# EFFECTIVENESS OF ATM SECURITY MECHANISMS: A REVIEW ANALYSIS

**M.J.A. Sabani[1] & U.M. Rishan[2]**

Correspondence: mjasabani@seu.ac.lk

## ABSTRACT

In the modern hasty word, Banks and ATM (Automated Teller Machine)s are inevitability possessions of all humans. With the use of ATMs people can do several financial transactions and related activities day to day life. The common authentication mechanism uses in ATM is card with PIN (Personal Identification Number) for the secure transactions since long time ago. But nowadays cause of the higher advancement in technology tends alert and fear among banks and ATM users thus it is important to overcome the problem to safe ATM activities. In this study, analyzes the recent and popular authentication mechanisms related to ATM security and recommends better solution from the past studies to increase ATM security in the process of authentication and to protect from illegal physical activities at the ATM. This study compares different combination of authentication mechanism including the classical PIN method and recommends the best solution by weighting four important attributes namely security Performance, Accuracy, Cost and Flexibility in terms of security. Based on the total score weighted from the comparison this study recommends a secure solution as a combination of two methods from the past studies. A two-step verification method with "PIN and Fingerprint or S-code (Secure-code) with OTP (One Time Password)" was identified as the best solution for authentication since its higher security and flexibility to the users, meanwhile another mechanism with "GPS and sensors" was recommended for the protection against the illegal physical activity and for providing post- tracing capability.

**Keywords:** ATM, security, authentication, two-step verification, OTP.

## INTRODUCTION

In this modern digital era, security and privacy are very important for every individual on everywhere in this world. Because of the rapid advancement of science and technology and its challenges against the security and privacy, upcoming developments are being developed with solid security solutions. Be that as it may, then again, dangers are likewise being presented to breach these security levels. In spite of the fact that improvement in automation has a constructive outcome generally speaking, yet different money related firms like banks and its applications like ATM are still exposed to burglaries and cheats.

Persistently expanding number of challenges to the security of banking information in automated banking frameworks prompts a diminishing in the nature of banking administrations given by banks at the national and universal dimension, paying little respect to their type of proprietorship. Therefor it is essential that give a superior security frameworks to the Banks and ATM

[1] Department of Information and Communication Technology, South Eastern University of Sri Lanka,
[2] Department of Information and Communication Technology, South Eastern University of Sri Lanka,

administrations for shielding individuals' money and different stuffs from burglaries and fraud.

The aim of this study is to analyze the security systems of Banks and ATMs in contemporary and find the advantages and disadvantages of those security systems as well as find out or recommend secure systems for those services.

## METHODOLOGY

This study was carried out from the facts on different articles related to the security aspects of banks and ATM services. The common security risks were identified and compared different security measures published in several studies.

Security measures were tabularized in terms of its cost, performance, flexibility and accuracy, and they were compared using ordinal data values to identify efficient method.

A scoring scheme given below was used to weight the attributes to compare with numerical evidence. The allocated weight for each attribute were varied based on their security importance as that the Performance and Accuracy are more important than the Cost and Flexibility.

### *Score scheme for attributes*

Performance (0-12)

Very High (VH) - 12　High (H) - 9　Medium (M) - 6

Low (L) -3　Very Low (VL) – 0

Accuracy (0-8)

Very High (VH) – 8　High (H) - 6　Medium (M) - 3

Low (L) -0

Cost (1-5)

Very High (VH) - 1　High (H) - 2　Medium (M) - 3

Low (L) - 4　Very Low (VL) - 5

Flexibility (1-5)

Yes (Y) -5　No (N) -1

Based on the comparison an efficient solution to authenticate and protect ATM services was recommended.

