International Journal of Engineering & Technology, 7 (4) (2018) 3999-4002

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.15176
Research paper

Multi-tier authentication approach for ATMS

S. Vasanthapriyan [1] *, S. Thuseethan [2], C. U. Wimalasooriya [3]

[1] Department of Computing and Information Systems, Sabaragamuwa University of Sri Lanka, Sri Lanka
[2] School of Information Technology, Deakin University, Australia
[3] Department of Computer Science and Software Engineering, University of Canterbury, New Zealand
**Corresponding author E-mail: priyan@appsc.sab.ac.lk*

Abstract

ATM has become insecure since incredible increase of trendy crimes related to this. Currently, ATM authentication is insecure, use no more than an access card with a PIN for verification. This research looked into the development of a multi-tier authentication approach that inte-grates more than one mechanism in the identity verification process used in ATMs. Recently biometric identification techniques have be-come popular such as facial recognition and fingerprint recognition. It has made significant efforts to rescue the insecure situation at the ATM points. These days Pattern Drawing is also one of the most growing security mechanisms. The combined authentication approach is to serve the purpose both the identification and authentication that card and PIN do in recent years. Proposed plan includes face recognition, fingerprint and pattern drawing together as layers. As far as security concerns proposed approach shows four times better performance than the existing approach in real environments.

Keywords: *ATM; Facial Recognition; Fingerprint Recognition; Pattern Drawing; PIN.*

1. Introduction

At present, consumers have realized to rely on and trust the ATM to conveniently do their banking activities; many people are using ATM machines frequently. ATMs are just machines allow electronic transactions located in different places. The rapid growth of banking technology has numerous pros and cons in the day to day activities of the bank and transactions are the initiation of ATMs. The main advantage for customers is they can make several basic transactions without the assistance of bank staffs for 24 hours. Other than that by using ATM, users can accomplish numerous banking activities like money transfer, cash withdrawal, credit card payment, paying bills such as phone and electricity bills. It is more convenient for users to handle their accounts which are given by banks and to conduct transactions through ATMs.

Security is always a serious and common issue in ATM system practised today. It is identified that the necessity of security in banking system playing vital role meanwhile there is urgency for improving that. During the last decade there had been a proliferation of different types ATM frauds around the globe and reasonably decreased somehow. Figure 1 indicates the frauds occurred in UK during last five years. The management of such risks associated with ATM fraud and weakening its impact are important issues that are faced by financial institutions as fraud techniques have become more progressive with enlarged occurrences.

In the area of ATM Security, the existing framework [1] has ten essential functions ranges from AF-SEC-01 to AFSEC-10.

i) Identification and Verification;
ii) Controlled Access and Authorization;
iii) Protection of Confidentiality;
iv) Protection of Data Integrity;
v) Strong Accountability;
vi) Activity Logging;
vii) Alarm Reporting;
viii) Audit;
ix) Security Recovery;
x) Management of Security;

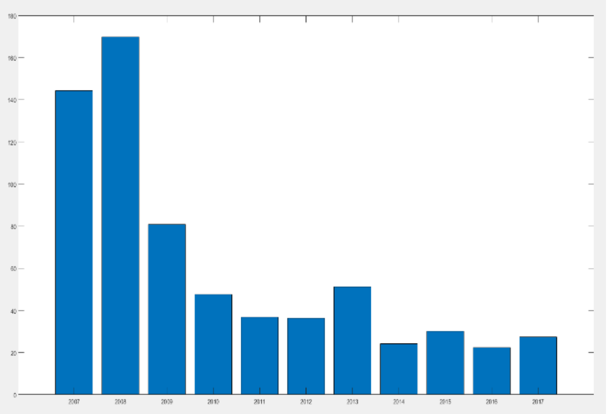

Fig. 1: Counterfeit Card Fraud in the UK (Source: Https://Www.Financialfraudaction.Org.Uk/Fraudfacts17/ Last Accessed 01 May 2018).

However, all these security requirements have not taken into consideration in this research. AF-SEC-01 has been considered here. Traditionally, it has been handled by requiring the combination of the readable card (i.e. ATM debit and credit cards) and private password known as Personal Identification Number (PIN). PIN number has to be remembered forever by the customer and it shouldn't be shared with others to avoid illegal access of account details [2]. Whatever the crime related to ATMs is certainly a serious issue; it affects customers as well as the bank. If any crime occurs then the trustworthiness of bank will be in question.

Thieves engage with ATM cheating put a clear, thin and rigid plastic sleeve into the card slot of ATM. By doing this, when you insert your ATM card, the machine can't read the strip at all, so it will be expecting you to re-enter the PIN [3]. While doing this, the hackers will note the tap of your PIN and he can effortlessly guess the 4-digit PIN. The thieves then remove the plastic sleeve and use their account. The key solution stated here to this problem is the combination of biometrics authentication and Pass Pattern.

