorization is allowed only after inserting a RFID (Radio-frequency identification) into the ATM machine. For authorizing the RFID Card [3], RFID Reader is used. After checking it with existing data, if both the data matches it will move to next stage. In this stage various security measures like PIN, face, fingerprint, alert indication, location tracing, IoT sensors etc are used. If data don't match it will exit the system as shown in fig. 1. But this security alone cannot prevent the increasing number of ATM frauds and physical attacks.

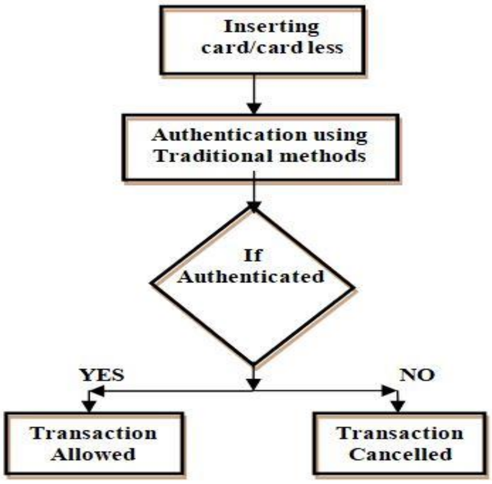

Fig. 1. Architecture flows of traditional security system.

Different literature review suggested various additional technologies to tackle these problems which are discussed below.

1.1 Face Recognition Technology

Face recognition is done by camera place at the door of ATM counter [2]. The face detection is done by either biometric technique or computer application which recognizes the customer from image or video frame. The door will open only if the face is detected. The detection is accomplished by using techniques like blurred human shapes or skin tones. Face recognition is done by using Haar cascade classifier for face recognition to increase ATM security [3]. The facial detector is applied on each frame of the captured image. Then a recognition model of the face is built from the frame using local binary pattern histogram (LBPH) and it is recognized.

1.2 Fingerprint Verification Technology

The fingerprint detected by the sensor is scanned for the biometric trait in the template database [4]. In the decision module the similarities in the matcher module is checked and authorization is granted.

1.3 Internet of Things (IoT) Technology

The physical ATM attacks can be prevented by using IoT techniques [2]. In this paper temperature sensor, vibration sensors (SW-420, Comparator LM393) and tilt sensors are used. If any one of the above sensors records value more than the threshold, an alert will be send through face book or twitter by using IoT techniques. The system will work by using Arduino (ATmega 328) [23].

1.4 Global Positioning System (GPS) and Global System for Mobile Communication (GSM) Technology

ATM attacks can also be reduced by using GSM and GPS technology [5]. If ATM is tampered an SMS will be send to the main controlling station through GSM. If cash box is robbed it can be tracked by using GPS.

1.5 OTP Verification

The transactions can also be authorized based on OTP verification [3]. The transactions are authorized only after confirmation of the message by the user which may be a onetime password (OTP) or confirmation message. The OTP is send by using GSM technology.

1.6 Card less Transactions

ATM transactions are done without using ATM cards by combining IoT and computer vision for enhancing ATM security [3]. Transactions are authorized on the basis of face recognition, fingerprint verification and OTP authentication without ATM card and PIN.

3. Discussions

The different methods of enhancement of ATM security system compared to the traditional ATMs in various literature papers are analyzed and discussed in the Table 1. A traditional ATM security system uses only ATM card and PIN to provide safe ATM transactions. Since the incidences of ATM attacks are increasing worldwide various literatures suggest different technologies to increase ATM security. The different technologies suggested include face recognition [9], fingerprint verification, OTP authentication, and smart phone applications to prevent electronic theft. The physical attacks can be prevented by using temperature sensor, vibration sensor or tilt sensor with IoT technique. The other technologies used include GPS and GSM technology. Even transactions without using ATM cards were proposed to increase security. The merits and demerits of different literature papers are discussed. The technologies used in this paper are ATM card, PIN and Smartphone for ATM security [1]. The merits of this system are that it will prevent ATM skimming and remote fraud even if card and PIN is not available by using smart phone technology. The demerits of the system are that ATM transactions cannot be completed if Smartphone is not working. The technologies used in this paper are ATM card, PIN, face recognition, temperature sensor, vibration sensor, tilt sensor and IoT technique [2]. The merits of this system include different sensors which are accurate and easily available. It will also prevent both physical and electronic theft. The demerits of the system are that, system will not capture and store photos and videos during suspicious activity.

