International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)

Impact Factor: 5.858 (SJIF-2019), e-ISSN: 2455-2585

Volume 6 , Issue 8 , August -2020

ENHANCING THE SECURITY OF ATM TRANSACTION BY PROVIDING THREE FACTOR AUTHENTICATION

Mitul Patel

School of Engineering P Savani University, Surat

Abstract— In our daily-life, we use ATM for cash Transaction. One of the important parameter that we need to consider during ATM transaction is Security. In current ATM system, we use the two factor authentication (ATM card and 4 digits PIN) for performing transaction. But we have observed that there are some vulnerabilities possible with such types of transaction which will give loop hole for attacker to perform some attack on ATM transaction. In this paper, we have designed a model to enhance the security of ATM by applying Three Factor Authentication. Along with ATM card and ATM PIN, if we include the third factor (face recognition) then we can have a better security compared to the two factor authentication.

Keywords— ATM, PCA, Three Factor Authentication

I. INTRODUCTION

We are living in an era of Technology where money is an essential component of daily activities. In the ancient times, people need to visit Banks to withdraw and deposit money where they follow traditional approach of form filling to perform any transaction. Nowadays due to the Technology evolution, ATM machines are available for performing any transaction. ATM machines can be used for performing any transaction from any places at any time. As the data is transferred through online mode, it requires the security at various stages of transaction. ITU-T has provided five security services that are needed when performing any online transmission [1]:

- ***Data Confidentiality*** – protecting data from unauthorized disclosure
- ***Data Integrity***-protecting data from unauthorized modification
- ***Authentication***- authentication (proof of origin/entity authentication) of sender or receiver
- ***Non-repudiation*** – protection against repudiation of sender or receiver
- ***Access Control*** – protection against unauthorized access to data

The first step in Banking Transaction is to validate the user whether he/she is authenticated person for performing any transaction or not.

A. AUTHENTICATION IN BANKING

Authentication means to check whether the user at other side (sender/receiver) is authenticated user (having rights to send or receive data) or not. Authentication technology basically checks the user's identification with the stored identification in database to check whether there is matching or not. If matching is found, user is authenticated otherwise the user is not authenticated and he will be not given any access to use further information. The simplest example of user authentication is password-based authentication [3]. When the user registers with any web-site or any organization, he has to prove his unique user ID and password which is stored on authentication server. When the user wants to login again, his credentials are checked with stored credentials. Only the users having matching credentials can login to system and get further information [3].

In multifactor authentication, user is authenticated by more than one factor. It can be accomplished through biometric factors like fingerprint, iris, voice or some possession factors like security keys. There are basically three types of authentication factors used in multifactor authentication [3].

1) Knowledge: Something that the user knows e.g. password and PIN. There are two kinds of knowledge-based authentication: Static KBA and Dynamic KBA. In static KBA, users have to set answers of some security questions when they set up a system or password-protected profile. If the password is forgotten or the user wants to renew the password, he has to provide the answers to security questions that he has provide earlier. In dynamic KBA [4], the user will be provided such type of security questions whose answers are known to user as well as the system. The IT systems know the answer by performing some data mining technique on previously gathered data of the user. Although the security criticality of dynamic KBA is high, many companies prefer static KBA due to the challenges involved in dynamic KBA.

2) Possession: Something the user has e.g. hardware token. Users are authenticated by some devices or objects like smartcards and Universal Serial Bus (USB) [5]. The tokens (devices) used in possession-based authentication can be connected tokens or disconnected tokens. Connected tokens can be card readers, wireless tags or USB tokens while a disconnected token [5] device will use a built-in screen to display authentication data which is then utilised by the user to sign in, where and when prompted.

3) Inherence: Something that verifies the user e.g. Fingerprint or voice. Inherence factor are biometric factors of users [3]. The user is authenticated based on some physiological characteristics like fingerprint, iris movement or voice or user is authenticated based on some behavioural characteristics. Some distinguish and repeatable features can be extracted from the user for the purpose of automated identification.