## ATM FRAUD METHODS

Most of the banks offer a number of financial and non-financial prominent services through ATM. While providing financial services such Cash Withdrawal, Utility Bills Payment and Inter (and Intra)-bank Fund Transfer, etc. they provide non-financial services such Balance Enquiry, Mini Bank Statement, PIN Change, etc. (Shaikh & Shah, 2012)

Nowadays ATM fraud is very common and different methods were used to do these illegal activities, some of the common and frequently used methods are Card Skimming, Card/Cash Trapping and Transaction Reversal Fraud (TRF).These methods could be achieved through different tools and techniques such shoulder surfing, hidden camera, Skimmers and keypad overlays (Sankhwar & Pandey, 2016).

### Shoulder Surfing:

The activity of observing the PIN while entering to the ATM by the authorized person. More number of ATM machines kept in a single room gives more opportunity for such activities. Also this technique could give chance to observe many information of the card holder such name, CVV, card number, expiry date

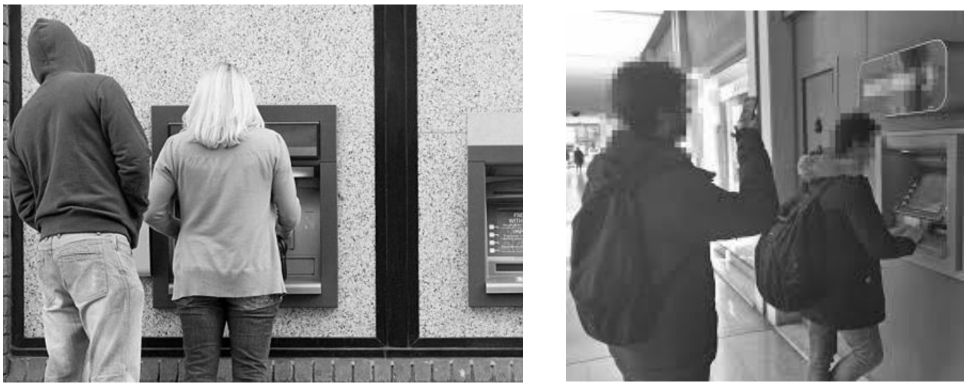

*Figure 1. Shoulder Surfing Technique (Model pictures fetched on Google image search)*

### Hidden Camera:

PIN of a card can be caught using different types of imaging gadget such camera and camera focal points. This is well-known technique used nowadays by fixing a hidden and tiny imaging devices in appropriate place.

### Skimmer and keypad overlays:

Skimming is a strategy utilized by the programmers/ hackers to catch secret information from the magnetic strip of the ATM card to get personal information to use along with the PIN. Using the keypad overlay keystroke of the PIN can be recorded and stored for later use.

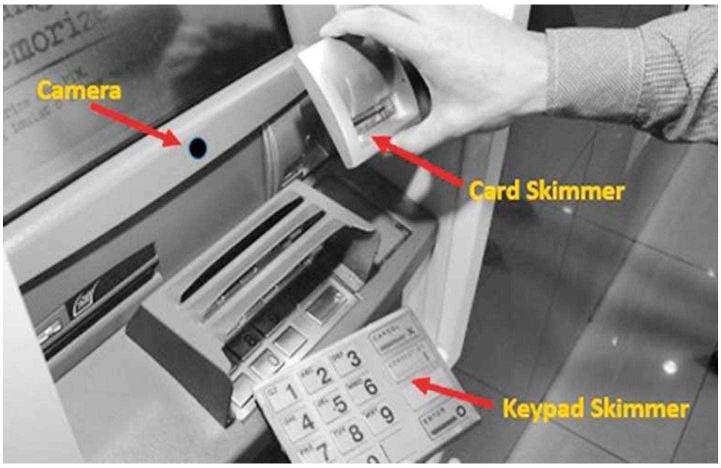

*Figure 2. Hidden Camera, Skimmer and Keypad overlay methods (Model picture fetched on Google image search)*

This study is carried out to analyze and compare the effectiveness of the ATM Security from different studies.

## LITRATURE REVIEW

There are many researches had been done related to the security of the Banks and its applications such ATM service, online banking, etc. It can be understood that nowadays, most of the security systems provide two or more factor authentication to increase the security.