This paper proposes one multi-tier security framework including two biometric methods and one mathematical Pass Pattern method. This proposed system has evaluated under certain limitations as a prototype

2. Analysis of existing technologies

2.1. Present controls

These days ATMs are giving so much of assistance to the economic world in various ways. Several problems were resolved with the invention of these ATM machines such as release the traffic inside the bank during peak hours. But customers have to follow control mechanisms to get access to ATMs. By considering the number of transactions being handled by several branches of a particular commercial bank, secured and proper control in the form of authentication and identification is significant. Several control parameters have been imposed together in place to make sure the interests of all stakeholders such as cardholders, issuers, third party processors and acquirers. In this manner existing controls imposed mainly include two parts, those are cards and pins. In cards, details are guarded safely with the help of strong algorithms. During communication, strong encryption is embossed and PANs are masked. On the other hand, PINs are secured in several ways; dispatched separately to users, selectable pin options are used to avoid insider compromise.

2.2. Biometric system

Biometrics is the science or technology which measures the behavioural or physical characteristics of human and that can be captured and statistically analyzed with another sample or human. In this sense, in the field of computer science, biometrics denotes to technologies that measure and analyzes characteristics of the human body. Authentication by biometric verification is becoming popular in corporate and public security systems. For the authentication purposes, some of them have been used such as DNA, eye retinas, fingerprints, voice patterns, facial patterns. The driving force behind the biometric verification has been convenience and easy. Any biometric characteristic which satisfies the following requirements can be used for authentication purposes [3]:

i) Universality: All human should acquire the particular biometric characteristic [4].
ii) Distinctiveness: This is a unique characteristic of every individual and there is considerable dissimilarity between any two persons [5].
iii) Permanence: The characteristic which should be constant over a particular time period and remains unchanged [6].
iv) Collectability: The nature of the characteristic could be measurable using a sensing device [7].
v) Performance: The level of accuracy and how much quick in recognition, the resources needed to reach the expected level of recognition and the environmental and operational factors that influence the speed and accuracy [8].
vi) Acceptability: Up to which extent people are keen on accepting to use a specific biometric identifier [9].
vii) Resistance/Circumvention: The level of difficulty to bypass or defeat a particular system [10].

2.3. Comparison of biometric system

Human physical characteristics can be accurately determined and verified using biometrics technology. To express it simply, instead of PINs it turns the human body as verification, which cannot be 100 % impersonated by others. Among these four methods, we chose fingerprint and face recognition as second and third layers based on our analysis. The following are some important papers proposed by various authors all around the world for enhancing the security using face recognition. The single biometric check has proposed in all previously proposed systems and it has been stated that a single biometric is not enough to impose security on data sensitive systems. More than one method should be incorporated to make it more efficient in such sensitive background. But Iris identification and voice verification cost more than other methods and maintenance is also extremely difficult. This makes the existing system more cost and more complicated. Having such a complicated system may fit urbanized areas, but can't match easily in rural areas. At the same time, it increases the expenses of the particular financial organization. Table 1 shows the comparison of biometric methods

Table 1: Comparison of Biometric Methods

Methods	Pros	Cons
Finger print	Comparison of several features of the finger- print pattern like arch, loop and whorl	Creating a forged and latent fingerprints is very easy and cause issues
Iris	One of the more secure methods of authentication and unambiguous positive identification of an individual	It can be forged by wearing contact lenses with an iris pattern
Face	Can be done with the help of one video or image file. No need of special equipment	Less effective because of variety of variations of one person's face
Voice	Provides two way securities with your voice and the word which you have used	Easy to do forgery using mimicry

2.4. Dynamic pattern drawing system

Normally human can easily identify and remember shape or pattern than the set of characters; Dynamic Pattern Drawing is a growing scheme of authentication technique based on this idea. Rather than traditional passwords, users can authenticate by drawing the patterns as the password. It is very useful because of simplicity, immune to all possible attacks, doesn't require extra computational power and hardware. Figure 2 indicates the traditional pattern drawing password mechanism.

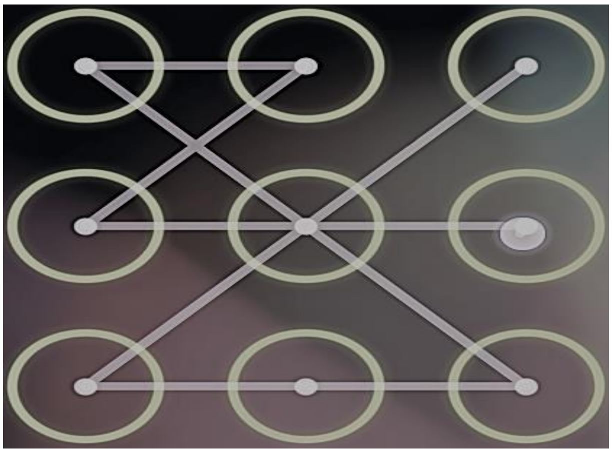

Fig. 2: Pattern Drawing Password Mechanism.