Table1.Comparision results of the different ATM security systems

	Card/ Card less	**Traditional methods Used**						**Types of ATM Security**	**Merits**	**Demerits**
		PIN	**Face**	**Fingerprint**	**Alert Indication**	**Location Tracing**	**IoT Sensors**			
[1]	Card	Yes	Yes				Yes	Protection against electronic theft.	Prevent ATM skimming and remote frauds.	Working Smartphone is required.
[2]	Card	Yes	Yes				Yes	Protection against both electronic theft and physical attacks.	Sensors are accurate and easily available.	Captured photos or videos not stored
[3]	Card less	No	Yes	Yes	Yes		Yes	Protection against electronic theft.	Easy, fast and card less transaction.	Face recognition is less accurate.
[4]	Card	Yes		Yes				Protection against electronic theft.	Fast and secure.	Fail to identify the fingerprint. Direct contact causes hygienic problem.
[5]	Card	Yes		Yes	Yes	Yes	Yes	Protection against both electronic theft and physical attacks.	Secured and authenticated Transaction.	Manipulation and unauthorized entity can occur during transaction.
[6]	Card	Yes						Protection against electronic theft.	Cost effective.	Limited capacity in individual user transactions.

The technologies used in this paper are Face recognition, fingerprint verification, OTP authentication, computer vision and IoT technique [3]. The merits of this system include easy, fast and card less transactions in ATM counter. The demerits of the system are less accuracy of the face recognition technique. The technologies used in this paper are ATM card, PIN and fingerprint verification [4]. The proposed system is fast and secure. The demerits of the system are its failure to identify the fingerprint in some cases. There is a chance of card duplication in some cases. And also it causes hygienic problem as direct contact is required. The technologies used in this paper are ATM card, PIN, IR sensor GPS, GSM and fingerprint verification [5]. The merits of this system are secure and authenticated transactions. The demerits of the system are that it can be manipulated and can cause an unauthorized entity doing the transactions. The technologies used in this paper are ATM card, PIN, remote ATM video surveillance using M2M technology [6]. The merits of this system are its cost effectiveness and make ATM safe from intruders and thefts. The demerits of the system are its limited capacity when coming down to the individual user transactions.

On the basis of analyses of different literatures it was concluded that none of the system provide total security from both electronic theft and physical attacks. This research helps to compare different concepts which can be added to the traditional ATM security [10]-[17] to provide a safe and secure ATM system. This research may also help in future to develop a multilayer ATM security system. Based on the analysis we would like to suggest a system in the future which can increase ATM security [24] by combining technologies like ATM card, PIN, face recognition, fingerprint identification, and GSM technology to reduce chances of electronic theft. Physical attacks can be prevented by adding IoT based techniques which include the use of sensors to detect changes in temperature and humidity. So by combining above technologies both electronic theft and physical attacks can be prevented.

4. Conclusions

In this literature review different method of ATM security measures were analyzed and compared. The recent trend is to combine the traditional PIN verification along with either biometrics or IoT. But fingerprint is the most commonly used biometric technology [18]-[22]. The combination of various techniques ensures that ATMs are secure from different attacks. The various methods discussed in this paper are yet to be implemented. Some of the systems are cost efficient but others are not. Therefore it is necessary to design and implement a method that is least expensive and provide multilayer security. In the future we can increase ATM security by combining technologies like ATM card, PIN, face recognition [7], fingerprint identification [12], and GSM technology to reduce chances of electronic theft. Physical attacks can be prevented by adding IoT based techniques which include the use of sensors like temperature sensor, humidity sensor and MEMS sensor. So this novel methodology helps to prevent both physical and ATM related fraud attacks.