From an earlier study it was identified that reduces the PIN's insufficient security problem can be replaced by the computer generated number with biometric security (Bhosale, 2014).

It was reported that biometric authentication is a process or ability of individual to prove his or her own identity using biometric input or authenticate ourselves in case of ATM transactions (Jebaline & Gomathi, 2015) . And also it mentioned that include the biometric authentication with PIN will increase the security of ATM and reduce the chances of PIN forgery (Jebaline & Gomathi, 2015).

In this era Biometric applications has turned out to be increasingly well known and is utilized for individual distinguishing proof in ATM frameworks (Nelligani, Reddy & Awasti, 2016).

Biometric systems are considered as improved authentication methods in security systems for such ATM and Banking systems, even though it is improved, it has some drawbacks and disadvantages as well. It needs huge storage or information base to store data, It has been discovered some issues while authenticating and these type of authentication systems need great speculation and support costs (Ray, 2015).

It was identified that in case of biometric technologies Iris and Retina always have its higher performance of security when compared with face detection and fingerprint. Accuracy and stability also very high in both methods comparing with face detection and fingerprint techniques. Meanwhile fingerprint provide higher stability and medium Accuracy, but with lower cost (Karovaliya, Karedia, Oza &. Kalbande, 2015). Also they have suggested a system that working with one time password (OTP) and facial recognition techniques. In that system user first need to swipe the particular card and the camera at the bank recognize the face of that particular person from the database. If the face matched with the database then a onetime password will send to that person’s phone. The person can do ATM relevant work using the OTP. In case if camera found more than one person at the room it will block the account for security purpose. So it will be an affective system for getting more accurate security level in ATMs (Karovaliya, et al., 2015). In addition to that OTP, the system generate it with a random number generator technique and uses MD5 hashing technique for integrity as well.

A study was identified another security system for ATM by using Biometrics and OTP. In that system particular person must use the PIN at the ATM, once the person authenticated with the PIN the ATM will give two options to select either OTP or Biometric. By selecting OTP person will get a message via phone. Or else person can use Finger print to access ATM activities (Hamid, 2015). This is somewhat better option when compare with traditional PIN only system and also it provide flexibility like giving fingerprint option in case of problems in phone.

A method was found that work with Palm Vein Biometric Technology to protect against ATM issues. This system also uses two way verifications system by Palm Vein Technology and user identification number (UIN). Bank gathers the UIN when user creates account into particular bank and when they want to use the ATM they need to scan their hand with palm sensor and then it will check the palm Vein and UIN. The transaction can be possible only if they matched, otherwise it will be rejected (Prasanthi, Hussain, Kanakam & Chakravarthy, 2015). This is also a better solution than normal PIN authentication, but the disadvantage is there is no any alternative way in an emergency situation because of uniqueness and pattern matching problems.

In another security system, user initially needs to use his or her card and PIN for first step verification. Once it succeeded then it move to second step verification. In the second level verification the face image should be matched with user repository image in the bank then transaction could be started, if it is not matched then it will hold the card inside the ATM and send the message to bank staffs (Kibona, 2015). Even though it uses two step verification the chance of failure could be high since it comparing with images in the repository and also it will block the card in the ATM.

A study suggested a security system for preventing ATM robbery. This system uses many sensors and GPS system. First sensor place at the door entry point which prevent more than one entry of ATM user and other sensor placed at ATM which has two sensors namely, vibrate and motion sensors. These sensors sense the damage or any unwanted physical activities at the ATM. Finally GPS placed in ATM which will be used to send the location of particular ATM. In case of any uncomfortable entry or any other illegal issues happened at the ATM the doors will be locked (Maiti, Vaishnav, Ingale & Suryawanshi, 2016). In this method in addition to traditional method they have used multiple techniques to increase the protection, but it seems that more complex when compare with other method. But it is very useful to trace and catch the persons involved in the illegal activities.