3. Proposed approach

Last few years, many authors tried researching on enhancing ATM security using biometrics and some other existing methodologies. Even though, they could not derive efficient methodologies with multi-tier architecture. The proposed approach has four distinct tiers. It is as described in Figure 3. Furthermore, Algorithm 1 also describes the proposed approach.

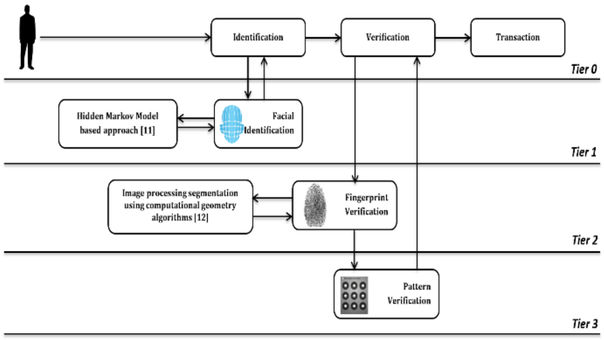

Fig. 3: System Architecture.

```
Algorithm 1. Proposed system flow
1     User inserts ATM Card:
2     Tier 0
3     User identification GOTO STEP 3
4     Using facial recognition for identification: Tier 1
5     If validated identification GOTO STEP 5 ELSE GOTO STEP 10
6     Finger print verification: Tier 2
7     Pattern verification: Tier 3
8     If verified successfully GOTO STEP 8 ELSE GOTO STEP 10
9     User gets authenticated
10    Executes Transaction
11    Stop
```

3.1. Tier O

This is the top level flow of the ATM mechanism. The user enters to do transactions in ATM; inserts the card issued. Before enters, the Transaction mode ATM system should identify and verify the right user. Once the user enters the card he/she will be directed to identification phase where the ATM system recognizes the valid user. After the identification process, all identified users are directed to verification stage where identified users are validated.

3.2. Tier 1

In Tier 0, once the user inserts the ATM card, the machine requests the facial identification which checks with the database. This procedure can be done in Tier 1 as facial identification where the captured image has been processed with existing database. The process of identification is shown in Figure 4. If the face matches with the database, he/she will be directed to Tier 2 with successful identification. If the face doesn't match, he/she will be exited from the ATM system. To recognize face Hidden Markov Model [12] has been used.

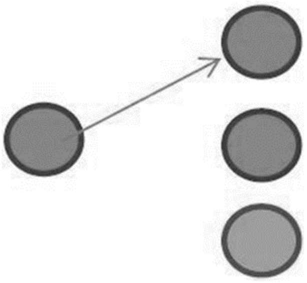

Fig. 4: Process of Identification.

3.3. Tier 2 and Tier 3

Once the user passes the identification processes positively he/she has to go through the two-tier verification process. In fingerprint and pattern drawing verifications are imposed in these two tiers respectively. We used the method proposed by Chrissikopoulos and Alexandris [12] based on image processing segmentation using computational geometry algorithms to verify the fingerprint of the user. Meanwhile, users are verified with a pattern given to them. Successful pass of tier 2 and 3 routes the user to make transactions.

4. Testing and evaluation

4.1. Laboratory based functional prototype testing

To understand the technological working flow without trained users, we formed the functional prototype evaluations. We have carried out this trial with approximately three hundred (300) participants. As the initial test of the prototype, the assessment was chiefly concentrated on the performance of the technology such as accuracy and reliability. From the sequence of testing carried out, we have proved that the proposed system is realistic and could be implemented in a real environment. The result of the initial test is indicated in Table 2.

Table 2: Result of the Initial Test

Tiers	Major Test	Attempts					
		=1	%	=2	%	>2	%
Tier 1	Facial Identification	247	82.33	43	14.33	10	3.33
Tier 2	Finger Print	203	67.67	88	29.33	09	3.00
Tier 3	Pattern	289	96.33	08	02.67	03	1.00

Based on the results, the reliability level is excellent (96.33%) in tier 3 and very good (82.33%) in tier 1. In tier 2, however, the reliability level is not in the expected level (just over 67%) due to several reasons. However, only a few candidates find difficulties in all three tiers-3.33%, 3.00% and 1.00% in tier 1, tier 2 and tier 3 respectively. Although the overall reliability of the proposed system is lower compared to the current system, the accuracy is far better. In terms of accuracy, the current system is vulnerable against major problems such as forgetting ATM pin number, loss or damage of ATM cards, the danger of card getting stuck and any fraudulent activities related to ATM card and PIN. Various forms of fraud are eliminated, ranging from; card theft, Pin theft, Card reader and PIN pad techniques, force withdrawal and lot more. The result of the accuracy test is excellent showing 100% preciseness-no any illegal detection permitted throughout the experiment.