References

1. Embarak, O.H., 2018, November. A two-steps prevention model of ATM frauds com-munications. In 2018 Fifth HCT Information Technology Trends (ITT) (pp. 306-311). IEEE.
2. Jacintha, V., Nagarajan, J., Yogesh, K.T., Tamilarasu, S. and Yuvaraj, S., 2017, December. An IOT Based ATM Surveillance System. In 2017 IEEE International Conference on Com-putational Intelligence and Computing Research (ICCIC) (pp. 1-6). IEEE.
3. Hazra, S., 2019, March. Smart ATM Service. In 2019 Devices for Integrated Circuit (De-vIC) (pp. 226-230). IEEE.
4. Das, S. and Debbarma, J., 2011. Designing a biometric strategy (fingerprint) measure for enhancing atm security in indian e-banking system. International Journal of Information and Communication Technology Research, 1(5).
5. Nelligani, B.M., Reddy, N.U. and Awasti, N., 2016, August. Smart ATM security system using FPR, GSM, GPS. In 2016 International Conference on Inventive Computation Tech-nologies (ICICT) (Vol. 3, pp. 1-5). IEEE.
6. Raj, M.M.E. and Julian, A., 2015, March. Design and implementation of anti-theft ATM machine using embedded systems. In 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015] (pp. 1-5). IEEE.
7. Gusain, R., Jain, H. and Pratap, S., 2018, February. Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology. In 2018 3rd International Con-ference On Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-5). IEEE.
8. Wang, C., Guo, X., Chen, Y., Wang, Y. and Liu, B., 2017. Personal PIN leakage from wear-able devices. IEEE Transactions on Mobile Computing, 17(3), pp.646-660.
9. Winoto, A.S., Kristianus, M. and Premachandra, C., 2020. Small and slim deep convolutional neural network for mobile device. IEEE Access, 8, pp.125210-125222.
10. Sankhwar, S. and Pandey, D., 2016, February. A safeguard against ATM fraud. In 2016 IEEE 6th International Conference on Advanced Computing (IACC) (pp. 701-705). IEEE.
11. Rupanagudi, S.R., Ranjani, B.S., Bhat, V.G., Surabhi, K., Reshma, P.R., Shruthi, G., Sarayu, K.P., Sangeetha, R., Rao, B.R. and Vasanti, S., 2015, September. A high speed algorithm for identifying hand gestures for an ATM input system for the blind. In 2015 IEEE Bombay Section Symposium (IBSS) (pp. 1-6). IEEE.
12. Nawaya, J.J., Jemimah, N. and Oye, N.D., 2019. Designing a Biometric (Finger) Using Mul-tispectral Imaging Biometric Authentication Measures for Enhancing ATM Security in Ni-geria.
13. Rasiah, D., 2010. ATM risk management and controls. European Journal of Economics, Fi-nance and Administrative Sciences, 21(2014), pp.161-171.
14. Rasanayagam, K., Kumarasiri, S.D.D.C., Tharuka, W.A.D.D., Samaranayake, N.T., Sa-marasinghe, P. and Siriwardana, S.E., 2018, December. CIS: An Automated Criminal Iden-tification System. In 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS) (pp. 1-6). IEEE.
15. Balwir, S.P., Katole, K.R., Thakare, R.D., Panchbudhe, N.S. and Balwir, P.K., 2014. Secured ATM Transaction System Using Micro-Controller. International Journal of Advanced Research in computer science and software engineering, 4(4).
16. Ajaykumar, M. and Kumar, N.B., 2013. Anti-theft ATM machine using vibration detection sensor. international journal of advanced research in computer science and software engi-neering, 3(12).
17. Maiti, S., Vaishnav, M., Ingale, L. and Suryawanshi, P., 2016. ATM robbery prevention us-ing advance security. Int Res J Eng Technol (IRJET), 3(02), pp.2395-0056.

18. Oko, S. and Oruh, J., 2012. Enhanced ATM security system using biometrics. International Journal of Computer Science Issues (IJCSI), 9(5), p.352.
19. Jebaline, G.R. and Gomathi, S., 2015, March. A novel method to enhance the security of ATM using biometrics. In 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015] (pp. 1-4). IEEE.
20. Onyesolu, M.O. and Ezeani, I.M., 2012. ATM security using fingerprint biometric identifer: An investigative study. International Journal of Advanced Computer science and applica-tions, 3(4), pp.68-72.
21. Padmapriya, V. and Prakasam, S., 2013. Enhancing ATM security using fingerprint and GSM technology. International Journal of Computer Applications, 80(16).
22. Kassem, M.A., Mekky, N.E. and EL-Awady, R.M., 2014. An enhanced ATM security sys-tem using multimodal biometric strategy. International Journal of Electrical & Computer Sciences, 14(4), pp.9-16.
23. Saranraj, B., Dharshini, N.S.P., Suvetha, R. and Bharathi, K.U., 2020, March. ATM security system using Arduino. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 940-944). IEEE.
24. Hooda, K., 2016. ATM security. Int. J. Sci. Res. Publ, 6(4), pp.159-163.
25. Kumbhar, Vijay. "Factors affecting on customers’ satisfaction an empirical investigation of ATM service." (2011): 144-156.