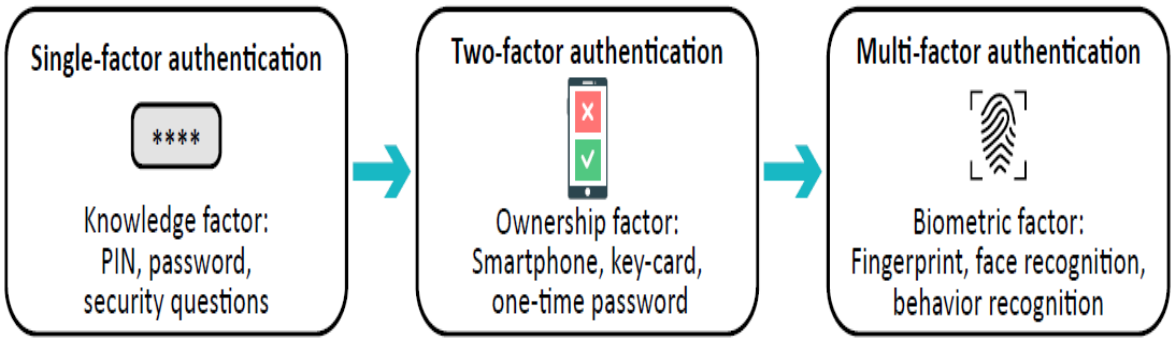

Fig 1: Evolution from Single Factor Authentication to Multifactor Authentication [11]

As shown in Fig 1, In ATM transaction, the user is authenticated by two factor authentication:

1. ATM card that is possession factor of Multifactor authentication
2. 4-Digit ATM pin that is knowledge factor of Multifactor authentication

B. Attacks on ATM transaction using Two Factor Authentication

1. Eavesdropping: If your ATM card and PIN number is stolen, attacker can perform the transaction on your account.
2. Spoofing: ATM cards can be cloned to access user's account or there have been cases of incidents of fraud where criminals have used fake machines or have installed fake keypads or card readers to existing machines. These have been used to record customer's pin number and bank accounts and have then used this information to create fake accounts and steal money from customers.
3. Brute-force attack: ATM does not prevent identity theft and fraud. Using the brute force, if we try to crack the current static four digit PIN it can be done in 9999 attempts, thus weakening the security.

C. Biometric Comparison [13]

TABLE I

COMPARATIVE ANALYSIS OF VARIOUS AUTHENTICATION FACTORS OF MUTIFACTOR AUTHENTICATION

	Multifactor Authentication								
[16]	**Knowledge (Something user know)**		**Possessions (Something user has)**				**Inherence (Something user is) (Biometric)**		
	Static Scheme	**Dynamic Scheme**	**Connected Tokens**			**Disconnected Tokens**	**Fingerprint readers**	**Iris Scanners**	**Voice**
			Card Readers	**Wireless tags**	**USB tokens**				
Security Criticality	Low	High	High	Low	High	High	High	High	Low
Computational Cost	Low	High	High	High	High	Low	Low	High	High
Advantages	Pre-agreed Questions and answers, easy to set up	able to prevent fraud and offer customers added protection	More secure than Payment cards and adaptable to system	No need of LOS, Easy to deploy in Real time Applications	Third Part Authentication Increase trust	Simple to Use, immune to coverage, latency, and delivery issues, Supports data Signing function	Economic and easy	Most accurate, one sample can last for lifetime	Reliable Easy to use
Disadvantages	Attacker can Use public Information of entity to find answers	difficult to implement and requires hard-to-acquire information	Installation And Distribution of certificates	Easily intercepted, Limited coverage Range	User need to carry an additional Smart card	Possibility of web attacks, breach of codes, susceptible to fraudster attack if OTP generator poorly implemented	Time taking, dry and dirty fingertips	Expensive, Susceptible To poor Image Quality	Stealing Of Voice is Possible, Require more File storage

II. PROPOSED THREE FACTOR AUTHENTICATION IN ATM TRANSACTION:

As shown in Table I, three factor authentication involves something a user knows, something a user has, and something a user is. Examples would be a password (something a user knows), an RSA token (something a user has), a fingerprint (something a user is). Three-factor authentication is mainly used in businesses and government agencies that require high degrees of security. The use of at least one element from each category is required for a system to be considered three-factor authentication. In this paper, along with Two factors of ATM authentication, third factor possession is also included for ATM transaction. We have included the Face Recognition as possession factor for ATM transaction [Fig 2]:

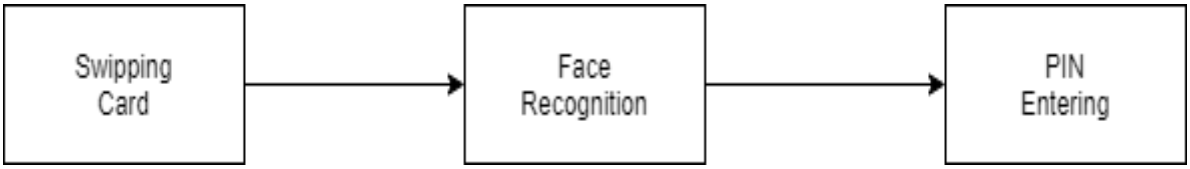

Fig 2: Three Factor Authentication

A. *Facial Recognition*

At this stage a user simply needs to look into the camera installed on ATM. In general, face recognition techniques can be divided into two groups based on the face representation they use:

1. Appearance-based: It uses holistic texture features and is applied to either entire face or only to the specific regions in face image. Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminate Analysis (LDA) fall under this category [8].
2. Feature-based: It uses geometric facial features (mouth, eyes, nose, etc.) and geometric relationships between them [8].