It was found that here is a proposed a system with three-tire authentications. This system starts with registration of banking activities. The user of this Bank must register at the bank along with fingerprint and mobile number through banking staffs. Once the user wants to do a transaction he/she must use the card and need to provide the PIN first. Once it is authenticated the person need to use fingerprint and it must match with bank database, as the third step OTP will send to the user’s phone as the final authentication to initiate the transaction process (Onyesolu & Okpala, 2017). This is more secure than other models meanwhile it’s a time consuming method.

Another system was suggested with finger print and GSM feedback model. In this system user wants to register the bank account and want to give the fingerprint to particular bank. The Bank will give an s-code (secret code) for the specific user. When the user wants to access the ATM he/she want to enter PIN of ATM card then it moves to the second step verification. In second step there are two ways. In first way user must use fingerprint, if that match with database then able to do transaction. If fingerprint not work in case of any issues then user must enter s-code to the ATM and it will send OTP to user’s phone, using that user can do the transaction process. If s-code is wrong then ATM account will be blocked (Okokpujie, Olajide, John, & Kennedy, 2016). In this method it could be noticed that it has an alternative method for fingerprint authentication in an emergency situation it can be done by using a reliable person and theft can be protected using two way verification with OTP, so it is better security model for ATM and Banks than the other methods.

It was suggested that working with only PIN can be crack by hackers or can be misused by someone else so it was suggested a PIN with OTP (Sankhwar

& Pandey, 2016). It is simple and little bit more security than traditional method, also it prevent the card clone and skimming from others (Sankhwar & Pandey, 2016).

## COMPARISION AND DISCUSSION

*Table 1 Comparison of Security Systems*

| No. | Security System | Perfor-mance | Accuracy | Cost | Flexibility | Total score |
|---|---|---|---|---|---|---|
| 1 | PIN (Classical Method) | VL (0) | VH (8) | VL (5) | N (1) | 14 |
| 2 | PIN and Fingerprint | L (3) | H (6) | L (4) | N (1) | 14 |
| 3 | PIN and Face Detection | L (3) | M (3) | M (3) | N (1) | 10 |
| 4 | PIN and Iris - Retina | H (9) | VH (8) | H (2) | N (1) | 20 |
| 5 | Face Detection and OTP | M (6) | H (6) | M (3) | N (1) | 16 |
| 6 | PIN and OTP or Biometric (Fingerprint) | M (6) | H (6) | M (3) | Y (5) | 20 |
| 7 | Palm Vein and UIN | H (9) | H (6) | H (2) | N (1) | 18 |
| 8 | PIN and Face Image | M (6) | L (0) | M (3) | N (1) | 10 |
| 9 | Sensors with GPS with Other method (PIN) | M (6) | M (3) | VH (1) | N (1) | 11 |
| 10 | PIN, Fingerprint and OTP | VH (12) | H (6) | M (3) | N (1) | 22 |
| 11 | PIN and Fingerprint or S-code and OTP | VH (12) | H (6) | M (3) | Y (5) | 26 |

Table 1 shows eleven (11) different combination of authentication methods including classical method to compare and discuss about the advantages and disadvantages. Security Performance, Accuracy, Cost and Flexibility were selected as the important attributes for the comparison.

PIN only authentication method is the classical method which is used by most of the users since it is easy and conventionally used from the beginning. But the method numbers 2, 3 and 4 in table 1 use two-factor authentication methods implemented with biometric feature in addition to PIN authentication.

Iris-Retina provides higher security performance and accuracy than the other two biometric methods. However the cost for Iris-Retina is more expensive than face detection and fingerprint methods.

Face detection and OTP, gives users for two-factor authentication with OTP method used instead of PIN. It has a disadvantage that it depends on another device to get OTP, therefore in case of battery dead or missed of phone makes trouble in transactions. But, normally face detection biometrics identification system does not given higher cost like Iris-Retina (Karovaliya,.et al., 2015). The flexibility of these method numbers 1, 2, 3, 4 and 5 in table 1 are low since there is no any alternative for authentication.