4.2. Laboratory based usability testing

In the second stage of the testing prototype, the assessment was largely concentrated on the usability of the taken technology and the system. Since the technology is not cohesive, participants are required to remember whatever needed to perform when they asked to re-operate the system after some time. Due to this, the reliability of this approach was in question. Most of the participants have noted that the system was slightly slower than anticipated, and
19% reported experiencing problems using the system. Perhaps, not surprisingly, the new approach was considered usable- strongly accepted by 97% of participants because of its high level of usability. After the completion of prototype testing, several changes have made, were merged into a self-service ATM with appropriate graphical interfaces with well-organized task flows for users. During the development, we ensure the maximized usability to reduce the negative impact on user's mind. It was very crucial during the prototype development. From our university, 80 students were randomly selected and asked to undergo the lab usability trail of our authentication system.

The expert level of using computer systems varied from one human subject to another. The majority of human subjects were around 20 to 24 since they all are undergraduates. The gender distribution is 69% of males and rest of the others are females.

The identification process has been undertaken by a properly structured facial recognition system. After the identification with the use of facial recognition, users had 100% satisfaction about the enrolment of the ATM, had triggered a positive change in their opinion about the identification approach. Immediately after the identification, users are routed towards two layered verification process. After the two-step verification process of logging into the system, 91%

of users quoted a positive change in attitude. Only a few had some concerns, 9% users feel uncomfortable while using the two-step verification. Under the laboratory conditions of the prototype system, 94% of users accepted that they have gone through a more secure authentication system and felt confident while using the system. Only 6% still have some concerns and negative perspective about the proposed approach.

Overall, the system's level of usability is adequately meeting the expectations of the users involved in the testing process.

5. Conclusion

As the usage of ATM in money transactions is increasing, it opens the path to several security threats. Usually, greater security and convenience can be achieved by applying biometrics than any other traditional methods of personal recognition in any computational systems. Here the major reason for integrating biometric systems in ATMs is to increase the overall security. The final result of the research shows that respondents are much comfortable with the proposed system while enjoying the greater security. Despite the drawbacks in reliability, the proposed system has significant improvement as its accuracy is far better than the current systems showing 100% preciseness.

References

[1] The ATM Forum Technical Committee, ATM Security Framework 1.0, AF-SEC-0096.000, February 1998.

[2] S.S.Das and Debbarma, "Designing a Biometric Stradegy fingerprint Measure for enhancing ATM Security in Indian e-banking system", International Journal of Information and Communication Technology Research, Volume.1,No.5,pp.197-203, (2011).

[3] Jain A.K, Ross A. and Prabhakar S, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, 14, 4-20, 2009. https://doi.org/10.1109/TCSVT.2003.818349.

[4] Ross, A., & Jain, A., "Information fusion in biometrics", Pattern recognition letters, 24(13), 2115-2125, (2003). https://doi.org/10.1016/S0167-8655(03)00079-5.

[5] Jain, A. K., Ross, A., & Prabhakar, S., "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20, (2004). https://doi.org/10.1109/TCSVT.2003.818349.

[6] Faundez-Zanuy, M., "Data fusion in biometrics", IEEE Aerospace and Electronic Systems Magazine, 20(1), 34-38, (2005). https://doi.org/10.1109/MAES.2005.1396793.

[7] Chang, K., Bowyer, K. W., Sarkar, S., & Victor, B., "Comparison and combination of ear and face images in appearance-based biometrics", IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9), 1160-1165, (2003). https://doi.org/10.1109/TPAMI.2003.1227990.

[8] Mansfield, A. J., & Wayman, J. L., Best practices in testing and reporting performance of biometric devices, Teddington, Middlesex, UK: Centre for Mathematics and Scientific Computing, National Physical Laboratory, 2002.

[9] Deane, F., Barrelle, K., Henderson, R., & Mahar, D., "Perceived acceptability of biometric security systems", Computers & Security, 14(3), 225-231, (1995). https://doi.org/10.1016/0167-4048(95)00005-S.

[10] Derawi, M. O., Nickel, C., Bours, P., & Busch, C., "Unobtrusive user authentication on mobile phones using biometric gait recognition", 2010 Sixth International Conference on in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), (2010).

[11] Salah, A. A., Bicego, M., Akarun, L., Grosso, E., & Tistarelli, M.,"Hidden Markov Model-based face recognition using selective attention", International Society for Optics and Photonics in Electronic Imaging 2007,(2007).

[12] Chrissikopoulos, M. P. E. M. V., & Alexandris, N., "Secure fingerprint verification based on image processing segmentation using computational geometry algorithms", ACTA Press, (2003).