Our model uses Principal Component Analysis. To build Eigen faces, good data is required for component matching. The Eigen faces are ordered from largest to lowest, where the Eigen faces having larger eigenvalue finds greater variance as compared to those having less eigenvalue. From this set of Eigen faces only first K of them are selected which exhibits most of the unique properties. An advantage of PCA to other methods is that the 90% of the total variance is contained in 5-10% of the dimensions [8]. There are some advantages of PCA based Facial Recognition which makes it suitable for application in ATM transaction [8]

1. Time taken for computation is very less as it considers only the essential components from images.
2. Based on multiple face images as input, i.e. it considers multiple input images of each person with different expressions and under different lightening conditions.
3. Demands less storage space for storing dataset.
4. Smaller database representation since only the trainee images are stored in the form of their projections on a reduced basis.
5. Reduced dimensions increase the efficiency of the process.

B. Steps for authentication:

1. If it’s first time access of ATM card, generate the new PIN by sending OTP information on mobile phone. Also perform the PCA based facial recognition and store the features in data-base.
2. For the next use of ATM card, Capture the image from the webcam and detect face from it. If more than one face us captured in an image, then temporary block the access of account for security and privacy reasons. If only one face is captured, then continue the process.

C. Flow-chart for Three Factor Authentication in ATM transaction

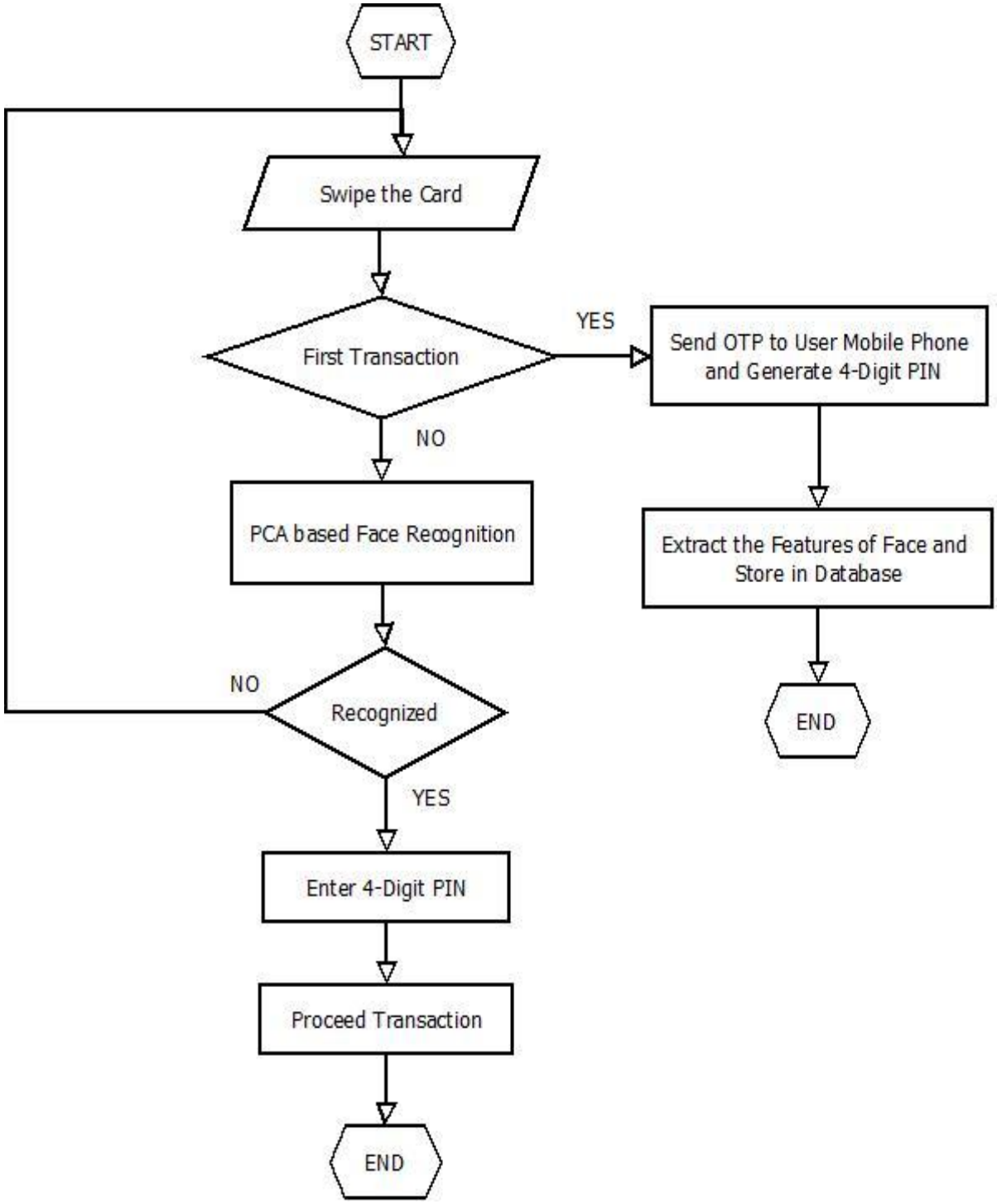

Fig 3: Flow-chart for Three Factor Authentication in ATM Transaction

D. Drawback of the Model

One of the major drawbacks is if the camera is not working properly then it's not possible to recognize the face which can hinder the transaction. Also the face is changed due to beard or aging, the camera is not able to match with stored features of face so it might possible that face can't be detected.

III. CONCLUSIONS AND FUTURE WORK