Method number 5 provides alternative authentication method. It gives options to choose OTP or biometric (fingerprint) method as the alternative one for other thus it is flexible than the methods discussed above.

Palm Vein and UIN security system Bank ATM needs an additional sensor to scan user's hand, so the cost for that system is not much higher and also it provides two way verification. The performance and Accuracy are higher than traditional methods but there is no flexibility.

PIN and Face image method is not much preferred, because to match an image in the database with a captured image using a camera may produce many errors. Also it may consume more computing power and time to process image. Therefore the performance and accuracy are not much ideal and the cost for database and other devises are higher.

The method shown at the number 9 designed for reducing robberies of ATM and it consist of many sensors and devices, thus the cost is very high. This method can be used as additional security (physical) of any authentication method, thus the performance, accuracy and flexibility are depend on the method used for authentication. However this is a very useful method for the purpose of trace culprits after any illegal attempt happened at the ATM. By use it as hybrid method with a best two-factor or three-factor authentication method then the security will reach the peak.

The method with PIN, fingerprint and OTP system given at method number 10 in table 1 provides a high security with three-factor authentication. It is very difficult to crack this system. The accuracy of this system is very high and the cost is not much higher like with advanced sensor. But the main drawback of this method is no flexible and will consumes some more time for authentication process.

The identified drawback of above method is fulfilled on last method given in table 1. It provide flexibility with security at alternative authentication step. It's a cheaper method when comparing with its security performance because it needs only fingerprint sensor while providing higher performance with more flexibility. This system provide flexibility by two different category of second step verification. Therefore this can be considered as the best authentication method among all the method that were discussed on this paper. However there is gap for physical security of ATM is still exist. And only technologically sound people will desire to use this kind of system since it has some complexity

## CONCLUSION

Here it has been discussed most of the available and popular ATM security systems. Among the all methods it is able to conclude that two-factor and three-factor authentication methods are providing higher security to ATM protection and also it is necessary to provide physical security to protect against the robberies in ATM.

From this study it can be concluded that the authentication method with PIN and Fingerprint or S-code and OTP is the best method to provide secure authentication of ATM access. Meanwhile the system including GPS and sensors provide solution for physical security of an ATM system to protect and trace illegal activities at the ATM.

Therefore it can be recommended that a system with the combination of both these systems will provide a best security solution for ATMs in terms of authentication and illegal physical activities.

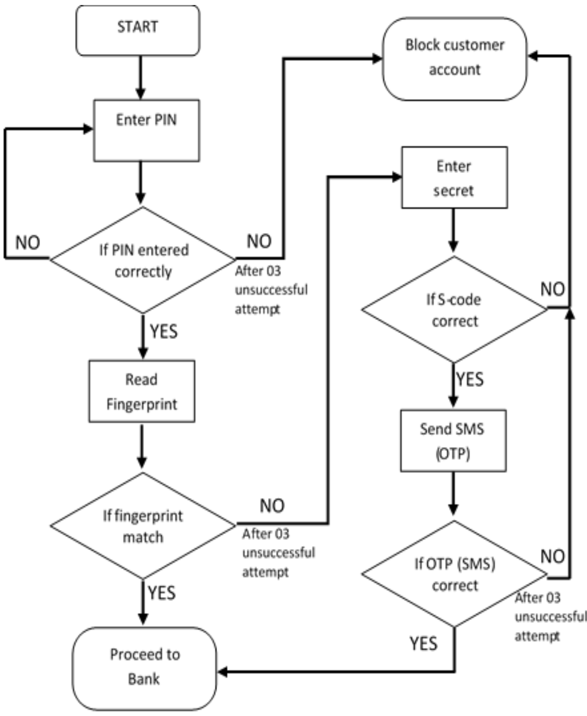

*Figure 3 Recommended Authentication Model (Okokpujie et al., 2016)*

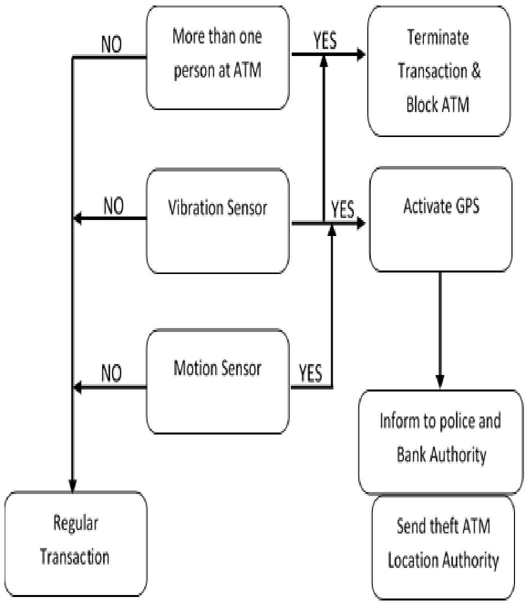
More than one person at ATM
NO
YES
Terminate Transaction & Block ATM
Vibration Sensor
NO
YES
Activate GPS
Motion Sensor
NO
YES
Regular Transaction
Inform to police and Bank Authority
Send theft ATM Location Authority

*Figure 4 Recommended illegal physical activity protection model (Maiti et al., 2016)*

## REFFERENCES

Shaikh, A. A., & Shah, S. M. (2012). Auto Teller Machine (ATM) Fraud – Case Study of a Commercial Bank in Pakistan, *International Journal of Business and Management*, 7(22).

Bhosale, T. (2014 March). SECURITY IN E-BANKING VIA CARDLESS BIOMETRIC.

Jebaline, G. R. & Gomathi, S. (2015). A novel method to enhance the security of ATM using biometrics, *IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT*, ( pp. 2–5).

Nelligani, B. M., Reddy, N. V. U., & Awasti, N. (2016). Smart ATM security system using FPR, GSM, GPS, *Proc. Int. Conf. Inven. Comput. Technol. ICICT 2016*.

Ray, S. (2015). An Intelligent Vision System for monitoring Security and Surveillance of ATM, (pp. 3–7).

Karovaliya, M., Karedia, S., Oza, S., & Kalbande, D. R. (2015). Enhanced security for ATM machine with OTP and Facial, *Procedia - Procedia Comput. Sci.*, 45, (pp. 390–396).

Hamid, M. (2015). Securing ATM with OTP and Biometric, *Int. J. Recent Innov. Trends Comput. Commun.*, 3(4), (pp. 2041–2044).

Prasanthi, A. S., Hussain, B. V., Kanakam, S. M., & Chakravarthy, P. (2015). Palm Vein Biometric Technology : An Approach to Upgrade Security in ATM Transactions, *Int. J. Comput. Appl.*, 112(9), (pp. 1–5).

Kibona, L. (2015) Face Recognition as a Biometric Security for Secondary Password for ATM Users . A Comprehensive Review, *Ijsrst* |, 1(2), (pp. 1–8).

Maiti, S., Vaishnav, M., Ingale L., & Suryawanshi, P. (2016). Atm Robbery Prevention Using Advance Security, (pp. 1022–1024).

Onyesolu M. O., & Okpala, A. C. (2017, October). Improving Security Using a Three-Tier Authentication for Automated Teller Machine ( ATM ), (pp. 50–56).

Okokpujie, K., Olajide, F., John, S., & Kennedy, C. G. (2016). Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128 with GSM Feedback Mechanism.

Sankhwar, S., & Pandey, D., (2016 June). A Safeguard against ATM Fraud, *Proc. - 6th Int. Adv. Comput. Conf. IACC 2016*, (pp. 701–705).