In this paper, we have proposed a system that can enhanced the security of ATM transaction by performing Three factor authentication rather than tradition two factor authentication. The Three Factor Authentication includes the three factors: ATM Card, ATM PIN and Face Recognition for performing any transaction. For performing the Face Recognition, we have suggested to use PCA based face recognition because it requires less computation time and less storage space to store trainee images. Facial recognition techniques are more challenging compared to other biometric techniques so it requires more efficient algorithm which can perform the face recognition efficiently. There are some flaws in face recognition which can be overcome by focusing on only basic features of faces like eyes, nose and ears.

REFERENCES

[1] William Stalling, "*Cryptography and Network Security Principles and Practices*", Fourth Edition, Prentice Hall Publications.

[2] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. "*A. Handbook of Applied Cryptography*". ISBN 0-8493-8523-7.

[3] Syed Zulkarnain, Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann, "*A Review on Authentication Methods*", University Malaysia Perlis.

[4] M. L. Das et al., "*A Dynamic ID-based Remote User Authentication Scheme*", IEEE Transactions on Consumer 630 Electronics, Vol. 50, No. 2, MAY 2004

[5] Jiang Yu, Chuan-fu Zhang, "*Design and Analysis of a USB-Key based Strong Password Authentication Scheme*"

[6] Mahmoud Musa Mohammed, Dr. Muna Elsadig, "*A Multi-layer of Multi Factors Authentication Model for Online Banking Services*", International Conference on Computing, Electrical and Electronic Engineering (ICCIEEE),2013, IEEE.

[7] Kresimir Delac, Mislav Grgic, "*A Survey of Biometric Recognition Methods*", 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia

[8] Mohsin Karovaliyaa, Saifali Karediab, Sharad Ozac, Dr. D.R.Kalbande ,"*Enhanced security for ATM machine with OTP and Facial recognition features*", Procedia Computer Science 45 (2015) 390 – 396, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

[9] Olufemi Sunday Adeoye, "*EVALUATING THE PERFORMANCE OF TWO-FACTORAUTHENTICATION SOLUTION IN THE BANKING SECTOR*", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012

[10] Asoke Nath, Tanushree Mondal," Issues *and Challenges in Two Factor Authentication Algorithms*", IJLTET, Vol.6 Issue 3 January 2016

[11] Aleksandr Ometoy, Sergey Bezzateev,Niko Mäkitalo,Sergey Andreev ,Tommi Mikkonen,Yevgeni Koucheryavy,"*Multi-Factor Authentication: A Survey*", Cryptography 2018, 2, 1; doi:10.3390/cryptography 2010001

[12] Kyungnam Kim," *Face Recognition using Principle Component Analysis*"

[13] Mitul Patel," *A survey on various existing Authentication Mechanisms and their comparison based on Security Criticality and Computational Cost*", IJTIMES, Volume 4, Issue 6, June-2018